ЭЛЕКТРОННЫЕ ДЕНЬГИ

Перевод Руководства ФАТФ по цифровому профилю*

АВГУСТ 2020

При поддержке ЦК НТИ «Центр распределенных реестров СПБГУ»

Ассоциация участников рынка электронных денег и денежных переводов «АЭД» - отраслевая ассоциация, созданная в 2010 году.

Ассоциация является широко признанным центром компетенции по платежам, специализированному финансовому регулированию, повышению доступности финансовых услуг и финансовым инновациям как в России, так и за рубежом. Основные задачи АЭД – устойчивое развитие отрасли, распространение лучших деловых практик и оказание экспертной поддержки для государственных органов и частного сектора.

Сайт Ассоциации: www.npaed.ru, npaed@npaed.ru

Перевод: Анна Леонова
Редактор: Павел Шуст

FATF Guidance on Digital Identity: https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity.pdf

Аннотация Ассоциации к переводу Руководства

В марте 2020 года Группа разработки финансовых мер борьбы с отмыванием денег подготовила Руководство по использованию систем цифрового профиля в целях идентификации клиентов. Изначально рынок ожидал, что Руководство будет затрагивать все методы удаленной надлежащей проверки клиентов в целом. Но в результате ФАТФ описала (хотя и довольно подробно) один из таких механизмов.

Мы, как потребители, уже довольно активно используем цифровые профили – сведения о нас хранят социальные сети, банки, мобильные операторы, бюро кредитных историй и многие другие организации. Другое дело, что надежность этих цифровых профилей очень разная – где-то информация фиксируется со слов, где-то проверяется только частично. В Руководстве детально описывается, как оценить надежность системы цифрового профиля и его уместность для использования в целях идентификации клиентов. Причем хранить цифровые профили смогут не только государственные органы, но и частные организации.

Цикл работы любой системы цифрового профиля легко объясняется принципами IVCId, о которых мы писали ранее. Но, справедливости ради, стоит отметить, что цифровые профили – это не панацея.

Во-первых, существует множество альтернативных, менее затратных методов удаленного подтверждения личности. Тем временем, реализация цифрового профиля – мероприятие весьма затратное.

Во-вторых, любая система цифрового профиля подразумевает единое место хранения клиентских данных. И это в любом случае проблема. Потому что самые надежные меры защиты от киберрисков делают систему экономически невыгодной, а их отсутствие – потенциально уязвимой.

В-третьих, системы цифровых профилей очень часто монопольны. На развивающихся рынках это почти неизбежность. Этот вопрос мало поднимается в Руководстве, потому что не входит в его периметр, но этот риск очевиден. Еще более очевидно, что правительства будут настаивать на том, чтобы такие системы были государственными.

Поэтому вряд ли Руководство, неофициальный перевод которого мы сегодня представляем, отвечает на все вопросы, связанные с удаленной идентификацией. И вряд ли его можно использовать как безусловный план действий. Но совершенно точно этот документ повысит популярность этого решения в глобальном масштабе и будет склонять к выбору именно такой регулятивной опции. К добру это будет или не к добру – посмотрим.

Как и всегда, мы готовы дать разъяснения или организовать обучение по новому документу и теме цифровых профилей в целом. Подробности – по телефону и почте.

Оглавление

ОСНОВНЫЕ ПОЛОЖЕНИЯ

1. Каждый год объем безналичных платежей растет в среднем на 12,7%; согласно прогнозам, к 2020 году число безналичных операций достигнет 726 миллиардов ежегодно[1]. К 2022 году 60% мирового ВВП будет производиться в форме цифровых товаров и услуг[2]. С точки зрения ФАТФ, в этом контексте особенно важно разобраться, как устанавливается личность клиентов, использующих цифровые финансовые сервисы. В мире активно развиваются технологии цифрового профиля, на их основе разрабатываются системы цифровой идентификации. Это Руководство должно помочь регуляторам, субъектам финансового мониторинга[3] и другим заинтересованным сторонам разобраться, как можно использовать системы цифрового профиля для выполнения некоторых элементов надлежащей проверки клиентов согласно 10 Рекомендации.

2. Чтобы внедрить риск-ориентированный подход, рекомендованный в этом Руководстве, критично важно понять, как работают системы цифрового профиля. Во втором разделе приводятся краткие характеристики систем цифрового профиля, которые более подробно описаны в Приложении А.

3. В разделе 3 приводятся основные требования ФАТФ, в том числе обязанность идентифицировать и проверять личность клиента с использованием «надежных, независимых» и первичных документов, данных или информации (Рекомендация 10(а)). В контексте использования систем цифрового профиля, требование «надежности и независимости» означает, что такая система должна опираться на технологию и процедуры, которые обеспечивают высокое качество результатов ее работы. Руководство разъясняет, что идентификация и обслуживание клиентов без личного присутствия может характеризоваться стандартным уровнем риска или даже пониженным уровнем риска, если используется надежная система цифрового профиля и применяются меры снижения рисков.

4. Риск-ориентированный подход, который положен в основу этого Руководства, основан на стандартах оценки надежности систем цифрового профиля (далее – стандарты оценки), который разработан широким кругом экспертов в разных юрисдикциях. ISO и IEC консолидируют эти стандарты и одновременно обновляют другие свои документы, относящиеся к идентификации, информационной

[1] Capgemini & BNP Paribas (2018), World Payments Report 2018, доступно по ссылке https://worldpaymentsreport.com/wp-content/uploads/sites/5/2018/10/WorldPayments-Report-2018.pdf

[2] International Data Corporation (IDC), IDC FutureScape: Worldwide IT Industry 2019 Predictions

[3] Для целей данного Руководства, к «субъектам финансового мониторинга» относятся финансовые учреждения, провайдеры услуг виртуальных активов (VASPs), а также установленные нефинансовые предприятия и профессии (УНФПП), определенные Стандартами ФАТФ, которые обязаны проводить надлежащую проверку клиента в случаях, указанных в 22 Рекомендации. В июне 2019 года ФАТФ пересмотрела 15 Рекомендацию («Новые технологии») и пояснительную записку к ней, чтобы, среди прочего, возложить обязательства по выполнению требований к надлежащей проверке клиента, согласно 10 Рекомендации, и на провайдеров услуг виртуальных активов.

безопасности, защите персональных данных, чтобы в конечном итоге получить комплексный стандарт по цифровым профилям. Стандарты надежности устанавливают разные «уровни надежности». Они оценивают степень надежности и независимости всей системы цифрового профиля и отдельных ее элементов. Хотя стандарты надежности в разных странах могут отличаться, для простоты настоящее Руководство ссылается на стандарт NIST[4] и e-IDAS[5]. Юрисдикциям разных государств следует применять подход, изложенный в этом Руководстве, с учетом национальных технических стандартов и стандартов надежности[6].

5. Стандарты надежности систем цифрового профиля и законодательство по ПОД/ФТ адресованы разным аудиториям. Настоящее Руководство связывает две эти категории документов между собой. Как показано в таблице ниже, основные элементы систем цифрового профиля могут использоваться для исполнения требований по идентификации и верификации личности согласно Рекомендации 10(a), поэтому стандарты надежности и прочие технические стандарты могут быть небесполезны при оценке надежности и независимости систем, которые используются для идентификации клиента в целях ПОД/ФТ.

[4] Руководство по цифровому профилю NIST 800-63 состоит из комплекта документов: Руководство по цифровому профилю NIST SP 800- 63-3 (обзор); NIST SP 800-63A: Руководство по цифровому профилю: Регистрация и проверка подлинности; NIST SP 800-63B Руководство по цифровому профилю: Аутентификация и управления жизненным циклом; и NIST SP 800-63C, Руководство по цифровому профилю: Федеративность и подтверждение аутентификации.

[5] Регламент ЕС N°910/2014 об электронной идентификации и удостоверительных сервисах для электронных транзакций на внутреннем рынке.

[6] Отдельные юрисдикции могут не иметь разработанных стандартов оценки именно для систем цифрового профиля, однако могут иметь актуальные технические стандарты для других продуктов и услуг, например, стандарты по информационной безопасности.

Требования надлежащей проверки клиента (физическое лицо)	Основные элементы системы цифровых профилей
Идентификация/верификация – Рекомендация 10 (а)	Подтверждение личности и регистрация (с привязкой профиля к конкретному лицу) – Кто это лицо? На данном этапе происходит сбор данных (имя, дата рождения, удостоверение личности и т.д.), подтверждение идентификационных данных и проверка их принадлежности конкретному лицу. Привязка профиля к конкретному лицу – создание аутентификаторов, которыми владеет и управляет конкретное лицо. Аутентификация - Является ли человек владельцем учетной записи? На данном этапе необходимо установить, действительно ли лицо владеет ранее выданными идентификаторами и контролирует их. Организация должна соблюдать требования Рекомендации 10(а), если она проводит идентификацию/верификацию потенциального клиента на основе ранее созданного цифрового профиля.

6. Данное Руководство разъясняет две вещи: (1) в Рекомендации 10(а) речь идет об аутентификации клиента, который уже зарегистрирован в системе цифрового профиля, независимой от финансового учреждения и (2) качественная аутентификация клиента при предоставлении доступа к счету может быть полезна для снижения рисков ОД/ФТ.

7. Раздел 5 содержит основные рекомендации для регуляторов, субъектов финансового мониторинга и других организаций касательно того, как применять риск-ориентированный подход и системы цифрового профиля для идентификации и верификации личности, а также для обновления данных о клиентах в соответствии с Рекомендацией 10(d). Мы рекомендуем технологически-нейтральный подход (то есть не советуем конкретную систему цифрового профиля). Он основан на двух элементах:

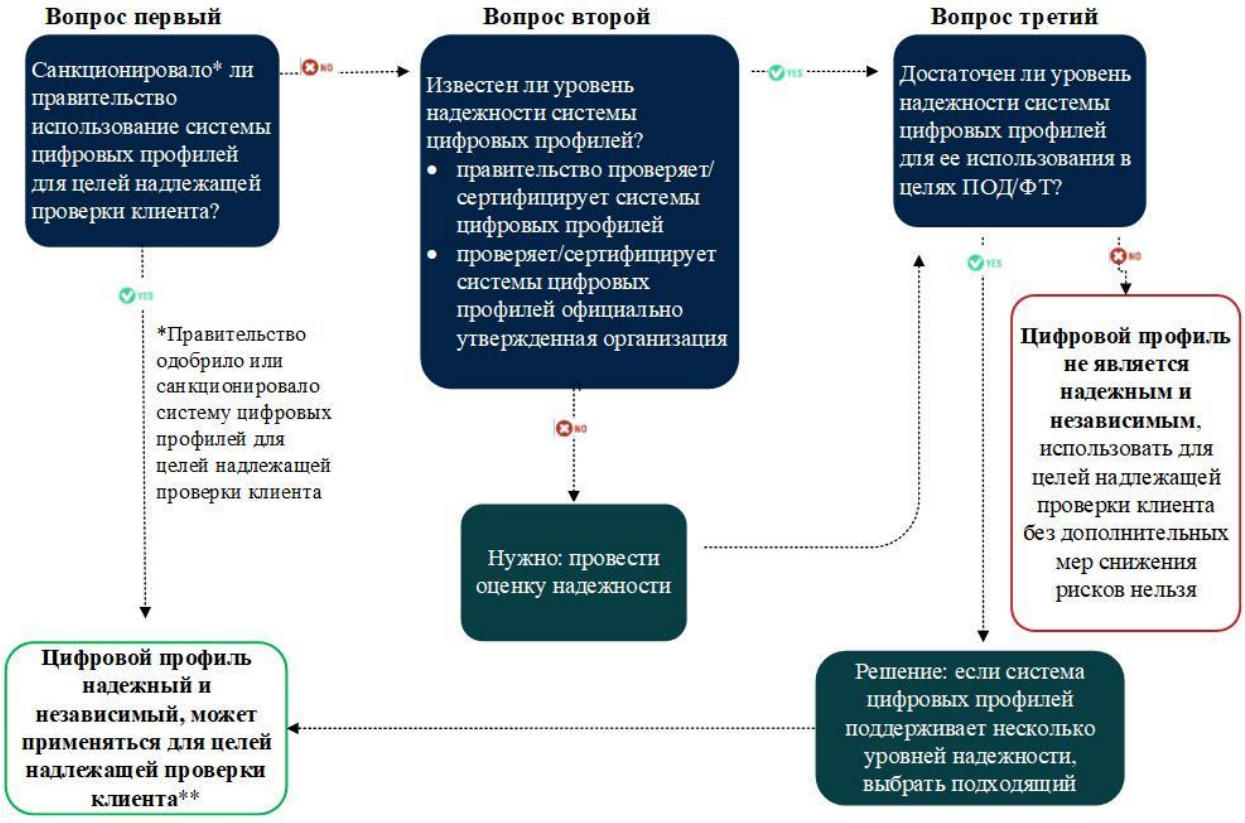
    a. чтобы понять, насколько система цифрового профиля отвечает требованиям надежности и независимости, надо оценить качество каждого из ее элементов (в том числе, технологии, архитектуру и внутренние процедуры) и

b. понять, обеспечивает ли система цифрового профиля достаточный уровень надежности и независимости в контексте именно потенциальных рисков ОД/ФТ, мошенничества и других злоупотреблений.

8. Раздел 5 поясняет, как использовать стандарты качества для оценки надежности/независимости. Здесь также приводится примерный алгоритм принятия решения о том, стоит ли применять цифровой профиль для проведения некоторых элементов надлежащей проверки клиента в соответствии с Рекомендацией 10. Этот алгоритм стоит адаптировать к конкретным обстоятельствам юрисдикции и отдельных организаций. Разработанный алгоритм учитывает, что в зависимости от конкретной системы цифрового профиля и местного законодательства, конкретные решения могут приниматься разными регуляторами и компаниями.

9. Настоящее Руководство не имеет обязательной юридической силы. Оно уточняет стандарты ФАТФ, которые являются технологически нейтральными.

Рис. 1. Описание процесса для субъектов финансового мониторинга



** должны быть соблюдены требования 10 Рекомендации, а также при необходимости приняты соответствующие меры по минимизации риска

10. В Разделе 4 описываются некоторые преимущества и риски систем цифрового профиля. Многие из этих рисков точно так же присущи и для обычных бумажных документов. Однако подтверждение личности или аутентификация через открытые каналы связи (Интернет) создает особые риски – например, возникают опасности кибератак или масштабных хищений персональных данных. С другой стороны, системы цифрового профиля, которые отвечают стандартам надежности могут усилить меры по ПОД/ФТ, способствовать повышению доступности финансовых услуг, улучшить потребительский опыт и снизить затраты финансовых организаций.

11. Руководство описывает, как системы цифрового профиля можно использовать для повышения доступности финансовых услуг. Во-первых, такие системы могут помочь государствам более гибко и прогрессивно подходить к подтверждению личности граждан – в том числе, в целях оказания финансовых услуг. Во-вторых, сами стандарты оценки надежности систем цифровых профилей не предписывают каких-то конкретных процедур подтверждения личности: а значит, их можно адаптировать к конкретной ситуации страны. Наконец, риск-ориентированный подход к надлежащей проверке клиента в принципе может способствовать повышению финансовой доступности – в соответствии с Руководством ФАТФ по финдоступности и ПОД/ФТ (с дополнениями от 2017 года).

Рекомендации для регулирующих органов

12. Следует разработать четкие руководства и нормативные акты, обеспечивающие риск-ориентированное использование надежных и независимых систем цифрового профиля для целей ПОД/ФТ. В качестве первого шага следует оценить, какие в стране есть системы цифрового профиля и как они соотносятся с требованиями по идентификации, верификации и текущей надлежащей проверке клиента (в том числе, хранению данных, полаганию на меры третьих сторон).

13. Необходимо оценить, допускает ли регулирование и внутренние регламенты регуляторов использование систем цифрового профиля – и при необходимости скорректировать их с учетом особенностей страны. Например, регуляторы могут разъяснить поднадзорным субъектам, что идентификация без личного присутствия может характеризоваться стандартным или даже пониженным риском, если для этого используются системы цифрового профиля, отвечающие стандартам надежности.

14. Следует разработать принципы и критерии, по которым можно было бы оценить процедуры, порядок и условия подтверждения личности. С учетом активного развития технологий цифрового профиля, это позволит стимулировать развитие ответственных инноваций, без необходимости постоянно менять регулирование.

15. Нужно разработать нормативные акты, процедуры надзора и проверок, которые бы позволяли поднадзорным субъектам применять риск-ориентированный подход в

управлении рисками (в том числе, мошенничества и ОД/ФТ), с использованием доступной информации, процессов и технологий.

16. При анализе рисков и возможностей систем цифрового профиля и разработке регулирования, следует консультироваться с широким кругом заинтересованных лиц. Также необходимо оценить уже существующие в стране стандарты систем цифрового профиля и иные технические стандарты, которые разработаны органами по кибербезопасности, защите персональных данных. Согласно Рекомендации 2, для понимания и оценки рисков систем цифрового профиля следует обеспечивать сотрудничество и координацию со всеми уполномоченными органами: это необходимо, в том числе, чтобы синхронизировать требования по ПОД/ФТ и требования по защите персональных данных.

17. Следует рассмотреть возможность усиления взаимодействия с частным сектором – не только с финансовыми организациями, но и с провайдерами услуг цифрового профиля, чтобы лучше понять риски и разработать меры по их минимизации. Одним из механизмов может быть создание регулятивных песочниц, которые бы помогли протестировать использование систем цифрового профиля в контексте местного законодательства по ПОД/ФТ. Следует также стимулировать сотрудничество между участниками рынка – оно поможет выявить потенциальные уязвимости в системах цифрового профиля.

18. Также следует поддержать развитие и внедрение надежных, независимых систем цифрового профиля, проводя их аудит и сертификацию, либо назначая для этих целей специальные экспертные органы[7]. Поддержка таких экспертных органов в тех странах, где этим не занимаются сами регуляторы, необходима для формирования независимой системы сертификации и аудита систем цифрового профиля. Регуляторам рекомендуется гармонизировать требования разных стандартов систем цифрового профиля, чтобы у всех местных акторов было единое понимание того, что такое «независимая, надежная» система цифрового профиля.

19. При разработке национальных систем цифрового профиля, следует применять стандарты оценки надежности таких систем. Регуляторам следует раскрывать информацию о том, как работает их система цифрового профиля и как оценивается надежность ее работы.

20. Следует поддерживать гибкий, риск-ориентированный подход к использованию систем цифрового профиля, чтобы обеспечить повышение доступности финансовых услуг. В некоторых случаях может быть актуальна подготовка руководства об

[7] Такие экспертные сертификационные органы могут предоставлять услуги в рамках конкретной юрисдикции или региона, либо работать на международном уровне.

использовании систем цифрового профиля разного уровня надежности для разных уровней мер по надлежащей проверке клиента.

21. Отслеживать тенденции в развитии систем цифрового профиля, чтобы впоследствии обмениваться лучшими практиками и знаниями, а в будущем – разрабатывать более эффективные и гибкие системы цифрового профиля для использования как внутри страны, так и в международном масштабе.

Рекомендации для регулируемых субъектов

22. Следует понимать базовые компоненты систем цифрового профиля, в том числе, подтверждения личности и аутентификации, и как они соотносятся с элементами надлежащей проверки клиента (см. Раздел 2 и Приложение А)

23. Применять информированный риск-ориентированный подход при использовании систем цифрового профиля, в том числе:

    a. понимать уровень надежности системы цифрового профиля, в особенности подтверждения личности и аутентификации;

    b. убедиться, что этот уровень надежности приемлем для рисков ОД/ФТ, характерных для типа клиента, продукта, юрисдикции, географического охвата и проч.

24. Следует оценить, адекватны ли системы цифрового профиля с более низким уровнем надежности для проведения упрощенных мер по надлежащей проверке клиента, в условиях пониженных рисков.

25. Если в соответствии с внутренними правилами обслуживание клиента без личного присутствия характеризуется повышенным риском, следует изучить возможность переклассификации такого формата обслуживания как стандартного или пониженного риска, если при этом используется независимая, надежная система цифрового профиля и применяются меры по снижению рисков.

26. Где это применимо, стоит использовать меры борьбы с мошенничеством и обеспечения кибер-безопасности и для повышения надежности подтверждения личности, и для текущего мониторинга деловых отношений. Например, можно использовать защитные механизмы в системах цифрового профиля для борьбы с мошенничеством (например, мониторинг аутентификации, попытки использования украденных или скомпрометированных учетных данных).

27. Поднадзорным субъектам следует обеспечить доступ к информации, необходимой для идентификации и верификации физических лиц. Для достижения этой цели следует активно взаимодействовать с регуляторами, законодателями и провайдерами услуг цифрового профиля.

Рекомендации для провайдеров систем цифрового профиля[8]

28. Следует понимать требования законодательства по ПОД/ФТ к надлежащей проверке клиента (в первую очередь, идентификации, верификации и постоянному мониторингу деловых отношений), а также хранению данных.

29. Следует обеспечить аудит и сертификацию системы цифрового профиля со стороны государства, экспертного органа, а если таковых нет, то международного сертификационного органа. Если возможно, участвовать в регулятивных песочницах или схожих механизмах, чтобы оценить уровень надежности системы цифрового профиля.

30. Предоставлять поднадзорным субъектам информацию об уровне надежности системы цифрового профиля для целей идентификации, аутентификации и, если это применимо, федеративности и интероперабельности.

[8] Хотя Стандарты ФАТФ применимы только к субъектам финансового мониторинга (например, к финансовым учреждениям, поставщикам услуг виртуальных активов, установленным нефинансовым предприятиям и профессиям), данное Руководство содержит актуальную справочную информацию для провайдеров систем цифровых профилей, которые предоставляют услуги этим субъектам (для целей исполнения требований ФАТФ). В конечном счете ответственность за выполнение требований ФАТФ несет субъект финансового мониторинга.

РАЗДЕЛ I: ВВЕДЕНИЕ

31. Группа разработки финансовых мер борьбы с отмыванием денег делает все возможное, чтобы глобальные стандарты по ПОД/ФТ стимулировали ответственные инновации. В связи с этим, ФАТФ поддерживает использование новых технологий, которые соответствуют целям по снижению рисков ОД/ФТ и повышению доступности финансовых услуг[9].

32. Активное развитие систем цифрового профиля достигло переломного момента. Стандарты и технологии систем цифрового профиля достигли такого уровня, что вскоре такие системы будут широко доступны. Такие технологии включают в себя: биометрию, почти повсеместное проникновение Интернета и мобильных телефонов (включая активную эволюцию и распространение смартфонов с камерами, микрофонами и другими технологиями); идентификаторы цифровых устройств (например, MAC- и IP-адреса[10], номера мобильных телефонов, сим-карты, геолокация), сканеры высокого разрешения (для сканирования ID-карт, водительских удостоверений, лицензий и иных документов), передача видео высокого разрешения (для удаленной идентификации, верификации и противодействия подлогам изображения), искусственный интеллект и машинное обучение (например, для проверки действительности удостоверений личности), технология распределенного реестра.

Потенциальные преимущества

33. Системы цифрового профиля, которые отвечают технологическим и организационным стандартам, могут повысить надежность, безопасность и удобство идентификации потребителей в разных областях – в финансовом секторе, здравоохранении, государственном управлении. Эти системы мы называем системами, отвечающими стандартам надежности.

34. В контексте стандартов ФАТФ, надежные и независимые системы цифрового профиля могут:

- использоваться для упрощения идентификации и верификации клиента при приеме на обслуживание
- использоваться для текущего мониторинга деловых отношений
- способствовать иным мерам по надлежащей проверке клиента, и

[9] См. позицию ФАТФ по финтеху и регтеху (от 3 ноября 2017 г.), доступно по ссылке www.fatf-gafi.org/publications/fatfgeneral/documents/fatf-position-fintech-regtech.html.
[10] MAC-адреса идентифицируют устройства, IP-адреса идентифицируют Интернет-подключения.

- способствовать мониторингу транзакций для выявления подозрительных операций, в том числе для снижения рисков мошенничества и иных типов риска.

35. Такие системы могут также потенциально снижать затраты поднадзорных субъектов, позволяя им направлять ресурсы на иные функции по ПОД/ФТ.

36. Надежные и независимые[11] системы цифрового профиля также могут способствовать повышению доступности финансовых услуг: у социально уязвимых групп населения будет возможность подтверждать личность, в том числе, удаленно, для получения финансовых услуг. Чем больше людей пользуется услугами регулируемых финансовых организаций, тем эффективнее меры по ПОД/ФТ.

Потенциальные риски

37. Для систем цифрового профиля могут быть характерны и риски ОД/ФТ, которые необходимо понимать и минимизировать. Те организации, которые не смогут этого сделать, автоматически нарушают требования Рекомендации 10 (a), согласно которой необходимо определять, устанавливать и минимизировать риски, связанные с использованием новых технологий[12].

38. Эти риски детально рассмотрены в разделе 4. Крупномасштабные системы цифрового профиля, которые не отвечают требованиям надежности, могут быть подвержены кибератакам, направленным на весь финансовый сектор или саму систему цифрового профиля. Вследствие кражи персональных данных актуальными могут быть риски разглашения персональных данных и мошенничества[13]. Все эти уязвимости могут негативно сказываться и на эффективности мер по ПОД/ФТ. Риски могут быть различны в зависимости от типа системы цифрового профиля, но их последствия по сравнению с более традиционными методами идентификации могут быть более разрушительными из-за масштабов атак. Новые технологии и эффективные процессы идентификации и аутентификации могут минимизировать эти риски. Подробнее о подходах к минимизации – в Разделе 4 и Разделе 5.

39. ФАТФ разработала настоящее Руководство, чтобы указать, как системы цифрового профиля могут использоваться в соответствии с определенными глобальными стандартами по ПОД/ФТ.

Цель и целевая аудитория

[11] Для удобства, термин «надежный» в некоторых случаях используется как синоним «надежности, независимости».
[12] 15 Рекомендация (для финансовых институтов и поставщиков услуг виртуальных активов) и 22 Рекомендация (для установленных нефинансовых предприятий и профессий)
[13] Персональные идентификационные данные - любая информация, которая сама по себе или в сочетании с другой информацией может идентифицировать конкретного человека.

40. Это Руководство должно помочь правительствам и регуляторам понять, как можно использовать системы цифрового профиля для выполнения глобальных требований по ПОД/ФТ. Так, оно адресовано регуляторам, надзорным и проверяющим органам, органам по защите персональных данных и отвечающим за кибрербезопасность, а также государственным органам со смежными мандатами (например, по повышению доступности финансовых услуг).

41. Руководство также адресовано представителям частного сектора, в том числе субъектам финансового мониторинга и провайдерам систем цифрового профиля. Оно также может быть полезно для международных организаций, неправительственных организаций и иных организаций, вовлеченных в оказание услуг с использованием систем цифровых профилей и предоставления технического содействия.

Сфера руководства

42. Это Руководство сфокусировано на применении требований 10 Рекомендации – идентификации и верификации клиентов при приеме клиентов на обслуживание с использованием систем цифрового профиля. Также рассматривается возможность использования систем цифрового профиля для текущей надлежащей проверки клиента (в том числе, мониторинга операций). В Руководстве описано применение Рекомендации 17 (Доверие к мерам третьих сторон) к ситуациям, когда один субъект финансового мониторинга предоставляет доступ к системе цифрового профиля другому аналогичному субъекту.

43. Согласно принципу технологической нейтральности, требования Рекомендации 11 по хранению информации не зависят от того, хранятся сведения в физической или электронной форме. Однако, при использовании систем цифрового профиля необходимо обратить внимание на некоторые технические особенности хранения данных и обеспечения доступа к ним. Подходы к хранению информации в системах цифровых профилей будет зависеть от технических и организационных решений, а также требований законодательства и договорных отношений. Например, если система цифрового профиля управляется государством, у государственных органов по определению будет доступ ко всей содержащейся в ней информации. Если система цифровых профилей предоставляется негосударственной компанией, информация, которая в ней содержится, будет храниться частной организацией. Также некоторая часть информации может получаться или верифицироваться напрямую из цифрового источника (например, государственной или частной базы данных). В этом случае условия хранения и доступа к данным, наличие меток времени и источника может соответствовать Рекомендации 11. Все эти вопросы адекватно описаны в законодательстве по ПОД/ФТ и цифровым профилям, а частные организации урегулировали эти вопросы в своих договорных отношениях.

В связи с этим, требования к хранению данных в этом Руководстве не рассматриваются.

44. В этом Руководстве основной акцент делается на идентификации физических лиц. Руководство не рассматривает использование систем цифрового профиля для идентификации и верификации личности представителей юридических лиц, а также выполнения иных элементов процесса надлежащей проверки клиента – например, выявления бенефициарных владельцев (Рекомендации 10 (b)), понимания целей и природы деловых отношений (Рекомендация 10(c)), хотя надежные и независимые системы цифровых профилей для целей выполнения этих требований и важны.

45. В Руководстве рассматриваются государственные (или действующие от имени государства[14]) и негосударственные системы цифрового профиля. Среди государственных систем описываются, в первую очередь, универсальные – то есть те, которые могут использоваться для любых целей; также приводятся примеры специальных систем цифрового профиля – например, базы данных о социальном страховании или иные, которые могут использоваться субъектами финансового мониторинга и провайдерами систем цифрового профиля. В Разделе 2 приводится более подробная информация о классификации систем цифрового профиля.

46. Руководство не устанавливает стандарты оценки качества, независимости или надежности систем цифрового профиля, их технологий, процедур и архитектуры. Вместо этого документ опирается на стандарты, которые разработаны или находятся в разработке иных организаций и в разных юрисдикциях. В Разделе 2 приводится описание технических стандартов, в Разделе 5 и приложении E – дополнительная информация.

47. Руководство включает пять приложений и глоссарий:

- *Приложение A*: Описание базовой системы цифрового профиля и ее участников: более детальное описание концепций, указанных в Разделе 5.
- *Приложение B*: Примеры – описываются примеры использования систем цифрового профиля в разных юрисдикциях, в том числе, для надлежащей проверки клиента и обеспечения доступа к финансовым услугам.
- *Приложение C*: Принципы идентификации для устойчивого развития – описывает проблематику менеджмента, защиты персональных данных и

[14] Система цифрового профиля предоставляется «от имени государства», когда правительство по договору или иным другим способом привлекает UNCHR, иную организацию для обслуживания этой системы. В таком случае функции по подтверждению личности выполняет негосударственная организация.

операционного управления, с которой сталкиваются юрисдикции и организации[15].

- *Приложение D*: Стандарты оценки систем цифрового профиля и организации, разрабатывающие технические стандарты – перечень организаций, которые разрабатывают технические стандарты (за исключением национальных и региональных организаций), которые подготовили стандарты оценки систем цифрового профиля.
- *Приложение E*: Обзор стандартов оценки систем цифрового профиля в ЕС и США – в качестве примера приводятся региональные стандарты оценки систем цифрового профиля в ЕС и США.
- *Глоссарий* – описание терминологии, связанной с системой цифрового профиля и используемой в Руководстве.

[15] Данные принципы были разработаны и коллективно одобрены 25 партнерами, международными организациями, неправительстенными организациями, ассоциациями частного сектора и государственными структурами.

РАЗДЕЛ II: ТЕРМИНОЛОГИЯ В СИСТЕМАХ ЦИФРОВОГО ПРОФИЛЯ И ИХ КЛЮЧЕВЫЕ ОСОБЕННОСТИ

Что мы понимаем под термином «личность»?

Концепция официальной личности

48. Личность – сложная концепция с множеством разных значений. Для целей ФАТФ, в контексте Рекомендации 10(a), т.е. «идентификации клиента и проверки личности клиента», под «личностью» понимается официальная идентичность, которая отличается от личной или социальной идентичности, актуальной для неофициальных целей (например, нерегулируемого коммерческого, социального взаимодействия в интернете или личном присутствии). Руководство рассматривает только использование систем цифрового профиля для подтверждения «официальной личности» в целях получения финансовых услуг.

49. Для целей настоящего Руководства[16], **официальная личность** – это характеристика личности, которая:

a. основана на чертах личности (характеристиках или признаках), которые определяют уникальность человека в целом или в конкретном контексте; и

b. признается государством для регуляторных и иных официальных целей.

Подтверждение личности

50. **Подтверждение личности** обычно опирается на предоставленный государством регистрационный документ или сертификат (например, свидетельство о рождении, идентификационная карта, учетные данные в системе цифрового профиля), в котором содержатся ключевые атрибуты человека (например, имя, дата и место рождения).

51. Критерии для подтверждения личности могут варьироваться в зависимости от юрисдикции. Установление необходимых атрибутов личности и процедур ее подтверждения – суверенное право государства. Со временем эти требования могут меняться, под влиянием технологических и культурных тенденций. При установлении критериев для подтверждения личности, государства могут использовать фиксированный подход, основанный на правилах, либо подход, который основан на принципах и устанавливает только требования к конечным результатам, а не процессу его достижения. Второе решение более гибкое. С учетом быстрого развития технологий и стандартов цифрового профиля, он позволяет

[16] Использование ФАТФ этого определения для целей настоящего Руководства не заменяет определения, которые используются иными международными организациями, устанавливающими глобальные стандарты.

регуляторам стимулировать инновации и, установив требования однажды, не менять их впоследствии.

52. Государства-члены ЕС используют общие стандарты надежности с учетом национальных требований, таких как использование различных национальных процедур и документов, удостоверяющих личность, при условии, что результат соответствует требованиям eIDAS. В зависимости от контекста, в котором необходимо проверить те или иные данные, могут использоваться различные источники, такие как, например, соответствующие реестры, документы и данные различных органов. В рамках ЕС, авторитетные источники могут варьироваться от страны к стране даже в схожих ситуациях, но структура eIDAS их гармонизирует и способствует признанию каждой стороной. Международная организация по стандартизации (ИСО)[17] в настоящее время разрабатывает глобальные стандарты идентификации физических лиц для получения финансовых услуг, в том числе в цифровом контексте.

53. Во многих странах подтвердить личность можно с помощью систем подтверждения личности **общего назначения**: например, национальных ID-систем или систем регистрации актов гражданского состояния. Такие системы обычно по умолчанию используются для проверки личности государственными органами и частными компаниями. Однако они есть не во всех странах.

54. В странах также обычно есть **неуниверсальные** системы подтверждения личности (также называемые «функциональными»), которые используются в ограниченных целях: например, для получения государственных пособий, сдачи налоговой отчетности, голосования, подтверждения права водить автомобиль, а в некоторых государствах – и для получения финансовых услуг. Примеры таких систем – налоговые идентификаторы, водительские права, карточки избирателей, номера социального страхования, документы беженцев. В некоторых юрисдикциях они могут использоваться и для официального подтверждения личности, особенно в странах без универсальных систем.

55. Обычно инструмент подтверждения личности предоставляется государством или от его имени. Но сейчас такие инструменты предоставляются частными компаниями или в сотрудничестве с частным сектором, и признаются государством для онлайн подтверждения личности (например, NemID в Дании), так же, как и те, что предоставлены государством.

56. Беженцам удостоверение личности может предоставляться международно признанной организацией с соответствующим мандатом[18]. См. Box 18

[17] Консультативная группа технического комитета 68 по стандартам ИСО (SAG), рабочая группа 7.
[18] См. Конвенцию о статусе беженцев 1951 года, статьи 25 и 27 и Статут Управления Верховного комиссара Организации Объединенных Наций по делам беженцев 1950 года.

Что мы понимаем под системой цифрового профиля?

57. Системы цифрового профиля используются для подтверждения личности онлайн и офлайн, с разной степенью надежности.

58. В этом Руководстве рассматриваются системы цифрового профиля полного цикла, включающие процесс регистрации и аутентификации. Такие системы могут быть очень разными и задействуют разные организации и технологии. В этом Руководстве мы используем комплексное определение цифрового профиля.

59. Не все элементы систем цифрового профиля обязательно являются цифровыми. Некоторые элементы подтверждения личности или регистрации могут осуществляться в цифровой или нецифровой форме, но **привязка профиля к конкретному лицу, аутентификация, делегирование – должны быть цифровыми.** Эти понятия подробнее рассмотрены в следующем разделе.

60. Цифровые технологии могут использоваться в системах цифрового профиля по-разному, например:

    - В форме электронных баз данных, в том числе на базе распределенных реестров, для получения, подтверждения и хранения данных;
    - В форме учетных данных для подтверждения личности при доступе к электронным и автономным приложениям;
    - В форме биометрических данных для идентификации и аутентификации физлиц;
    - Как набор API, платформ и протоколов для идентификации, верификации и подтверждения личности в онлайне.

Ключевые компоненты систем цифрового профиля

61. Как указано в стандартах NIST по цифровому профилю, **такие системы** имеют два обязательных и один необязательный элемент. За каждый из этих элементов могут отвечать государственные или негосударственные организации. В разных странах и учреждениях эти элементы могут называться по-разному. Подробное описание каждого из них приведено в ***Приложении А: описание базовой системы цифрового профиля и ее участников***

Первый обязательный компонент - проверка личности и регистрация

62. Этот компонент отвечает на вопрос: ***Кто вы?*** Он включает в себя сбор и проверку информации о человеке; создание учетной записи (регистрация) и предоставление лицу аутентификаторов для доступа к этой учетной записи.

63. Этот компонент имеет непосредственное отношение к требованию идентификации/проверки Рекомендации 10(а) (см. Раздел III).

Рис. 2. Идентификация и регистрация

Примечание. Данный рисунок лишь иллюстрирует процесс идентификации и регистрации клиента, представленные шаги могут быть реализованы в произвольном порядке. Главная цель – это идентифицировать и верифицировать лицо и связать его с идентификационной информацией. Подробнее см. в Приложении А.

64. Проверка личности и регистрация могут проводиться следующими способами:

- Сбор: лицо предоставляет данные о себе лично или онлайн (например, заполнив онлайн-форму, отправив селфи-фотографию, загрузив фотографии паспорта или водительских прав и т.д.).
- Проверка: цифровая или физическая проверка подлинности документа и точности указанных в нем данных (например, проверка защитных элементов, сроков действия и проверка данных через сторонние источники).

- Контроль дубликатов: нужно убедиться, что лицо с такими же данными не регистрировалось в системе ранее (например, с помощью поиска дубликатов записей, биометрии и/или специальных алгоритмов).
- Верификация: необходимо убедиться, что данные действительно принадлежат конкретному лицу (например, с помощью распознавания лица и противодействия подмене изображения).
- Регистрация учетной записи и выдача учетных данных: создание учетной записи и предоставление средств доступа к ней (например, в форме паролей, генератор одноразовых кодов (OTC) на смартфоне, смарт-карт PKI19[19], сертификатов FIDO и т.д.). Этот процесс включает и аутентификацию (см. ниже).

Второй компонент: аутентификация и управление цифровым профилем

65. Аутентификация отвечает на вопрос: ***является ли человек владельцем учетной записи?*** Подтверждается это с помощью ранее выданных аутентификаторов.

66. Существует три типа факторов, которые могут быть использованы для аутентификации (см. Рис.3 ниже): (1) владение (что-то, чем вы владеете, например, криптографические ключи); (2) знание (что-то, что вы знаете, например, пароль); (3) свойства субъекта (например, биометрия).[20]

67. Аутентификация может проводиться по-разному и на основе разных типов факторов. Эти факторы имеют различные уровни безопасности – более подробно риски аутентификации рассмотрены в разделе V. Использование одного фактора обычно не считается надежным, поэтому используется несколько одновременно.[21]

[19] Инфраструктура открытых ключей (PKI)

[20] Описанные в Руководстве компоненты аутентификации не являются аналогом "усиленной аутентификации клиента (SCA)", как она описывает в законодательстве ЕС. Является ли аутентификация усиленной (согласно Директиве (ЕС) 2015/2366, PSDII) или нет, следует оценивать по критериям, указанным в PSDII и Технических стандартах по надежной аутентификации клиентов и безопасной связи в соответствии с PSDII (RTS on SCA & CSC), а не по Руководству ФАТФ.

[21] По мере развития цифровых профилей данный вопрос становится все более сложным. Аутентификация клиента может осуществляться не одномоментно, а в течение протяженного периода времени: в таком случае ее эффективность и надежность зависит не от того, сколько используется аутентификационных факторов, а общего качества оценки разноплановых динамических данных: каким образом клиент входит в систему, из какой локации, насколько часто и с какой целью, какие использует IP-адреса, какие поведенческие и биомеханические паттерны для него актуальны.

Рис. 3. Факторы аутентификации

Источник: World Bank ID4D

Вох 1. Роль аутентификации в обеспечении надлежащей проверки клиента и других мер ПОД / ФТ

- После того как человек прошел проверку личности и зарегистрировался в системе цифрового профиля, он может использовать учетные данные и аутентификаторы, привязанные к его аккаунту, чтобы “подтвердить” свою личность третьей стороне (например, регулируемому субъекту). У аутентификации есть особая цель: в отличие от проверки личности, когда проверяют корректность персональных данных, аутентификация нужна, чтобы подтвердить, что лицо действительно является тем, за кого он/она себя выдает. Поэтому способность системы цифрового профиля защититься от мошенников и самозванцев является ее важной характеристикой.
- "Аутентификация" существующих клиентов также является важной мерой безопасности. В принципе, те же аутентификационные данные, которые использовались при открытии счета, могут использоваться и при получении доступа к нему. Хотя так бывает не всегда. Например, финансовые организации могут выдавать собственные аутентификаторы (пин-коды, токены) и(или) привязывать их к мобильным телефонам или браузерам (согласно стандартам FIDO).

68. ***Управление жизненным циклом цифрового профиля*** – это набор действий, в случае снижения безопасности или надежности ***аутентификаторов***: например, в результате потери, кражи, неавторизованного дублирования, истечения срока действия или отзыва.

Третий (опциональный) компонент: механизмы переносимости и интероперабельности

69. Цифровые профили могут быть переносимыми. То есть аутентификаторы, предоставленные клиенту, можно использовать для подтверждения личности в сторонних государственных и частных организациях; при этом собирать каждый отдельно и верифицировать данные не нужно. Переносимость может быть реализована с использованием разных протоколов и подходов. Например, в Европе Регламент eIDAS предусматривает трансграничное признание систем цифрового профиля.

70. Переносимость цифрового профиля можно обеспечить путем использования единой архитектуры и протоколов обмена данными между разными информационными системами, то есть интероперабельности. Британский сервис GOV.UK Verify – пример переносимого цифрового профиля - см. Box 16

Технические стандарты систем цифрового профиля и способы их оценки

71. Технические стандарты и методы оценки технологий, процессов и архитектуры систем цифрового профиля разрабатываются:

- на национальном и наднациональном уровнях (например, в Европейском Союзе, Канаде и Австралии);
- международными организациями по стандартизации или такими отраслевыми организациями, как Международная организация по стандартизации (ИСО), Международная Электротехническая комиссия (МЭК), Альянс Fast Identity Online (FIDO), Фонд OpenID Foundation (OIDF), Международный союз телекоммуникаций (ITU) и GSMA.

72. В ***Приложении D*** приведены организации, разрабатывающие такие стандарты и методы оценки.

73. Разные методы оценки, которые разрабатываются в отдельных юрисдикциях, различаются по числу уровней, но очень близки по содержанию. Технические стандарты систем цифрового профиля разрабатываются с оглядкой на существующие аналоги, поэтому их содержание сближается. В 2018 году ISO совместно с Международной электротехнической комиссией выпустила международный стандарт проверки личности и регистрации физических лиц

(ISO/IEC 29003:2018). В настоящее время ISO пересматривает системы качества аутентификации (ISO/IEC 29115:2013) и рассматривает возможность включения вопросов цифрового профиля в принципы управления рисками (ISO 3100:2018). Кроме того, ISO работает над обновлением, согласованием и синхронизацией всех других стандартов ISO для создания всеобъемлющих международных стандартов надежности систем цифрового профиля.

74. Это Руководство преимущественно ссылается на Руководство по цифровым профилям NIST и европейский Регламент eIDAS. Для определения релевантных стандартов субъектам финансового мониторинга необходимо работать с ведомствами, ответственными за кибербезопасность и цифровые профили.

75. Технология цифровых профилей развивается довольно быстро, поэтому технические стандарты и методы оценки могут от нее отставать. Эти стандарты стоит использовать как полезные инструменты, но не стоит забывать, что максимальный уровень надежности, который в них предусмотрен – это не предел: если есть технологии, которые позволяют их превзойти, необходимо применять их.

РАЗДЕЛ III: СТАНДАРТЫ ФАТФ ПО НАДЛЕЖАЩЕЙ ПРОВЕРКЕ КЛИЕНТА

76. Этот раздел требует базового понимания того, как работают цифровые профили. Читателям рекомендуется ознакомиться с кратким описанием основных этапов разработки универсальных систем цифровых профилей в разделе II и Приложении A. Это описание предваряет содержание этого раздела – как соотносятся 10 Рекомендация (в первую очередь, критерии «надежности и независимости») и системы цифровых профилей.

77. Согласно 10 Рекомендации, финансовые организации должны быть обязаны проводить надлежащую проверку клиентов. Ниже разъясняется применение Рекомендации 10 (a) в контексте систем цифровых профилей. Степень применения мер надлежащей проверки будет зависеть от уровня риска, и определяется самим субъектом финансового мониторинга. В этом разделе также описывается, как системы цифрового профиля могут использоваться для выполнения иных требований Рекомендации 10(d).

Требования к идентификации/верификации клиентов (при принятии на обслуживание)

78. Регулируемые субъекты при установлении деловых отношений с клиентом обязаны идентифицировать клиента и удостоверить его личность, *используя надежные, независимые исходные документы, данные или информацию* (Рекомендация 10, пункт a).

Цифровые и аналоговые документы

79. 10 Рекомендация является технологически нейтральной. Согласно Рекомендации 10 (a), финансовые учреждения могут использовать “документы”, а также “информацию или данные” при проведении идентификации и проверке клиентов. Рекомендация 10 (a) не указывает цифровыми или аналоговыми они должны быть.

80. Хотя Рекомендация 10(a) требует, чтобы финансовые организации «надежно» устанавливали принадлежность данных конкретному лицу, она не устанавливает для этого каких-то конкретных процедур и не препятствует использованию систем цифровых профилей. Конкретные решения по этому поводу принимает каждая страна.

“Надежное, независимое” удостоверение личности

81. Чтобы оценить, как цифровые профили можно использовать для идентификации и верификации, сперва надо понять, что в контексте цифровых технологий понимается под «надежными, независимыми, первичными документами, данными и

информацией». «Надежность и независимость» можно определить по уровню надежности системы, которая оценивается на основе технических стандартов.

82. Чтобы понять, зачем в требованиях ФАТФ содержатся требования по «надежности и независимости», нужно взглянуть на их эволюцию.

83. В первой редакции Рекомендаций ФАТФ от 1990 года финансовым организациям предписывалось идентифицировать клиентов с использованием «официальных или иных надежных документов»[22]. Впоследствии эта формулировка не менялась при пересмотре Рекомендаций в 1996 и 2003 годах. В 2012 ФАТФ ввела дополнительное требование по «верификации личности», при этом информация и документы должны быть не только «надежными», но и независимыми. В рамках пересмотра 2012 года ФАТФ также перешла к более гибкому подходу, который предусматривал использование не только документов, но и данных и информации. В то же время отсылка к «официальным документам» была из текста удалена.

84. В контексте цифровых профилей «надежность и независимость» означает лишь то, что система цифрового профиля должна обеспечивать качественное подтверждение личности. Иными словами, в нее встроены механизмы минимизации рисков, указанных в разделе IV.

Риск-ориентированный подход к процедуре надлежащей проверки клиентов

85. Согласно 10 Рекомендации, охват мер по надлежащей проверке клиентов должен определяться в зависимости от уровня рисков. Эта Рекомендация и пояснительная записка к ней требуют оценить и минимизировать риски ОД/ФТ (в разрезе клиентов, стран, регионов, продуктов, услуг, операций и механизмов оказания услуг). В случаях повышенного риска следует применять усиленные меры по надлежащей проверке, а в случаях пониженного риска – можно использовать упрощенные. ФАТФ опубликовала руководство о применении риск-ориентированного подхода в целях повышения доступности финансовых услуг[23].

86. Как указано в разделе V, Рекомендации 1 и 10, а также пояснительные записки к ним, требуют применения мер, которые соответствуют уровням риска ОД/ФТ. Согласно

---

[22] Первоначально 40 Рекомендаций ФАТФ от июля 1990 года устанавливали требования к идентификации клиентов финансовых учреждений в целях усиления их роли в борьбе с отмыванием доходов от незаконного оборота наркотиков. 12 Рекомендация (1990 г.) цитируется в соответствующей части (добавлен курсив, пунктуация сохранена): *[Ф]инансовые учреждения* не должны вести анонимные счета или счета, открытые на явно вымышленные имена: необходимо разработать соответствующие законы, нормативные акты, заключить соглашения между надзорными органами и финансовыми учреждениями или соглашения о саморегулировании финансовых учреждений, которые *обяжут их идентифицировать клиента на основании официального или иного достоверного документа, удостоверяющего личность,* и регистрировать всех своих клиентов *при установлении деловых отношений или совершении операций (в частности, при открытии счетов или сберегательных книжек, заключении фидуциарных сделок, аренде сейфовых ячеек, совершении крупных кассовых операций).*

[23] ФАТФ (2013-2017), О мерах противодействия отмыванию денег и финансированию терроризма и обеспечению доступности финансовых услуг – С дополнением о надлежащей проверке клиента, ФАТФ, Париж www.fatfgafi.org/media/fatf/content/images/Updated-2017-FATF-2013-Guidance.pdf

Пояснительной записке к Рекомендации 1, субъекты финансового мониторинга должны принимать во внимание все факторы риска. В свою очередь Рекомендация 10, пояснительная записка к ней и пояснительная записка к Рекомендации 1 предусматривают, что дифференцированы могут быть и отдельные элементы надлежащей проверки клиента (например, для принятия клиента на обслуживание принимаются стандартные меры, а для текущего мониторинга деловых отношений – усиленные).

Деловые отношения без личного присутствия

87. ФАТФ разделяет способы ведения деловых отношений на «личные» и «**удаленные**». Под «личными» понимается взаимодействие при личном присутствии сторон, все из которых находятся в одном и том же месте и физически взаимодействуют. **«Удаленное» взаимодействие**, напротив, предполагает, что географически стороны находятся в разных местах и физически не контактируют[24].

88. В Пояснительной записке к Рекомендации 10 «деловые отношения без личного присутствия» в контексте надлежащей проверки клиента приведены как *пример потенциального* высокого риска. Тем временем, это не означает, что регуляторы и субъекты финансового мониторинга должны автоматически рассматривать эти ситуации как высокорискованные. В Рекомендациях ФАТФ они описаны всего лишь как *пример*.

89. Поскольку технологии, архитектура и стандарты систем цифрового профиля постоянно развиваются, при их надлежащем применении удаленная идентификация клиента может характеризоваться стандартным уровнем риска, а при использовании особенно надежных систем и дополнительных мер снижения рисков (например, ограничения функциональности или иных, которые описываются в Руководстве ФАТФ по финансовой доступности и Пояснительной записке к Рекомендации 10) – даже пониженным уровнем риска (см. также раздел "Особые вопросы, связанные с доступностью финуслуг, удаленной проверкой подлинности личности и регистрацией" далее в этом Руководстве).

Текущая надлежащая проверка деловых отношений

90. В соответствии с Рекомендацией 10 (d), регулируемые субъекты должны проводить «на постоянной основе надлежащую проверку деловых отношений и тщательный анализ сделок, совершенных в рамках таких отношений для того, чтобы убедиться в соответствии проводимых сделок сведениям о клиенте, его хозяйственной деятельности и характере рисков, в том числе, когда необходимо, об источнике средств».

[24] Определение взаимодействия в личном присутствии или без личного присутствия может варьироваться в разных странах. Например, в некоторых юрисдикциях видеоидентификация рассматривается как личное взаимодействие.

91. Как мы описывали в Разделе II и более подробно поясняем в Приложении А, **аутентификация** в системах цифрового профиля подтверждает, что человек действительно то лицо, которое ранее прошло процедуру регистрации. Поднадзорным субъектам, которые используют системы цифрового профиля для аутентификации уже имеющихся клиентов, рекомендуется использовать эти данные[25] для текущей надлежащей проверки клиента и мониторинга транзакций. Обычно эта информация используется для противодействия мошенничеству. Однако, благодаря использованию систем цифрового профиля, она может быть актуальна и для целей ПОД/ФТ.

92. Поднадзорные субъекты проводят аутентификацию своих клиентов, чтобы убедиться, что это действительно то лицо, которое прошло «надежную и независимую» идентификацию при заключении договора. Аутентификация подтверждает, что операции совершает конкретный человек. И, с этой точки зрения, она может повысить эффективность текущей надлежащей проверки клиента и мониторинга транзакций согласно Рекомендации 10(d).

Требования к доверию мерам третьих сторон

93. В этом разделе мы рассматриваем, как субъект финансового мониторинга может полагаться на идентификацию, проведенную третьим лицом в контексте использования цифровых профилей, (согласно Рекомендации 17) и выступать в качестве агента (в рамках аутсорсинга) иного субъекта финансового мониторинга (за рамками Рекомендации 17).

94. В соответствии с Рекомендацией 17 страны могут позволить компаниям[26] доверять мерам третьих сторон при идентификации/верификации клиентов[27] при условии соблюдения следующих условий:

- Третья сторона также должна быть субъектом регулирования, подпадающей под требования 10 Рекомендации по надлежащей проверке клиентов, а также находиться под адекватным надзором.
- Субъекты финансового мониторинга должны:
    - Немедленно получать необходимую информацию, касающуюся идентификации/верификации клиента;
    - Принять соответствующие меры, чтобы иметь возможность по запросу немедленно получить от третьей стороны копии

[25] Аутентификация-это один из элементов процесса предоставления доступа к счету. Для принятия решения о предоставлении доступа финансовое учреждение может также собирать дополнительные данные (например, геолокацию, IP-адреса и т. д.).
[26] 22 Рекомендация предусматривает, что требования 17 Рекомендации распространяются также на УНФПП.
[27] Согласно 17 Рекомендации, финансовые учреждения могут полагаться на меры третьих сторон для реализации элементов (a)-(c) мер по надлежащей проверке клиентов, зафиксированных в 10 Рекомендации, но не для текущего мониторинга деловых отношений. В настоящем Руководстве 17 Рекомендация рассматривается только в контексте «идентификации/верификации» согласно Рекомендации 10 (a).

идентификационных данных и другой соответствующей документации, относящейся к требованиям Рекомендации 10 (a);

- Удостовериться в том, что третья сторона регулируется и находится под надзором; соблюдает требования надлежащей проверки клиента и хранит информацию в соответствии с 10 и 11 Рекомендациями; и
- Учитывать риски, связанные со страной происхождения/нахождения третьей стороны.

95. Когда разрешается доверять третьей стороне, окончательная ответственность всегда остается за субъектом, который полагается на третью сторону.

Доверие к мерам третьих сторон в контексте использования цифрового профиля (когда регулируемые субъекты также являются провайдерами услуг цифрового профиля)

96. Если согласно местному регулированию субъект финансового мониторинга может полагаться на третью сторону, использующую для идентификации клиентов систему цифрового профиля, он должен обеспечить соблюдение следующих правил:

- Необходимо немедленно получать требуемую информацию, касающуюся личности клиента (включая сведения о надежности данных). Например, клиент с использованием системы цифрового профиля может подтвердить свою личность и поручить передать организации свои идентификационные данные, необходимые для заключения договора (к примеру, имя, дату рождения, идентификационный номер и прочее).
- Необходимо убедиться, что по запросу третья сторона предоставит информацию о клиенте (документы, данные, согласно Рекомендации 10(a)) или незамедлительно обеспечит к ней доступ. Например, можно убедиться, что при регистрации клиентов третья сторона фиксирует всю необходимую информацию и что методы аутентификации, которые она использует, позволяют без задержки по запросу получить эти данные.

Субъекты финансового мониторинга как провайдеры услуг цифрового профиля, за рамками действия Рекомендации 17

97. Субъекты финансового мониторинга, которые разработали собственные системы цифрового профиля могут выступать в качестве агентов для других регулируемых субъектов. Если это разрешено законодательствами, то эта модель будет оформляться как аутсорсинг при идентификации/верификации клиента. В этой ситуации требования к полаганию на третьи стороны согласно Рекомендации 17 не применяются, поскольку она затрагивает аутсорсинг и агентские отношения.

98. Как и другие поставщики услуг цифрового профиля, регулируемые организации, действующие в этом качестве, будут использовать свою систему цифрового профиля для проведения идентификации/верификации (и аутентификации) клиентов *от имени* делегирующей организации. Кроме того, как и другие поставщики услуг цифрового профиля, такие организации могут обратиться за сертификацией в соответствующие государственные органы или надежную частную организацию.

99. В любом случае, принципал по-прежнему несет ответственность за проведение *эффективной* идентификации/верификации и аутентификации клиентов с использованием системы цифрового профиля, и должен будет применять риск-ориентированный подход как описано в Разделе V.

РАЗДЕЛ IV: ПРЕИМУЩЕСТВА И РИСКИ СИСТЕМ ЦИФРОВЫХ ПРОФИЛЕЙ ПРИ СОБЛЮДЕНИИ ТРЕБОВАНИЙ ПОД/ФТ И СМЕЖНЫЕ ВОПРОСЫ

100. В этом разделе описываются некоторые потенциальные преимущества систем цифровых профилей для организаций, их клиентов и регуляторов, а также потенциальные риски, которые необходимо выявлять, понимать, контролировать, а также адекватно ими управлять и, при необходимости, применять меры по их смягчению. Эти преимущества и риски связаны как с обеспечением требований ПОД/ФТ, так и с расширением доступа к финансовым услугам.

101. Цель данного раздела - повысить осведомленность заинтересованных сторон о потенциальных рисках, характерных для технологий цифрового профиля, для их предотвращения с учетом риск-ориентированного подхода. Описание рисков не имеет своей целью препятствовать использованию надежных, независимых систем цифровых профилей, т. е. тех, которые отвечают соответствующим уровням надежности. Упоминание этих рисков также не означают, что системы цифровых профилей обязательно более уязвимы для злоупотреблений, чем традиционные методы идентификации/верификации.

102. В этом разделе также освещается ряд более значительных рисков, связанных с цифровыми профилями. Снижение этих рисков обычно не входит в прямую компетенцию органов по борьбе с ОД/ФТ, но они могут оказывать косвенное влияние на применяемые меры по ПОД/ФТ.

103. Хотя в этом разделе дается общий обзор некоторых рисков и проблем, провести их оценку можно на основе соответствующих стандартов. Юрисдикциям рекомендуется руководствоваться этими стандартами.

Потенциальные преимущества систем цифровых профилей

Меры по надлежащей проверке клиентов

104. Системы цифрового профиля используются в интересах клиентов, компаний и финансового сектора в целом. Потенциально, при предоставлении физлицам финуслуг такие системы могут иметь более высокий уровень надежности, безопасности, удобства, эффективности и конфиденциальности. Как обсуждается ниже, надежные, независимые системы цифрового профиля могут значительно улучшить процесс идентификации/верификации клиентов при принятии на обслуживание и аутентификации личности клиентов при авторизации. Кроме того, точная идентификация клиентов может повысить эффективность надлежащей проверки деловых отношений и мониторинга транзакций.

Минимизация ошибок, связанных с человеческим фактором

105. Традиционные методы проведения идентификации/верификации клиентов с использованием документов подразумевают контроль со стороны сотрудника. Например, сотрудник банка при открытии счета должен сравнить фотографии на официальном документе, удостоверяющем личность, с лицом, предъявляющим этот документ, а также принять решение о том, что предъявленный документ является подлинным. У персонала могут отсутствовать инструменты, технологии, подготовка, навыки и опыт, необходимые для выявления поддельных, измененных или украденных документов.

106. Использование надежных, независимых систем цифровых профилей потенциально может снизить вероятность человеческой ошибки при идентификации и проверке личности человека.

- Во-первых, даже в тех случаях, когда используется система цифрового профиля, в которой первичная регистрация осуществляется при личной явке[28], в большинстве случаев, сотрудник, проводящий регистрацию, будет иметь доступ к техническим средствам, которые позволят более эффективно обнаруживать поддельные и украденные идентификационные документы. Например, используются сложные и эффективные технологии, позволяющие выявить поддельные документы или получить надежные данные для удостоверения личности[29] (по крайней мере, если система соответствует стандартам надежности).

- Во-вторых, если процедуру аутентификации, т.е. определения того, что клиент является тем, за кого он себя выдает, проводит сотрудник, возникает риск субъективной ошибки, человеческого фактора, а при проведении этой процедуры системой цифрового профиля такой риск сводится к минимуму. Системы цифрового профиля с многофакторной аутентификацией с высокой степенью точности могут определить, что клиент, который хочет открыть счет или получить доступ к нему, фактически является тем лицом, которому первоначально были выданы идентификационные учетные данные.

Повышение качества и снижение стоимости обслуживания клиентов

107. Надежные, независимые системы цифровых профилей также могут улучшить пользовательский опыт, как во время заключения договора, так и при дальнейшем

[28] Как указано в разделе II и Приложении A, в рамках системы цифрового профиля проверка личности является одним из компонентов, который может осуществляться как удаленно, так и при личном присутствии.

[29] В настоящее время проверить некоторые элементы защиты документов, удостоверяющих личность (например, защитные элементы, видимые в ультрафиолете, специальная прошивка, перфорация) удаленно затруднительно или вовсе невозможно, но большинство документов, удостоверяющих личность, имеют защитные элементы, которые можно проверить и без личного присутствия.

взаимодействии с финансовой организацией. Удобство потребителей напрямую влияет на их лояльность и долю доведенных до конца регистраций. Повышение эффективности и простота процедур должны снизить затраты на установление деловых отношений с клиентами. Одно из исследований подтверждает, что использование системы цифрового профиля может снизить такие затраты на 90% и при этом сократить процедуру идентификации/верификации с нескольких дней или недель до считанных минут[30]. Такая экономия позволит направить высвободившиеся ресурсы на другие комплаенс-функции и способствовать повышению доступности финансовых услуг.

Мониторинг транзакций

108. Как указывалось выше, надежная аутентификация клиентов, которые уже находятся на обслуживании, позволяет более эффективно выявлять подозрительные транзакции и сообщать о них регулятору. Кроме того, в зависимости от операционной модели и таких факторов как наличие согласия пользователя и требования законов о защите персональных данных, с помощью цифрового профиля могут быть получены дополнительные данные о клиенте: геолокация, IP-адрес, сведения об устройстве. Такая информация может дать организациям более глубокое представление о поведении клиента, в дальнейшем это будет способствовать более качественному выявлению несвойственных для клиента, а, следовательно, подозрительных, операций, помогать правоохранительным органам в расследовании преступлений. Например, с помощью дополнительных данных, полученных организациями по различным каналам (включая интернет и мобильный телефон) в соответствии с местным законодательством, можно определить, кто контролирует счет; контролирует ли он несколько счетов; а также круг физических и юридических лиц, участвующих в финансовых операциях, проводимых с использованием этих счетов.

Доступность финансовых услуг

109. Стремительная цифровизация финансовых услуг повысила значимость надежных, независимых систем цифровых профилей для целей расширения доступа к финансовым услугам, особенно в развивающихся странах[31], где они стали основными драйверами финансовой доступности.[32] Разработка гибких стандартов, которые направлены на оценку результатов, а не процедур идентификации,

---

[30] McKinsey Global Institute (2019), Digital Identification, https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20identification%20A%20key%20to%20inclusive%20growth/MGI-Digital-identification-Report.ashx

[31] 26% людей, не имеющих доступа к финансовым сервисам и проживающих в странах с низким уровнем дохода, назвали отсутствие официальных документов, удостоверяющих личность, главным препятствием для получения финансовых услуг (по данным исследования Всемирного банка о глобальном состоянии финансовой доступности «Global Findex» 2017 года»).

[32] ФАТФ (2013-2017), О мерах противодействия отмыванию денег и финансированию терроризма и обеспечению доступности финансовых услуг - С дополнением о надлежащей проверке клиента, ФАТФ, Париж www.fatfgafi.org/publications/financialinclusion/documents/financial-inclusion-cdd-2017.html.

позволяет гражданам, у которых нет документов, удостоверяющих личность, зарегистрировать цифровой профиль по упрощенной процедуре (с менее строгими требованиями по идентификации и верификации) и получить доступ к низкорисковым финансовым продуктам. Стандарты также могут допускать регистрацию цифровых профилей на основе нестандартных источников (например, подтверждения от «доверенных лиц»). Кроме того, системы цифрового профиля позволяют пройти удаленную идентификацию и верификацию тем, кто находится в удаленных регионах и не имеет доступа к финансовым услугам. Эти вопросы более детально рассмотрены в разделе «Особые аспекты, связанные с доступностью финуслуг».

110. В развивающихся странах государственные выплаты в пользу граждан (например, выплаты на содержание детей и стипендии), выплаты зарплат бюджетникам, пенсий, а также возврат налогов, все чаще проводятся в безналичной форме, такая же тенденция просматривается и в коммерческой деятельности, и в розничных платежах. Аналогично, и гуманитарная помощь теперь предоставляется без использования наличных. Системы цифрового профиля облегчают получение доступа к счету, который необходим для всех вышеперечисленных действий.

111. Использование надежных, независимых систем цифровых профилей может сократить расходы на процедуру надлежащей проверки клиента и позволит повысить доступность финансовых услуг (см. Box 4 об индийском Aadhaar и Box 5 о Национальном реестре идентификации и гражданского состояния Перу). Повышение финансовой доступности содействует эффективности и расширению охвата режима по ПОД/ФТ.

Риски и проблемы, связанные с системами цифровых профилей

112. В данном Руководстве речь идет об использовании систем цифровых профилей для проведения определенных элементов процедуры надлежащей проверки клиента, а не об использовании традиционных систем идентификации на основе документов. Приводимые ниже аргументы не означают, что риски систем цифровых профилей перевешивают их преимущества, или что они в целом более рискованны, чем традиционные системы идентификации.

113. Как и любая система идентификации, надежность систем цифровых профилей зависит от надежности документов, процессов, технологий и внутренних процедур. Например, и в традиционных системах удостоверения личности, и в системах цифрового профиля личные данные могут быть украдены либо подделаны. Некоторые виды мошенничества менее актуальны для процедур идентификации в личном присутствии или когда те или иные функции не автоматизированы: например, «массовые атаки», которые чаще осуществляются при удаленном взаимодействии. Хотя некоторые методы защиты, характерные для систем

цифрового профиля (например, надежная аутентификация), снижают риски, типичные для бумажных документов, но зато повышают другие – например хищение, изменение или некорректное использование данных.

114. Технические сложности и риски систем цифрового профиля связаны с тем, что они используют открытую коммуникационную сеть (Интернет). Поэтому такие системы могут быть объектом кибератак. Если не предпринять соответствующих мер и не внедрить меры технологической защиты, лица, легализующие преступные доходы, террористы и другие преступники смогут создать фиктивные цифровые профили или незаконно получить доступ к профилям реальных людей.

115. Стандарты систем цифрового профиля помогают выявить, оценить и снизить риски каждого из компонентов цифрового профиля.[33] Ниже мы описываем проблемы, связанные с ненадежностью систем цифрового профиля. В частности, рассматриваются вопросы коннективности, кибербезопасности и неприкосновенности частной жизни.

116. Мы рассматриваем риски, связанные с регистрацией цифрового профиля и аутентификацией. Риски при регистрации – это, как правило, создание «фиктивных» профилей, которые впоследствии могут использоваться для совершения преступлений. Подобные риски минимизируются надежными механизмами проверки личности. Риски аутентификации, напротив, приводят к тому, что цифровой профиль реального человека может использоваться преступниками в собственных целях. В данном случае следует обратить внимание на внедрение эффективных механизмов аутентификации.

Риски, возникающие на этапе идентификации

117. В процессе идентификации есть два типа рисков: (1) кибератаки, которые приводят к компрометации персональной информации и представлению фальшивых документов (либо украденных у реального человека, либо созданных специально), и (2) компрометация провайдеров систем цифровых профилей или инфраструктуры цифровых профилей. В этом разделе рассматривается первый тип рисков; риски, связанные с компрометацией инфраструктуры, кибербезопасностью относятся к управлению системами цифрового профиля в целом и компьютерной безопасности, которые в охват настоящего Руководства не входят.

Риски кражи личности и создания фальшивых цифровых профилей (кибератаки, защита персональных данных и/или нарушениями безопасности)

118. В системах цифровых профилей риски предоставления фальшивых удостоверений личности (украденных или поддельных) могут быть даже выше, чем в традиционных

[33] См. Приложение Е, в котором более подробно рассматриваются уровни надежности идентификации (IALs); уровни надежности аутентификации (AALs); уровни надежности федеративности (FALs), используемые для оценки и снижения рисков на каждом из этих основных этапов.

системах идентификации.[34] **Украсть чужую личность** можно, завладев удостоверением личности с похожей фотографией, либо подделав чужой документ (например, переклеив фото). **Поддельные личности** – это комбинация реальных (обычно украденных) и поддельных данных; их можно использовать для открытия счетов и совершения незаконных операций. Используя поддельную личность, преступник представляется кем-то, кого в реальности не существует, а не крадет данные реального человека. Например, преступные группы могут создавать много синтетических цифровых профилей, частично основанных на реальных (украденных из скомпрометированных баз данных или иным путем), а частично – фальсифицированных данных. Используя синтетические цифровые профили, мошенники могут получить кредитную карту, либо онлайн займ, вывести деньги, а затем «забросить» счет. По мнению экспертов в области цифровых профилей, использование синтетических удостоверений личности представляет наибольший риск на этапе проверки подлинности и регистрации цифровых профилей в США.[35]

119. В целях иллюстрации в таблице ниже представлены эти риски и некоторые стратегии по их снижению при проверке личности и регистрации в соответствии с Руководством NIST.

Таблица 1. NIST – Минимизация рисков при идентификации и регистрации

Тип риска	**Описание**	**Стратегия по потенциальной минимизации риска**
Фальсифицированные документы	Заявитель предъявляет поддельное водительское удостоверение	Провайдер услуг цифрового профиля проверяет защитные элементы документа Провайдер услуг цифрового профиля уточняет подлинность документа у организации, его выпустившей, либо у другого надежного источника
Использование чужого удостоверения личности	Заявитель предъявляет чужой паспорт	Провайдер услуг цифрового профиля сверяет документ и биометрические данные заявителя с данными, полученными из организации, его выпустившей, либо из другого надежного источника

Источник: NIST 800-63A

Риски, связанные с аутентификацией и идентификацией

120. Уязвимости разных типов аутентификации могут быть источником рисков, позволяющих преступникам выдать себя за другого человека, открыть счет или получить несанкционированный доступ к продуктам, услугам или данным.

[34] Поисковый интернет-запрос «поддельные удостоверения личности» выдает в результатах сотни сайтов, продающих поддельные водительские права, паспорта, свидетельства о рождении, миграционные документы и другие официальные документы, качество которых может быть сопоставимо с настоящими документами.
[35] Встреча проектной группы ФАТФ с экспертами по цифровым профилям, сентябрь 2019 года.

121. Для иллюстрации, подобные уязвимости могут включать:

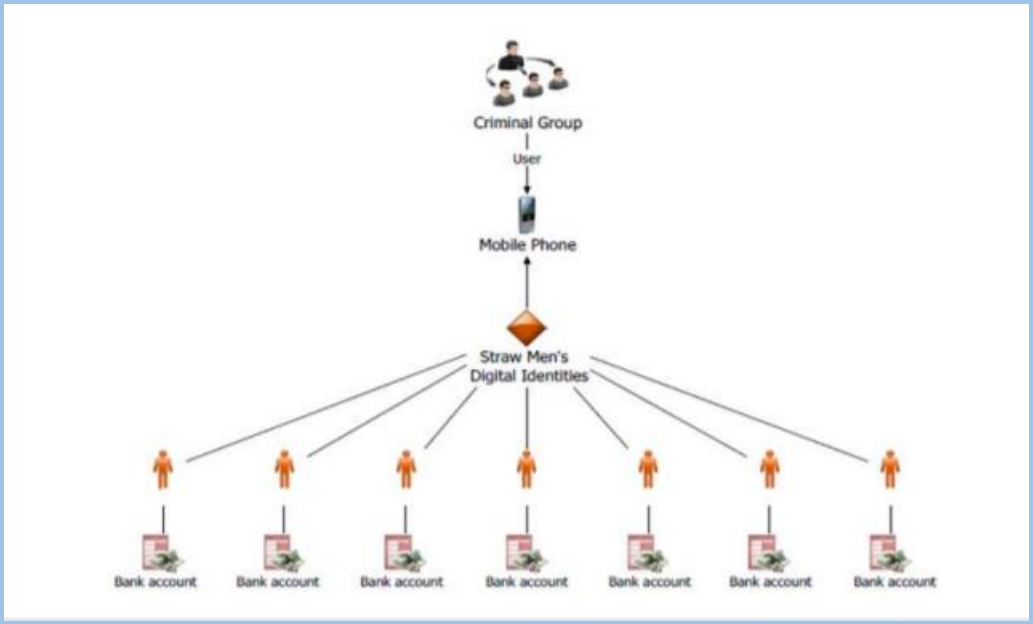
- Подбор данных: когда реквизиты доступа к счету (обычно украденные в ходе утечки данных) пытаются использовать в разных информационных системах. Такой подбор может быть успешен, если жертва, к примеру, использовала одинаковый пароль для доступа к разным счетам.
- Фишинг – это мошенническая попытка собрать данные у ничего не подозревающих жертв с помощью социальной инженерии (вводящие в заблуждение электронные письма, телефонные звонки, текстовые сообщения или веб-сайты и т.д.). Например, преступник представляется кем-то, кто заслуживает доверия (например, сотрудником банка) и пытается обманом заставить свою жертву сообщить имя, пароли и другие личные данные.
- Атака посредника или перехват данных имеет ту же цель, что и фишинг, и может выступать инструментом для фишинга, но в этом случае перехватываются сообщения между жертвой и поставщиком услуг.
- Кража PIN-кода: включает в себя незаметную кражу PIN-кода, введенного на клавиатуре ПК с помощью специальной программы, впоследствии украденный PIN-код используется для получения доступа к услугам.

122. Большинство уязвимостей методов аутентификации эксплуатируются без ведома жертвы, но в некоторых случаях преступления могут совершаться и с ведома клиента или провайдера услуг цифрового профиля. Например, пароль может быть украден, но в некоторых случаях клиент может предоставить его третьим лицам с преступными намерениями.

123. Например, преступные организации могут приобретать идентификационные данные у подставных лиц. У таких лиц уже может быть счет или они соглашаются открыть счет, чтобы передать управление им мошенникам.

Вох 2. Использование цифрового профиля подставными лицами

Швеция выявила риски, связанные с систематическим использованием цифровых профилей, оформленных на подставных лиц, для отмывания денег. Этот риск может быть актуален и при обслуживании клиента в личном присутствии, но в данном случае мы показываем, как такого рода злоупотребления могут быть реализованы в электронной форме. Платежные сервисы, позволяющие совершать операции в режиме реального времени, могут использоваться преступниками, которые некорректно используют цифровые профили, для быстрых переводов между разными счетами.



Когда преступные группы хотят отмыть деньги с использованием системы цифрового профиля, им сначала нужно открыть банковские счета: обычно через подставных лиц. Роль подставного лица состоит в том, чтобы открыть банковский счет, получить цифровой профиль и коды безопасности, а затем продать свои данные преступной группе. На одном мобильном телефоне или планшете можно использовать несколько цифровых профилей (см. диаграмму выше). Банковские счета затем контролируются преступной группой. Важно отметить, что подавляющее большинство цифровых профилей, которыми злоупотребляют преступные группы, регистрируются на легитимные документы, удостоверяющие личность.

Источник: Швеция

124. Ниже описаны некоторые из основных известных рисков, связанных с конкретными типами аутентификаторов, которые актуальны в контексте ПОД/ФТ.

125. **Риски, связанные с многофакторной аутентификацией**: пароли или коды доступа, которые, как предполагается, являются «секретными» аутентификаторами, уязвимы для взлома путем подбора паролей, фишинговых атак и массовых онлайн утечек данных. Причиной 81% случаев утечек были украденные слабые или оставленные по умолчанию пароли.[36] Такие дополнительные аутентификационные факторы, как одноразовые SMS-коды, усиливают защиту паролей, но и они могут быть уязвимы для фишинга и других атак. Устранить эти слабые места могут устойчивые к фишингу аутентификаторы, где хотя бы один фактор зависит от шифрования с открытым ключом[37] (например, аутентификаторы, построенные на основе сертификатов PKI или стандартов FIDO).

126. **Биометрические аутентификаторы**: такие аутентификаторы, как отпечатки пальцев и сканирование радужной оболочки глаза, труднее скомпрометировать, чем традиционные, и они становятся все более распространенными. Большинство смартфонов имеют встроенные сканеры отпечатков пальцев; некоторые смартфоны имеют встроенные сканеры радужной оболочки глаза; а возможности распознавания лиц встроены во многие компьютерные системы и смартфоны.

127. Массовая утечка биометрических данных может произойти из центральных баз данных.[38] Их также могут украсть и подделать с помощью фотографий с высоким разрешением, в том числе можно получить, например, узор радужной оболочки, или незаметно взять отпечаток пальцев. Однако в настоящее время эти типы атак не являются массовыми, т.к. они сложные и/или ресурсоемкие. Например, мошенники не могут массово использовать биометрические аутентификаторы, которые проверяются непосредственно на устройстве, поскольку нужен физический доступ к устройству клиента.

128. Биометрические данные имеют целый ряд других недостатков, которые ставят под сомнение их надежность при использовании в целях аутентификации, поэтому некоторые технические стандарты ограничили их использование для целей аутентификации (в отличие от проверки подлинности).[39] Отпечатки пальцев могут быть не прочитаны или прочитаны неправильно. Факторы распознавания лиц могут быть ненадежными из-за мимики, бороды, макияжа, различных условий освещения и т.д. Из-за неполноты данных, лица людей с темной кожей или имеющих некоторые этнические особенности хуже распознаются. Стоит отметить, что технология продолжает совершенствоваться. В отличие от аутентификаторов, основанных на

[36] Verizon 2018 Data Breach Investigation Report (DBIR), доступен по ссылке https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf.

[37] При шифровании с открытым ключом для человека, системы или устройства генерируется пара ключей. Закрытый ключ хранится в безопасности, а открытый – свободно передается третьим сторонам. Любой, у кого есть открытый ключ, может затем использовать его для шифрования сообщения для отправки владельцу закрытого ключа, зная, что только он сможет открыть его.

[38] В результате атаки на офис управления персоналом США в 2015 году было украдено 5,6 миллиона изображений отпечатков пальцев.

[39] См. NIST 800-63-3, NIST 800-63 (b) и Приложение E.

знаниях или владении, украденные биометрические аутентификаторы трудно аннулировать или заменить.[40]

129. **Риски, связанные с жизненным циклом идентификационных данных**. Намеренные или невольные ошибки в управлении жизненным циклом идентификационных данных и в управлении доступом к счетам, может поставить под угрозу целостность аутентификаторов, а значит компрометировать процедуры идентификации, верификации и текущего мониторинга операций.

130. **Неизвестные риски**. Системы цифровых профилей развиваются, и в ряде случаев технические изменения приносят не только улучшения, но и новые риски, которые неочевидны до тех пор, пока ими не воспользуются мошенники.

Препятствия для доступа к идентификационной информации для проведения текущей надлежащей проверки клиента и мониторинга транзакций

131. Цифровые методы аутентификации могут способствовать текущей надлежащей проверке клиентов и мониторингу транзакций. В случае, если компания использует стороннюю систему цифрового профиля, и сама не собирает информацию (такую как схемы операций, местоположение, доступ к устройствам и т.д.), то она может вовсе не иметь доступа к информации, необходимой для анализа поведения клиентов и моделей транзакций, и, соответственно, не может убедиться в соответствии проводимых сделок сведениям о клиенте, его хозяйственной деятельности и характере рисков, в том числе, когда необходимо, об источнике средств. В тех случаях, когда эта информация собирается в целях борьбы с мошенничеством, она также может быть полезна для целей ПОД/ФТ. Финансовые учреждения могут получить доступ к информации об использовании аутентификационных данных, чтобы выявить использование компрометированных, украденных или проданных цифровых профилей. Ее же можно использовать, чтобы решить, отправлять ли сообщение о подозрительной операции. Одним из важных преимуществ федеративной модели идентификации является то, что провайдеры услуг цифрового профиля и их клиенты могут бороться с мошенничеством совместно, а не только по отдельности.

Более широкие проблемы, связанные с системами цифровых профилей и мерами по ПОД/ФТ

Проблемы с подключением к системе цифровых профилей

132. Без надежной инфраструктуры использовать системы цифровых профилей невозможно. Однако они могут быть спроектированы таким образом, чтобы работать и в онлайн, и в офлайн режиме – чтобы не зависеть от доступа к интернету

[40] Хотя методы аннулирования биометрических данных существуют, в настоящее время их доступность ограничена, а технические стандарты их тестирования все еще находятся в стадии разработки.

или мобильной сети. При принятии решений об использовании систем цифрового профиля для целей надлежащей проверки клиента, следует принимать во внимание устойчивость доступа к сетям связи.

Национальные подходы к удостоверению личности

133. Ненадежность официальных документов, удостоверяющих личность, негативно влияет и на надежность систем цифрового профиля, которые на них полагаются. «Надежность и независимость» документов может снижаться из-за краж личности, подделок документов: особенно, если у них нет элементов защиты или их выдают без надлежащих проверок. Кражи данных из электронных баз являются источником аналогичных рисков: и для электронных, и для аналоговых систем идентификации.

134. Узкоспециализированная система цифровых профилей, которая создавалась не для финансового сектора, может и не справиться с нагрузкой и требованиями, предъявляемыми к процедурам надлежащей проверки клиента (см., например, Box 7 в Приложении II).

Риски, связанные с защитой данных и конфиденциальностью

135. Системы цифрового профиля осуществляют сбор и обработку персональных данных, в том числе биометрических. Стандарты систем включают в себя и требования по их защите. К тому же, чтобы предоставить клиенту больше контроля над персональными данными и тем, кто имеет к ним доступ, разрабатываются соответствующие технические решения (например, децентрализованные системы цифрового профиля).

136. Правительство обязано разработать требования, касающиеся конфиденциальности и защиты данных. Эти требования, как правило, распространяются и на системы цифрового профиля – например, им нужно оценить риски компрометации персональных данных, чтобы выявить потенциальные проблемы и механизмы контроля рисков. Национальные требования по защите данных важны для снижения рисков краж данных о личности и обеспечения кибербезопасности. Поэтому согласно Рекомендации 2, регуляторы в сфере ПОД/ФТ и защиты данных должны обеспечить совместимость разрабатываемых ими правил и требований.

Вопросы, связанные доступностью финансовых услуг

137. Если системой цифрового профиля не могут воспользоваться все (или почти все) жители, либо отдельная группа населения, это может снизить доступность финансовых услуг (или, во всяком случае, вряд ли ее повысит), что само по себе приводит к рискам ОД/ФТ. Введение обязательного использования цифрового профиля, который недоступен всему населению, чревато теми же последствиями, что и обязанность использовать документ, удостоверяющий личность, который есть не у всех. Отсутствие доступа к цифровым технологиям или низкий уровень

технологической грамотности могут усугубить риски исключения из финансовой системы. Этим рискам подвержены бедное и сельское население, женщины, лица, проживающие в неспокойных и затронутых конфликтами районах (например, беженцы и перемещенные лица), все, у кого нет мобильного телефона, смартфона или доступа к надежной сети связи. Если в системе цифрового профиля используется аутентификация только по биометрии, она также может снижать доступность финансовых услуг, поскольку некоторые биометрические методы плохо подходят для ряда уязвимых клиентов. У работников ручного труда биометрические считыватели часто не могут распознать отпечатки пальцев; с трудностями распознавания биометрии могут столкнуться и иные группы населения: например, у пожилых людей меняются черты лица, выпадают волосы или появляются другие признаки старения, болезни или иные факторы; могут не распознаваться лица некоторых этнических групп и лица с определенными физическими характеристиками, например, более темная пигментация кожи, форма глаз или борода.

РАЗДЕЛ V: ОЦЕНКА НАДЕЖНОСТИ И НЕЗАВИСИМОСТИ СИСТЕМ ЦИФРОВЫХ ПРОФИЛЕЙ В РАМКАХ РИСК-ОРИЕНТИРОВАННОГО ПОДХОДА К НАДЛЕЖАЩЕЙ ПРОВЕРКЕ КЛИЕНТА

138. Как отмечается в Разделе III, требование о том, что идентификация/верификация клиентов должна проводиться с использованием надежных, независимых “исходных документов, данных или информации”, означает, что системами цифровых профилей необходимо эффективно управлять, должны использоваться только те технологии, процессы и процедуры, которые обеспечивают необходимый уровень надежности, т.е. уверенность в том, что система цифровых профилей работает так, как она должна работать, и дает точные результаты. Система также должна быть защищена от внешних или внутренних атак, в том числе кибератак или неправомерных действий инсайдеров, чтобы не допустить создания фиктивных цифровых профилей или аутентификацию несанкционированных пользователей.

139. Чтобы выяснить, соответствует ли система цифровых профилей требованиям Рекомендаций 10 пунктов (a) и (d), правительствам, финансовым учреждениям и другим заинтересованным сторонам следует оценить следующие параметры:

    a. Определить уровень надежности системы цифровых профилей, учитывая ее технологии, архитектуру и управление для определения ее надежности/независимости; и

    b. Определить уровень надежности, независимости системы цифровых профилей в свете потенциальных рисков ОД/ФТ, мошенничества и других финансовых рисков, используя риск-ориентированный подход и учитывая уровень качества системы подтверждения цифровых профилей.

140. В зависимости от самой системы цифровых профилей и нормативно-правовой базы в конкретной юрисдикции, правительство и компании могут иметь разные обязанности при оценке уровней надежности системы.

141. Процесс принятия решений описывает ряд вопросов, на которые надо ответить финансовой организации при принятии решения об использовании системы цифровых профилей для идентификации и верификации клиента, а также для целей текущей надлежащей проверки.

Вопрос первый: санкционировало ли правительство систему цифровых профилей для целей надлежащей проверки клиента?

142. Если регулятор прямо разрешает использовать систему цифрового профиля, в том числе для целей надлежащей проверки клиента, компании могут делать это, не

проводя дополнительных оценок самостоятельно. Правительство фактически берет оценку надежности системы цифрового профиля на себя (по крайней мере, для стандартных рисков, связанных с надлежащей проверкой клиента). Однако в зависимости от законов о ПОД/ФТ и экосистемы цифровых профилей в отдельно взятой юрисдикции, компании могут обязать принять дополнительные меры (см. пункты 147 и 148 ниже).

143. Правительства могут обозначить свою позицию по вопросу использования систем цифровых профилей в целях надлежащей проверки клиента, издавая нормативные акты или руководства для компаний, разрешая или даже требуя использовать системы цифровых профилей для определенных этапов надлежащей проверки клиента. Правительство может дать разрешение на использование системы цифровых профилей в тех случаях, когда, например, оно же разработало и эксплуатирует эту систему и поэтому доверяет ей, или когда правительство располагает механизмом получения проверенной, сертифицированной информации об уровнях надежности системы.

144. Правительства также могут в определенной форме поддерживать конкретную систему цифрового профиля для использования финансовыми организациями. Например, когда государство предоставляет систему цифрового профиля, которую можно использовать для разных целей. Правительствам следует раскрывать информацию о том, как работают их системы цифрового профиля и каков уровень их надежности. Это справедливо и для систем цифровых профилей, которые используются только для получения финансовых услуг.

145. В зависимости от местного законодательства по ПОД/ФТ, организациям нужно будет дополнять использование систем цифрового профиля применением иных мер по ПОД/ФТ: в частности, в ситуациях повышенного риска (например, понимание целей установления деловых отношений). В некоторых юрисдикциях использование систем цифрового профиля может быть предусмотрено только для ситуаций пониженного риска.

146. Компаниям следует также рассмотреть возможность применения дополнительных мер снижения рисков, помимо тех, которые установлены законодательством: например, проверка дополнительных данных, использование дополнительных методов аутентификации или иных мер снижения рисков ОД/ФТ, в соответствии с внутренними программами контроля.

Вопрос второй: известен ли уровень надежности системы цифрового профиля?

147. В тех случаях, когда правительство прямо или косвенно не санкционировало использование конкретных систем цифровых профилей для целей надлежащей проверки клиента, компании следует определить уровень ее надежности.[41]

148. Если правительство проверяет или сертифицирует системы цифровых профилей (само или через организации, действующие от его имени[42]), то организации могут полагаться на эти оценки. Аналогичным образом, правительство может также утвердить экспертный орган, внутренний или иностранный, для проверки/аудита и сертификации уровней надежности систем цифровых профилей. Обзор некоторых из этих экспертных органов см. в Приложении D. Уровень надежности может быть определен для всей системы в целом, либо для отдельных ее компонентов, но информация об уровне надежности должна быть публично доступна.

149. Если правительство не разрешило использовать систему (системы) цифровых профилей в процессе надлежащей проверки клиента и не предоставило механизм для получения достоверной информации о ее уровне надежности, то компании должны сами определять надежность и независимость этой системы с помощью любого из этих механизмов:

    a. самостоятельно провести оценку, или

    b. получить информацию об уровне надежности системы у экспертной организации (даже если она не утверждена официально).

150. Если компания сама проводит оценку надежности, она должна тщательно провести надлежащую проверку провайдера системы цифровых профилей, включая его систему управления.

151. Компания должна использовать информацию от экспертной организации только в том случае, если у нее есть разумные основания полагать, что этот орган применяет соответствующие, публичные стандарты оценки систем цифровых профилей. Например, организация может быть сертифицирована для аналогичных целей другим правительством или широко признана экспертами в этой стране, регионе или на международном уровне.

[41] Как указывалось ранее в настоящем Руководстве, термин “уровень надежности” относится к уровню надежности или достоверности каждого из компонентов процесса идентификации с использованием цифрового профиля.

[42] Данные действия могут не осуществляться регулирующими органами по ПОД/ФТ, поскольку, вероятнее всего, такие органы не смогут определить, применяет ли организация приемлемые технические стандарты: это может входить в компетенцию иных ведомств. Каких именно – зависит от конкретной юрисдикции. Например, в США Управление служб общего назначения (GSA) одобрила ряд компаний, которые могут сертифицировать системы цифрового профиля, которые используются государственными органами.

Вопрос третий: можно ли пользоваться системой цифровых профилей в целях ПОД/ФТ?

152. После определения уровня надежности системы цифрового профиля, организация должна определить, насколько ее можно применять в целях надлежащей проверки клиента, с учетом риск-ориентированного подхода. Иными словами, может ли система цифрового профиля использоваться для идентификации/верификации клиента, текущей надлежащей проверки клиента, с учетом рисков услуги, операций и географии. Организациям следует проанализировать, насколько система цифрового профиля адекватна в контексте имеющихся рисков ОД/ФТ. В зависимости от местных требований по ПОД/ФТ, организации могут выбрать одну из нескольких систем цифрового профиля. Следует сопоставить надежность системы цифрового профиля и риски незаконных действий или ОД/ФТ, которым может быть подвержена организация.

153. В некоторых странах регулятор установил минимальный уровень надежности, который необходим в ситуациях стандартного или высокого риска ОД/ФТ. В свою очередь, компании могут выбирать разные системы цифрового профиля, которые обеспечивают такой уровень надежности, или выбирать подходящие способы подтверждения личности, предусмотренные этими системами. Этот выбор должен быть обусловлен характером рисков ОД/ФТ. Для ситуаций пониженного риска компании могут выбирать систему цифрового профиля самостоятельно.

Использование технических стандартов для применения риск-ориентированного подхода

154. Как обсуждалось выше, для снижения рисков ОД/ФТ, правительства (выступающие в качестве провайдеров систем цифровых профилей и/или регулирующих органов, надзорных органов или законодательных органов) и организации (как доверяющие третьим сторонам) должны учитывать соответствующие факторы риска, связанные с цифровыми профилями, и уровни надежности систем цифровых профилей. Ниже подробно разъясняется, что **стандарты надежности и прочие технические стандарты систем цифрового профиля** являются полезным инструментом для проведения такой оценки.

155. В связи с этим, правительствам и организациям рекомендуется учитывать стандарты надежности и прочие технические стандарты систем цифровых профилей, при оценке соответствия системы цифровых профилей критериям «надежности, независимости», установленным в Рекомендации 10(а). Также рекомендуется отдельно рассматривать надежность каждого из основных компонентов системы цифровых профилей, поскольку в зависимости от потенциальных факторов риска ОД/ФТ для каждого компонента системы цифровых профилей может требоваться

разный уровень надежности (проверка подлинности/регистрация, аутентификация или, если применимо, федеративность).

156. **Оценка надежности каждого из элементов системы** цифрового профиля позволяет применять более сбалансированный риск-ориентированный подход. Подобная оценка особенно актуальна в контексте доступности финансовых услуг. Технические стандарты портала GOV.UK и американский стандарт US NIST 800-63-3 предусматривают отдельные уровни надежности каждого элемента систем цифрового профиля.[43] Те стандарты, которые относятся к системе цифрового профиля в целом (например, Регламент eIDAS), могут использоваться и для оценки каждого компонента системы в отдельности.

157. Технологии систем цифрового профиля и связанные с ними технические стандарты постоянно развиваются.[44] Чтобы не препятствовать внедрению инноваций, эти стандарты устанавливают требования к качеству результатов, а не процедурам, которые используются для того, чтобы этих результатов достичь. Поэтому сами по себе стандарты допускают использование разных технологий и архитектур и сформулированы таким образом, чтобы сохранять актуальность в будущем. Странам не следует фиксировать конкретные процедуры: иначе вместо минимально достаточных они будут рассматриваться как максимально необходимые.

Использование технических стандартов в системах цифрового профиля

158. Стандарты надежности устанавливают технические требования к каждому элементу системы цифрового профиля.

159. Точно так же, как в пояснительной записке к 10 Рекомендации приводятся примеры разных факторов рисков ОД/ФТ, технические стандарты указывают те факторы, которые могут влиять на надежность элементов системы цифрового профиля. Соответственно, системы с более низким уровнем надежности могут быть подвержены ошибкам больше, чем системы с высоким. Данное Руководство не требует, чтобы системы цифрового профиля соответствовали какому-то конкретному уровню надежности.

160. Некоторые технические стандарты предусматривают оценку каждого компонента системы цифрового профиля в отдельности: не все они должны быть одинаково надежны. В контексте риск-ориентированного подхода, уровень надежности каждого элемента системы цифрового профиля должен соответствовать рискам

[43] Например, в соответствии с Руководством NIST установлены уровни надежности (1-3) для каждого из этапов процесса идентификации с использованием цифрового профиля: уровень надежности удостоверения личности (IAL); уровень надежности аутентификации и управления жизненным циклом данных (ALA); и уровень надежности федеративности (FAL).

[44] Следует признать, что стандарты цифровых профилей не всегда идут в ногу с развитием технологий. Например, к моменту выхода этого Руководства стандарты надежности и прочие технические стандарты систем цифрового профиля еще не предусматривали непрерывной аутентификации. Они также не включали понятие эволюционирующего профиля, поскольку оно связано с постоянной динамической проверкой личности.

ПОД/ФТ, мошенничества и иных преступлений. Даже при использовании стандартов, которые предусматривают оценку всей системы в целом, компании могут самостоятельно оценивать каждый отдельный из ее компонентов.

161. В ***Приложении Е*** представлены примеры технических стандартов, которые используются в ЕС и США; они иллюстрируют некоторые факторы, которые необходимо принимать во внимание при оценке надежности и независимости систем цифрового профиля.

Особые аспекты, связанные с доступностью финуслуг

Связь систем цифрового профиля, риск-ориентированного подхода и рисков ОД/ФТ

162. В идеале внедрение систем цифровых профилей обеспечит более надежное подтверждение личности: особенно в странах, где такой возможности пока нет. Однако, поскольку цифровые профили создаются на основе документов, удостоверяющих личность, там, где такие документы не универсально доступны, будут ограниченно доступны и цифровые профили.

163. Как указывалось выше, в странах с недостаточным уровнем доступности финансовых услуг следует использовать гибкие подходы к процедурам установления и подтверждения личности. Подобный подход позволит лицам, не имеющим доступа к финансовым услугам, подтвердить личность, не имея всего набора документов (например, не подтверждая адрес проживания, или предоставив подтверждение от доверенных лиц). Регуляторам следует применять риск-ориентированный подход к проведению надлежащей проверки клиента посредством систем цифрового профиля: особенно в странах, где недостаточный доступ к финансовым услугам является источником риска ОД/ФТ.

164. В 2017 году ФАТФ опубликовала дополнение к Руководству 2013 года по мерам ПОД/ФТ и доступности финуслуг, уделив особое внимание надлежащей проверке клиента и доступности финуслуг.[45] В документе освещаются меры по снижению рисков, которые должны предпринимать организации, исходя из уровня и характера рисков. В нем также представлены различные подходы к надлежащей проверке клиента для устранения трудностей, связанных с проверкой личности клиента, и, тем самым, расширения доступа к финуслугам. В частности, документ также описывает разные варианты надлежащей проверки клиента, которые позволяют обойти сложности, связанные с подтверждением личности. В Руководстве отмечается, что распространение цифровых финансовых услуг сопровождалось введением многоуровневой системы идентификации. Например, лица, не имеющие доступа к

[45] ФАТФ (2013-2017), О мерах противодействия отмыванию денег и финансированию терроризма и обеспечению доступности финансовых услуг - С дополнением о надлежащей проверке клиента, ФАТФ, Париж www.fatfgafi.org/publications/financialinclusion/documents/financial-inclusion-cdd-2017.html

финансовым услугам, могут воспользоваться ограниченно функциональными финансовыми услугами, без подтверждения личности.

165. Логику Руководства по доступности финансовых услуг 2017 года можно применить и к использованию систем цифровых профилей: если риски ОД/ФТ низки, то допустимо использовать системы с более низким уровнем надежности. Риски ОД/ФТ могут быть минимизированы, к примеру, и ограничением функциональности счета. Если в стране финансовые преступления совершаются, в основном, путем кражи логинов и паролей, то допустимо использовать систему цифрового профиля с высокой надежностью авторизации и пониженной надежностью процедур регистрации. Аутентификация клиента важна вне зависимости от того, используется полнофункциональный платежный продукт или малофункциональный счет: она обеспечивает и защиту от несанкционированных операций, и препятствует попыткам обойти установленные ограничения на сумму или частоту совершения транзакций.

166. Применение риск-ориентированного подхода при внедрении систем цифрового профиля критически важно для обеспечения доступности финансовых услуг. Риск-ориентированный подход способствует введению многоуровневого подхода к надлежащей проверке клиента, поскольку, согласно техническим стандартам, системы с менее надежными методами регистрации могут использовать упрощенные методы подтверждения личности (см. Приложение Е). Это значит, что лица, у которых нет документов, удостоверяющих личность, все равно могут зарегистрировать свой цифровой профиль. И впоследствии использовать его для открытия счета с ограниченным функционалом и лимитами.

167. К тому же, пользователи системы электронных подписей со временем могут выработать надежный цифровой след, по которому в будущем можно будет оценивать их уровень риска. В зависимости от подхода, принятого в конкретной стране, может поменяться концепция официальной личности: от фиксированной к динамической, которая со временем становится более надежной. В динамической модели официальной личности, чем больше лицо пользуется цифровыми финансовыми услугами и онлайн-сервисами, тем больше ему доступно разных способов подтверждения личности.

168. Динамический цифровой профиль поддерживает доступность финансовых услуг, даже если системы цифрового профиля не интероперабельны, поскольку помогает субъектам финансового мониторинга изучать клиентов и предлагать им более широкий набор финансовых услуг. Но еще более полезным он становится, если профиль интероперабелен: информация о паттернах поведения, совершаемых операциях, собранная одной организацией, может использоваться другими учреждениями.

Вох 3. Использование системы цифрового профиля для повышения доступности финансовых услуг, в рамках дифференцированного подхода к идентификации клиента

Физическое лицо, не имеющее доступа к финансовым услугам, хочет открыть базовый банковский счет, используя цифровой профиль, зарегистрированный без предъявления удостоверения личности. Такой цифровой профиль недостаточно надежен для однозначного удостоверения личности, но обеспечивает достаточно надежную аутентификацию.

Организация принимает клиента на обслуживание и открывает банковский счет с низким уровнем риска, с ограниченным максимальным балансом и ограниченным функционалом: запретом на трансграничные операции (эти ограничения основаны на анализе риска). Клиент указывает банковский счет в договоре с сотовым оператором, получает на него зарплату и совершает некоторые операции.

Чтобы определить паттерн поведения клиента, финансовая организация анализирует информацию о начислении зарплаты, социальных пособий и иных источниках средств, регулярные платежи за сотовую связь и жилищно-коммунальные услуги. Также анализируются иные сведения для верификации данных о месте жительства клиента. Со временем, финансовая организация может использовать информацию о паттернах поведения клиента (время и среднюю сумму операций, назначения платежей, геолокацию), чтобы повысить надежность аутентификации и более эффективно бороться с мошенничеством.

Национальное законодательство по ПОД/ФТ устанавливает принципы и результаты, которых должны достичь финансовые организации. Нормативная база требует от финансовых организаций иметь достаточные основания знать, кто их клиент, но не устанавливает конкретные процедуры, как это сделать. Со временем финансовая организация может использовать информацию, полученную в ходе обслуживания клиента, чтобы удостовериться в том, что знает клиента и понимает его профиль риска. Когда это понимание достаточно для регулятора и соответствует риск-аппетиту самой финансовой организации, она может открыть клиенту стандартный банковский счет с более высокими лимитами, широкой функциональностью, а позднее – и предоставить ему небольшой займ, который клиент мог бы использовать для старта своего бизнеса.

Такой подход к цифровому профилю отражает тот же принцип, который изложен в Руководстве ФАТФ по надлежащей проверке клиента и доступности финансовых услуг 2017 года. Руководство указывает, что лица, у которых нет документов, удостоверяющих личность, могут со временем могут проходить более полную идентификацию и переходить от низкорисковых продуктов к более полнофункциональным.

Источник: Казначейство США

Технические стандарты систем цифрового профиля могут способствовать расширению доступности финуслуг

«Доверенные лица»

169. Некоторые технические стандарты предусматривают возможность подтверждения личности через доверенных лиц: глав поселения, представителей местной власти, судей, работодателей, людей с хорошей репутацией (бизнесменов, адвокатов, нотариусов), специально обученных или сертифицированных лиц – в соответствии с местным законодательством[46].

170. Например, в соответствии с NIST использование доверенных лиц требует от провайдеров систем цифровых профилей:

- Установить письменные правила и процедуры, касающиеся определения доверенных лиц и их статуса, в том числе отзыва и приостановления этого статуса;
- Подтвердить личность доверенного лица на том же уровне, что и заявителя, и определить требования к минимальной идентификационной информации или документам, чтобы установить отношения между доверенным лицом и заявителем.

Удаленное подтверждение личности и удаленное принятие на облуживание

171. Как отмечалось ранее, системы цифровых профилей могут обеспечивать удаленную идентификацию/верификацию клиентов и допускать осуществление финансовых операций при стандартном или низком уровне риска. Технические стандарты допускают дистанционное подтверждение личности и регистрацию, что не препятствует признанию системы цифрового профиля надежной. См. Приложение Е.

[46] NIST 800-63A 4.4.2. IAL2 Trusted Referee Proofing Requirements.

Данная публикация предназначена только для ознакомления. Представленный перевод является неофициальным и не имеет юридической силы.

Ассоциация «АЭД» не несет ответственности за прямые или косвенные убытки, которые могут понести третьи лица, руководствуясь содержанием настоящей публикации.

Оригинал Руководства на английском языке доступен по адресу https://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html.

Предложения и комментарии к тексту данного документа Вы можете направить по адресу npaed@npaed.ru.