FATF

ЦИФРОВАЯ ИДЕНТИФИКАЦИЯ

МАРТ 2020

Группа разработки финансовых мер борьбы с отмыванием денег (ФАТФ) является независимой межправительственной организацией, разрабатывающей и популяризирующей свои принципы для защиты всемирной финансовой системы от угроз отмывания денег, финансирования терроризма и финансирования распространения оружия массового уничтожения. Рекомендации ФАТФ являются общепризнанными международными стандартами по противодействию отмыванию денег и финансированию терроризма (ПОД/ФТ).

Подробная информация о ФАТФ размещена на сайте: **www.fatf-gafi.org.**

Данный документ и/или любая включённая в него карта подготовлены без предубеждения и ущемления статуса или суверенитета над любой территорией, международных границ и разграничительных линий, а также названий любых территорий, городов или областей.

Неофициальный перевод подготовлен АНО МУМЦФМ

Ссылка на оригинальный документ:

FATF (2020), *Guidance on Digital Identity,* FATF, Paris,
www.fatf-gafi.org/publications/documents/digital-identity-guidance.html

Содержание

СПИСОК СОКРАЩЕНИЙ

AAL 1/2/3	Уровень надежности аутентификации (согласно стандартам Национального института стандартов и технологий США)
AL	Уровень надежности
ПОД/ФТ	Противодействие отмыванию денег и финансированию терроризма
API	Интерфейс прикладного программирования
ASP	Провайдер услуг аутентификации
НПК	Надлежащая проверка клиентов
CEN	Европейский комитет по стандартизации
CENELEC	Европейский комитет электротехнической стандартизации
CSP	Провайдер учётных данных
DCS	Сервис проверки документов
TPP	Технология распределённого реестра
УНФПП	Установленные нефинансовые предприятия и профессии
ETSI	Европейский институт телекоммуникационных стандартов
Регламент ЕС об электронной идентификации	Регламент (ЕС) №910/2014 «Об электронной идентификации и удостоверительных сервисах для электронных транзакций на внутреннем рынке»
FAL 1/2/3	Уровень доверия к федеративной интеграции (согласно стандартам Национального института стандартов и технологий США)
FIDO	Альянс «Fast Identity Online Alliance»
GDPR	Общий регламент по защите данных (ЕС)
GPS	Система глобального позиционирования
GSMA	Глобальная система мобильной связи
ИТТ	Информационные и телекоммуникационные технологии
IAL 1/2/3	Уровень надежности идентификации (согласно стандартам Национального института стандартов и технологий США)
ID	Идентификация личности
IDSP	Провайдер идентификационных услуг
МЭК	Международная электротехническая комиссия
ПЗР	Пояснительная записка к Рекомендации
IP	Межсетевой протокол
ISO	Международная организация по стандартизации
МСЭ	Международный союз электросвязи

IVSP	Провайдер услуг по верификации личности
LoA	Уровень надежности
MAC	Контроль доступа к среде передачи данных
ОД	Отмывание денег
MFA	Многофакторная аутентификация
НПО	Неправительственные организации
NIST	Национальный институт стандартов и технологий США
OIDF	Организация «OpenID Foundation»
PII	Информация, позволяющая установить личность
PIN	Персональный идентификационный номер
Р.	Рекомендация
РОП	Риск-ориентированный подход
SAG	Консультативная группа по стандартам
SCA	Усиленная аутентификация клиентов
ФТ	Финансирование терроризма
ПУВА	Провайдер услуг в сфере виртуальных активов
W3C	Консорциум Всемирной паутины
ВКБ ООН	Верховный комиссар ООН по делам беженцев

КРАТКИЙ ОБЗОР

1. Темпы роста объёмов цифровых платежей оцениваются в 12,7% в год, и прогнозируется, что количество таких операций достигнет 726 миллиардов к 2020 году[1]. Согласно оценкам, к 2022 году 60% мирового ВВП будет оцифровано[2]. Увеличение количества и объёмов цифровых финансовых операций требует от ФАТФ более глубокого понимания того, как происходит идентификация и верификация физических лиц в мире цифровых финансовых услуг. Быстрое развитие технологий цифровой идентификации приводит к появлению различных систем цифровой идентификации. Настоящее Руководство предназначено для оказания содействия государственным органам, регулируемым субъектам[3] и другим соответствующим заинтересованным сторонам в определении того, как системы цифровой идентификации могут быть использованы для реализации определённых элементов надлежащей проверки клиентов (НПК) в соответствии с Рекомендаций 10 ФАТФ.

2. Понимание того, как работают системы цифровой идентификации является важным и необходимым условием для применения риск-ориентированного подхода, рекомендованного в настоящем Руководстве. В Разделе II данного Руководства приведён краткий обзор ключевых характеристик систем цифровой идентификации, которые более подробно рассматриваются в Приложении «А».

3. В Разделе III обобщены основные требования ФАТФ, рассматриваемые в настоящем Руководстве, включая требование об установлении и проверке личности клиентов с использованием документов, данных или информации из «надёжных, независимых» источников (Рекомендация 10(а)). В контексте цифровой идентификации, требование о том, чтобы «источники цифровых документов, данных или информации» являлись «надёжными и независимыми», означает, что система цифровой идентификации, используемая для проведения НПК, должна быть основана на технологиях, надлежащем управлении, процессах и процедурах, обеспечивающих необходимый уровень уверенности в том, что система выдаёт точные результаты. В Руководстве разъясняется, что дистанционная идентификация клиентов и операций без личного контакта, при которых используются надёжные независимые системы цифровой идентификации, наряду с наличием надлежащих мер, направленных на снижение рисков, могут представлять стандартный или даже пониженный уровень риска.

Надёжные независимые системы цифровой идентификации, наряду с надлежащими мерами, направленными на снижение рисков, могут обеспечить стандартный или даже пониженный уровень риска.

[1] Консалтинговая компания «Capgemini» и Группа «BNP Paribas» (2018г.), *«World Payments Report 2018» («Обзор мировых платежей за 2018 год»)*, доступ по адресу: https://worldpaymentsreport.com/wp-content/uploads/sites/5/2018/10/World-Payments-Report-2018.pdf

[2] Международная исследовательская и консалтинговая компания «International Data Corporation» (IDC), IDC FutureScape: Worldwide IT Industry 2019 Predictions («Взгляд в будущее: прогноз развития мировой ИТ-индустрии на 2019 год»)

[3] Для целей настоящего Руководства «регулируемые субъекты» означают финансовые учреждения, провайдеров услуг в сфере виртуальных активов (ПУВА) и установленные нефинансовые предприятия и профессии (УНФПП), как они определены в Стандартах ФАТФ, и при условии, что они обязаны проводить надлежащую проверку клиентов в обстоятельствах, предусмотренных в Рекомендации 22. В июне 2019 года ФАТФ внесла изменения в Рекомендацию 15 (Новые технологии) и в Пояснительную записку к Рекомендации 15 с тем, чтобы, помимо всего прочего, распространить обязательства по надлежащей проверке клиентов, установленные в Рекомендации 10, на провайдеров услуг в сфере виртуальных активов.

4. В основе риск-ориентированного подхода, рекомендованного в настоящем Руководстве, лежит набор открытых согласованных механизмов надежности идентификации и технических стандартов для систем цифровой идентификации (далее по тексту «механизмы и стандарты надежности цифровой идентификации»), которые были разработаны в нескольких юрисдикциях. Международная организация по стандартизации (ISO) совместно с Международной электротехнической комиссией (МЭК) ведёт работу по стандартизации этих механизмов надежности цифровой идентификации и обновляет ряд технических стандартов ISO/МЭК, касающихся идентификации, безопасности информационных технологий и неприкосновенности личной жизни, в целях разработки комплексного глобального стандарта для систем цифровой идентификации. В рамках механизма надежности идентификации устанавливаются требования, касающиеся разных «уровней надежности» или «уровней доверия». Такие уровни надежности определяют степень уверенности в надёжности и независимости системы цифровой идентификации и её элементов. Хотя уровни надежности, установленные разными юрисдикциями, могут различаться в некоторых отношениях, для удобства пользования в настоящем Руководстве рассматриваются в основном механизмы и стандарты надежности цифровой идентификации Национального института стандартов и технологий США (NIST) (Руководства по цифровой идентификации NIST)[4] и Регламент ЕС об электронной идентификации[5]. Юрисдикциям следует рассматривать подход, изложенный в настоящем Руководстве, с учётом своих национальных механизмов надежности цифровой идентификации и других соответствующих технических стандартов[6].

5. Механизмы и стандарты надежности цифровой идентификации, а также нормативно-правовые акты в сфере ПОД/ФТ были разработаны, исходя их разных целей, и предназначены для разных пользователей. Однако в настоящем Руководстве механизмы и стандарты надежности цифровой идентификации и требования ФАТФ, касающиеся надлежащей проверки клиентов, рассматриваются в привязке друг к другу. Как видно из приведённой ниже Таблицы, ключевые элементы систем цифровой идентификации имеют отношение к конкретным требованиям по идентификации и верификации, установленным в Рекомендации 10(a). В этой связи механизмы надежности цифровой идентификации и технические стандарты в данной области, в которых определены указанные элементы и установлены требования к каждому уровню надежности, являются весьма полезным инструментом для оценки надёжности и независимости систем цифровой идентификации в целях ПОД/ФТ.

---

[4] Руководства по цифровой идентификации NIST 800-63 включают комплект документов: Руководство по цифровой идентификации NIST SP 800-63-3 - общий обзор; Руководство по цифровой идентификации NIST SP 800-63A – регистрация и подтверждение личности; Руководство по цифровой идентификации NIST SP 800-63B – аутентификация и управление жизненным циклом; и Руководство по цифровой идентификации NIST SP 800-63C – интеграция и утверждения

[5] Регламент (ЕС) №910/2014 «Об электронной идентификации и официальных сервисах для электронных транзакций на внутреннем рынке»

[6] В юрисдикциях может не иметься механизма гарантии цифровой идентификации или технических стандартов, касающихся систем цифровой идентификации, но могут иметься другие технические стандарты (например, стандарты информационной безопасности ИТ-систем), которые являются весьма актуальными для рассматриваемой темы.

Требования по надлежащей проверке клиентов (физических лиц)	Ключевые элементы систем цифровой идентификации
Идентификация (установление личности) /верификация (проверка личности) – Рекомендация 10(a)	Проверка и подтверждение подлинности личности, регистрация (с привязкой) – Кто ты такой? Получение атрибутов (имя, дата рождения, номер документа, удостоверяющего личность и т.д.) и свидетельств, подтверждающих эти атрибуты; проверка и подтверждение достоверности удостоверяющих личность свидетельств и отождествление их с конкретным человеком, личность которого подтверждена. Привязка – Выпуск учётных данных/аутентификаторов, связывающих лицо, во владении/под контролем которого находятся эти учётные данные, с человеком, личность которого подтверждена. Аутентификация – Являетесь ли вы человеком, чья личность установлена/проверена? Установление того, что привязывающие учётные данные находятся во владении и под контролем заявителя. Аутентификация применима в рамках Рекомендации 10(a), если регулируемый субъект проводит идентификацию/верификацию путём подтверждения того, что потенциальный клиент обладает ранее выпущенными учётными цифровыми идентификационными данными.

6. В настоящем Руководстве разъясняется, что (1) аутентификация имеет отношение к требованиям Рекомендации 10(a) в случаях, когда регулируемый субъект открывает счёт для клиента, имеющего ранее выпущенные учётные цифровые идентификационные данные (т.е. не внутренние цифровые идентификационные данные, выданные этим регулируемым субъектом); и, что (2) в контексте цифровых финансов и цифровой идентификации, эффективная аутентификация личности клиента для предоставления ему права доступа к счёту может содействовать мерам, принимаемым в целях ПОД/ФТ.

7. Раздел V является главным элементом настоящего Руководства. В нём даны руководящие указания для государственных органов, регулируемых субъектов и других соответствующих сторон по вопросам применения риск-ориентированного подхода к использованию систем цифровой идентификации в целях идентификации и верификации клиентов в соответствии с Рекомендацией 10(a), а также для содействия проведению постоянной проверки в соответствии с Рекомендацией 10(d). Рекомендованный подход является непредвзятым в плане используемых технологий (то есть, в нём не отдаётся предпочтение каким-либо конкретным типам систем цифровой идентификации). Этот подход включает в себя два элемента:

Применение **риск-ориентированного** подхода к использованию цифровой идентификации в целях НПК: (1) Понимание уровней надежности, обеспечиваемых системой цифровой идентификации; и (2) оценка, с учётом уровней надежности, того, является ли система идентификации достаточно надёжной и независимой в свете рисков ОД/ФТ.

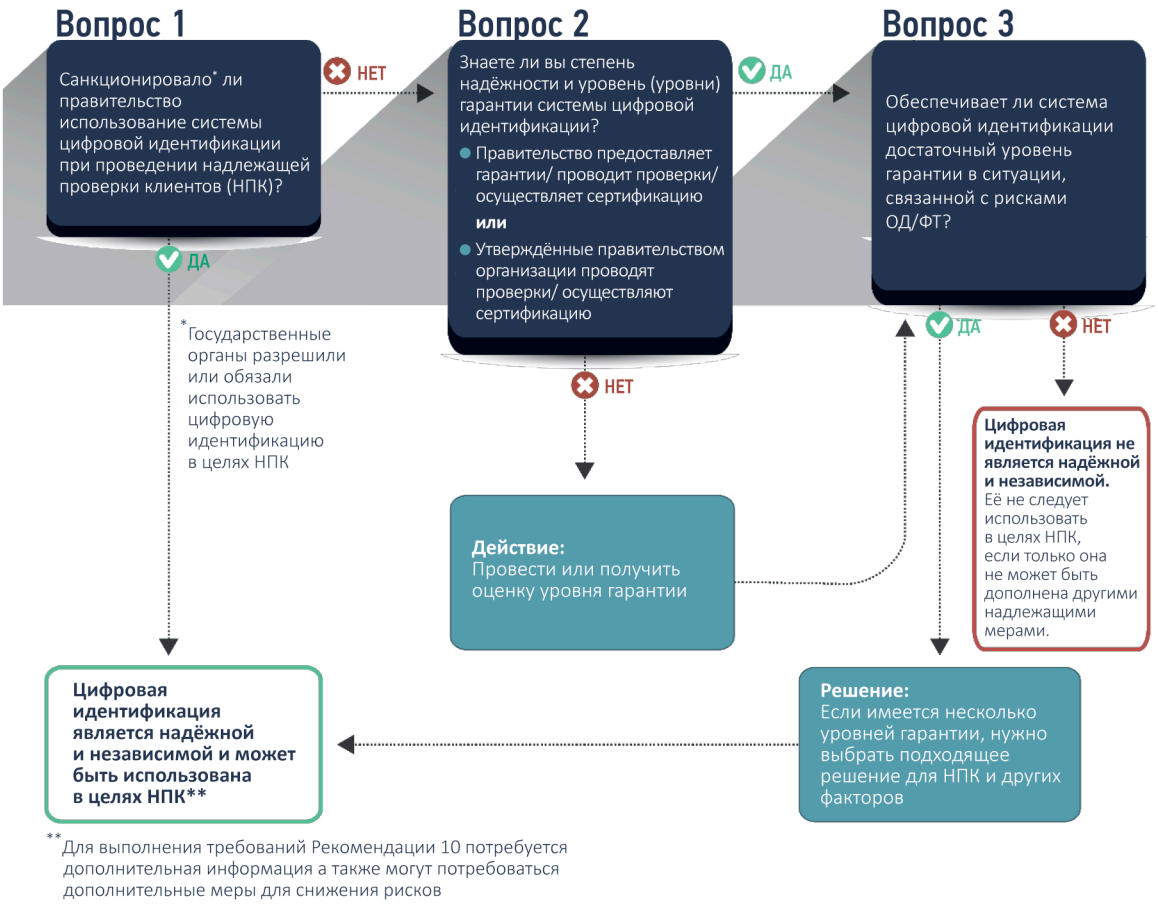
a. Понимание уровней надежности, обеспечиваемых основными элементами системы цифровой идентификации (включая её технологию, архитектуру и систему управления), для определения того, что она является надёжным независимым источником информации; и

b. Более широкое риск-ориентированное определение того, обеспечивает ли конкретная система цифровой идентификации, с учётом её уровней надежности, надлежащую степень надёжности и независимости в свете потенциальных рисков, связанных с отмыванием денег, финансированием терроризма, мошенничеством и другой незаконной финансовой деятельностью.

8. В Разделе V разъясняется, как использовать механизмы и стандарты надежности цифровой идентификации для оценки надёжности/независимости. В нём также определён процесс принятия решений, которым следует руководствоваться регулируемым субъектам при принятии решения о том, является ли использование цифровой идентификации для реализации некоторых элементов НПК подходящим в рамках Рекомендации 10 ФАТФ. Государственным органам и регулируемым субъектам придётся скорректировать этот процесс принятия решений с учётом конкретных обстоятельств и особенностей юрисдикции и отдельных субъектов. В зависимости от системы (систем) цифровой идентификации и нормативно-правовой базы, имеющейся в конкретной юрисдикции, государственные органы и регулируемые субъекты могут выполнять разные функции и обязанности в процессе оценки уровней надежности, обеспечиваемых системой идентификации, и её пригодности для целей НПК, как указано на приведённой ниже диаграмме принятия решений для регулируемых субъектов.

9. Настоящее Руководство не является обязательным для выполнения. В нём разъясняются действующие Стандарты ФАТФ, которые являются нейтральными в плане используемых технологий.

Рисунок 1: Процесс принятия решений для регулируемых субъектов



10. 10. В Разделе IV настоящего Руководства рассматриваются некоторые преимущества систем цифровой идентификации, а также представляемые ими риски. Многие риски, связанные с системами цифровой идентификации, также присутствуют при проведении идентификации с использованием документарных доказательств в бумажной форме. Однако проверка и подтверждение подлинности личности и/или аутентификация лиц с использованием открытых сетей связи (Интернета) обусловливает особые риски, характерные для систем цифровой идентификации – в частности риски, связанные с кибератаками и возможными крупномасштабными хищениями идентификационных данных. С другой стороны, системы цифровой идентификации, которые обеспечивают снижение этих рисков в соответствии с механизмами и стандартами надежности цифровой идентификации, имеют большой потенциал для укрепления мер НПК и мер контроля в целях ПОД/ФТ, расширения доступности финансовых услуг, развития клиентского опыта и снижения издержек регулируемых субъектов.

Системы цифровой идентификации могут содействовать расширению доступности финансовых услуг.

11. В настоящем Руководстве отмечен ряд путей и способов, посредством которых использование систем цифровой идентификации может способствовать расширению доступности финансовых услуг. Во-первых, системы цифровой идентификации могут позволить государственным органам использовать более гибкий, выверенный и прогрессивный подход к определению атрибутов, доказательств и процессов для подтверждения «официальной идентичности» – в том числе в целях идентификации и верификации клиентов при приёме на обслуживание таким образом, чтобы это содействовало решению задачи по расширению доступности финансовых услуг. Во-вторых, механизмы и стандарты надежности цифровой идентификации сами по себе обеспечивают некоторую гибкость, которая может использоваться в процессе проверки и подтверждения подлинности личности и аутентификации физических лиц, что, в свою очередь, может быть адаптировано для решения задач по расширению доступности финансовых услуг. И, наконец, при применении риск-ориентированного подхода к проведению надлежащей проверки клиентов, надзорные органы и регулируемые субъекты могут содействовать расширению доступности финансовых услуг, в том числе путём использования систем цифровой идентификации в соответствии с подходом, изложенным ФАТФ в дополнении к Руководству по вопросам НПК и доступности финансовых услуг от 2017 года.

Рекомендации для государственных органов

12. Следует разработать чёткие руководства или нормативные акты, позволяющие субъектам, регулируемым в целях ПОД/ФТ, использовать надёжные независимые системы цифровой идентификации соответствующим образом и на основе оценки рисков. В качестве отправной точки следует проанализировать системы цифровой идентификации, имеющиеся в юрисдикции, и определить, в какой степени они сообразуются с существующими требованиями или руководствами по проведению идентификации, верификации клиентов и постоянной надлежащей проверки (а также связанными с этим требованиями о хранении данных и документов и о возможности полагаться на третьи стороны).

13. Следует оценить, включают ли действующие нормативные акты и руководства по вопросам НПК, выпущенные всеми соответствующими органами, системы цифровой идентификации, и пересмотреть их, при необходимости, с учётом особенностей юрисдикции и существующих систем идентификации. Например, государственным органам следует

рассмотреть возможность разъяснения того, что принятие клиентов на обслуживание без личного контакта может представлять стандартный или даже пониженный риск в части НПК, если для удалённой идентификации/ верификации и аутентификации клиентов используются системы цифровой идентификации, обеспечивающие надлежащие уровни надежности.

14. Следует разработать и утвердить принципы, показатели и/или ориентированные на результат критерии при определении необходимых атрибутов, доказательств и процессов для подтверждения подлинности «официальной идентичности» (т.е. подтверждения личности) в целях проведения НПК. С учётом стремительного развития технологий цифровой идентификации, это поможет продвижению ответственных инноваций и перспективных регулятивных требований.

15. Следует утвердить политику, нормативные акты, а также надзорные и проверочные процедуры, дающие регулируемым субъектам возможность разработать эффективный комплексный «риск-ориентированный» подход, позволяющий использовать потоки данных, технологическую архитектуру и процессы в рамках всех соответствующих мер по управлению общими рисками и рисками, связанными с цифровой идентификацией, отмыванием денег, финансированием терроризма и мошенничеством, для усиления всех служб и подразделений, отвечающих за управление рисками и за их снижение.

16. Следует разработать комплексный многосторонний подход для понимания возможностей и рисков, связанных с цифровой идентификацией и выработкой нормативных актов и руководств по снижению этих рисков. Следует оценить и использовать (там, где это целесообразно) существующие механизмы и стандарты надежности цифровой идентификации, разработанные органами, отвечающими за вопросы идентификации, кибербезопасности/ защиты данных и неприкосновенности личной жизни (в том числе с учётом технологий, безопасности, управления и ресурсного обеспечения), в целях оценки уровней надежности, обеспечиваемых системами цифровой идентификации, для их возможного применения в процессе надлежащей проверки клиентов. В соответствии с Рекомендацией 2 ФАТФ следует обеспечить сотрудничество и взаимодействие с соответствующими государственными органами в целях выработки комплексного скоординированного подхода для понимания и снижения рисков в сфере цифровой идентификации и обеспечения совместимости требований ПОД/ФТ к системам цифровой идентификации с правилами по защите данных и неприкосновенности личной жизни.

17. Государственные органы, отвечающие за вопросы ПОД/ФТ, могли бы рассмотреть возможность создания механизмов в целях развития диалога и сотрудничества с соответствующими участниками частного сектора, в том числе с регулируемыми субъектами и провайдерами услуг цифровой идентификации, для содействия в определении ключевых возможностей и рисков, связанных с идентификацией, и выработки мер для снижения этих рисков. Такие механизмы могли бы включать «регуляторные песочницы», обеспечивающие контролируемую среду для тестирования и проверки того, как системы цифровой идентификации взаимодействуют с национальными нормативно-правовыми актами в сфере ПОД/ФТ. Государственные органы также могли бы рассмотреть возможность создания механизмов для содействия межотраслевому сотрудничеству в целях выявления и устранения уязвимостей существующих систем цифровой идентификации.

18. Следует рассмотреть возможность оказания поддержки и содействия в разработке и внедрении надёжных независимых систем цифровой идентификации путём их проверки и сертификации на соответствие прозрачным механизмам и стандартам надежности цифровой идентификации, или путём назначения экспертных организаций для исполнения этих функций. Если государственные органы сами не осуществляют проверку или сертификацию провайдеров услуг цифровой идентификации, то им рекомендуется оказывать поддержку и содействие в тестировании и сертификации уровней надежности, проводимой соответствующими экспертными организациями[7], с тем, чтобы в юрисдикции имелась надёжная система сертификации. Государственным органам также рекомендуется поддерживать усилия по гармонизации механизмов и стандартов надежности цифровой идентификации для выработки единого понимания того, что представляет собой «надёжная независимая» система цифровой идентификации.

19. Следует применять надлежащие механизмы и технические стандарты надежности цифровой идентификации при разработке и внедрении государственной системы цифровой идентификации. Государственным органам следует давать чёткие разъяснения относительно функционирования национальной системы цифровой идентификации и её уровней надежности.

20. Следует поощрять внедрение гибкого риск-ориентированного подхода к использованию систем цифровой идентификации в целях НПК, содействующего расширению доступности финансовых услуг. Следует рассмотреть возможность выпуска руководства для разъяснения того, как использовать системы цифровой идентификации с разными уровнями надежности для проверки и подтверждения подлинности личности/регистрации и аутентификации в целях проведения поэтапной многоуровневой надлежащей проверки клиентов.

21. Следует отслеживать тенденции и изменения в сфере цифровой идентификации для обмена знаниями и передовым опытом, а также для создания нормативно-правовой базы как на национальном, так и на международном уровне, которая будет содействовать внедрению ответственных инноваций и обеспечит большую гибкость, эффективность и функциональность систем цифровой идентификации как в отдельных странах, так и во всём мире.

Рекомендации для регулируемых субъектов

22. Следует понимать основные составные элементы систем цифровой идентификации, особенно касающиеся проверки, подтверждения подлинности личности и аутентификации, и то, как они сообразуются с элементами требований к НПК (см. Раздел II и Приложение «А»).

23. Следует применять обоснованный риск-ориентированный подход к использованию систем цифровой идентификации в целях НПК, что включает в себя:

[7] Такие экспертные организации по сертификации могут оказывать услуги в конкретной юрисдикции или регионе, или предлагать свои сертификационные услуги на международном уровне.

a. Понимание уровня/уровней надежности, обеспечиваемых системой цифровой идентификации, особенно, в части проверки и подтверждения подлинности личности и аутентификации, и

b. Обеспечение соответствия уровня/уровней надежности рискам ОД/ФТ, связанным с клиентами, продуктами, юрисдикциями, географическим охватом и т.д.

24. Следует рассмотреть, могут ли системы цифровой идентификации с более низкими уровнями надежности быть достаточными для проведения упрощённой надлежащей проверки в ситуациях, характеризующихся низким риском ОД/ФТ. Например, возможно ли применение, в разрешённых случаях, поэтапного подхода к проведению НПК, предусматривающего использование систем цифровой идентификации с разными уровнями надежности, для содействия расширению доступности финансовых услуг.

25. Если в силу внутренней политики или практики деловые отношения или операции без личного контакта всегда рассматриваются, как представляющие высокий риск, следует рассмотреть возможность пересмотра такой политики с учётом того, что меры по идентификации/верификации клиентов, основанные на надёжных независимых системах цифровой идентификации, наряду с имеющимися надлежащими мерами по снижению рисков, могут представлять стандартный или даже пониженный уровень риска.

26. В соответствующих случаях следует использовать меры и процедуры по противодействию мошенничеству и обеспечению кибербезопасности для содействия в проведении проверки подлинности цифровых идентификационных данных и/или аутентификации в целях ПОД/ФТ (в процессе идентификации/верификации клиентов при приёме на обслуживание, а также в процессе осуществления постоянной надлежащей проверки и мониторинга операций). Например, регулируемые субъекты могут использовать встроенные в системы цифровой идентификации элементы и функции, направленные на предупреждение мошенничества (т.е. функции отслеживания событий аутентификации в целях выявления случаев ненадлежащего использования цифровых идентификационных данных для доступа к счетам, в том числе, с использованием утерянных, украденных или проданных учётных цифровых идентификационных данных/аутентификаторов) для встраивания их в свои системы для проведения постоянной надлежащей проверки деловых отношений, а также для мониторинга и обнаружения подозрительных операций и направления государственным органам сообщений о таких операциях.

27. Регулируемым субъектам следует обеспечить, чтобы у них имелся непосредственно доступ или процессы, позволяющие государственным органам получать доступ к соответствующим идентификационным данным и доказательствам или цифровой информации, необходимой для установления и проверки личности физических лиц. Регулируемым субъектам рекомендуется взаимодействовать с органами регулирования и органами, занимающимися выработкой политики, а также с провайдерами услуг цифровой идентификации, для исследования путей и способов эффективного и результативного решения этой задачи в сфере цифровой идентификации.

Рекомендации для провайдеров услуг цифровой идентификации[8]

28. Следует понимать требования ПОД/ФТ в части, касающейся проведения надлежащей проверки клиентов (особенно идентификации/верификации клиентов и постоянной надлежащей проверки), а также другие соответствующие нормативные требования, включая требования о хранении регулируемыми субъектами данных, полученных в процессе НПК.

29. Следует обращаться за тестированием уровней надежности и сертификацией к государственным органам или к назначенной экспертной организации либо, в случае отсутствия такой организации, к другой международно признанной экспертной организации. При наличии возможности, следует участвовать в государственных «регуляторных песочницах» (или в других соответствующих структурах) для оценки уровней надежности, обеспечиваемых системами цифровой идентификации.

30. Следует предоставлять регулируемым субъектам «прозрачную» информацию об уровнях надежности системы цифровой идентификации в части проверки и подтверждения подлинности личности, аутентификации и, в соответствующих случаях, интеграции/функциональной совместимости.

[8] Хотя Стандарты ФАТФ распространяются только на регулируемые субъекты (т.е. на финансовые учреждения, провайдеров услуг в сфере виртуальных активов и установленные нефинансовые предприятия и профессии), настоящее Руководство также актуально в плане справочной информации для провайдеров услуг цифровой идентификации, которые предоставляют услуги регулируемым субъектам (в целях ФАТФ). Однако в конечном итоге за выполнение требований ФАТФ отвечают регулируемые субъекты.

РАЗДЕЛ I: ВВЕДЕНИЕ

31. Группа разработки финансовых мер борьбы с отмыванием денег (ФАТФ) стремиться обеспечить, чтобы международные стандарты в сфере противодействия отмыванию денег/финансированию терроризма (ПОД/ФТ) способствовали внедрению ответственных финансовых инноваций. В этой связи ФАТФ активно поддерживает использование новых технологий в финансовом секторе, которые соответствуют и содействуют реализации стандартов в области ПОД/ФТ и достижению целей расширения доступности финансовых услуг[9].

32. Стремительные темпы инноваций в сфере цифровой идентификации достигли переломной точки. Развитие стандартов, технологий и процессов цифровой идентификации достигло того уровня, когда системы цифровой идентификации стали или могут в скором времени стать доступными в глобальном масштабе. К числу таких технологий относится следующее: разнообразные биометрические технологии; почти повсеместная доступность Интернета и мобильных телефонов (включая стремительное развитие и совершенствование смартфонов с видеокамерами, микрофонами и другими «умными» технологиями); идентификаторы цифровых устройств и связанная с ними информация (например, MAC-адреса и IP-адреса[10], номера мобильных телефонов, SIM-карты, функции геолокации системы глобального позиционирования (GPS)); устройства сканирования с высокой чёткостью (для сканирования идентификационных карт, водительских удостоверений и других документов); системы передачи видеоинформации с высоким разрешением (позволяющие дистанционно устанавливать и проверять личность и получать доказательство того, что человек реально существует и жив); искусственный интеллект/машинное обучение (например, для определения действительности удостоверяющего личность документа, выданного государственными органами); и технология распределённого реестра.

Стремительные темпы инноваций в сфере цифровой идентификации достигли переломной точки ... Системы цифровой идентификации стали или могут в скором времени стать доступными в глобальном масштабе.

Потенциальные преимущества

33. Системы цифровой идентификации, отвечающие высоким стандартам в сфере технологий, организации и управления, имеют большой потенциал для повышения достоверности, безопасности, конфиденциальности и удобства идентификации физических лиц в самых различных ситуациях, связанных в том числе с финансовыми услугами, здравоохранением, услугами электронного правительства, в глобальной экономике цифровой эры. Такие системы цифровой идентификации относятся к системам с повышенными уровнями надежности.

34. Применительно к Стандартам ФАТФ, системы цифровой идентификации, имеющие надлежащую степень надёжности и независимости, могут:

* содействовать идентификации и верификации клиентов при приёме на обслуживание;
* содействовать осуществлению постоянной надлежащей проверки и тщательному анализу операций в процессе поддержания деловых отношений;
* содействовать реализации других мер в целях надлежащей проверки клиентов; и
* содействовать осуществлению мониторинга операций для выявления и направления сообщений о подозрительных операциях, а также содействовать мерам, принимаемым в целях общего управления рисками и предупреждения случаев мошенничества.

[9] См. позицию ФАТФ относительно финансовых и регуляторных технологий (от 3 ноября 2017 года), которая доступна по адресу: www.fatf-gafi.org/publications/fatfgeneral/documents/fatf-position-fintech-regtech.html.

[10] MAC-адреса определяют устройства, а IP-адреса определяют подключения.

35. Они также обладают потенциалом для снижения издержек и повышения эффективности деятельности регулируемых субъектов и позволяют перераспределить ресурсы на выполнение других функций и обязанностей, связанных с ПОД/ФТ.

36. Надёжные независимые[11] системы цифровой идентификации также могут содействовать расширению доступности финансовых услуг, позволяя людям, не имеющим доступ или имеющим ограниченный доступ к финансовым услугам, подтвердить свою «официальную идентичность» (т.е. личность) в различных обстоятельствах, в том числе дистанционно, для получения доступа к регулируемым финансовым услугам. Вовлечение большего количества людей в регулируемый финансовый сектор содействует дальнейшему укреплению механизмов и мер, направленных на противодействие отмыванию денег и финансированию терроризма.

Потенциальные риски

37. Системы цифровой идентификации также представляют риски ОД/ФТ, которые нужно понимать и снижать. Те регулируемые субъекты, которые не делают этого, также не смогут выполнить требования, установленные в Рекомендации 10(а), и требования Стандартов ФАТФ, которые обязывают регулируемых субъектов выявлять, оценивать и снижать риски ОД и ФТ, которые могут возникнуть в связи с использованием новых или разрабатываемых технологий как для новых, так и для уже существующих продуктов[12].

38. Эти риски подробно рассматриваются в Разделе IV. Крупномасштабные системы цифровой идентификации, не обеспечивающие надлежащие уровни надежности, представляют риски для кибербезопасности, позволяя, в том числе, осуществлять кибератаки, нацеленные на выведение из строя больших сегментов финансового сектора или на выведение из строя самих систем цифровой идентификации. Они также представляют серьёзные риски для неприкосновенности личной жизни, риски мошенничества и другие риски, связанные с финансовыми преступлениями, поскольку пробелы в системе кибербезопасности могут привести к крупномасштабным хищениям идентификационных данных и, как результат, к несанкционированному раскрытию информации, позволяющей установить личность[13]. Риски, связанные с управлением, обеспечением безопасности/ сохранности данных и неприкосновенности личной жизни, также влияют на меры ПОД/ФТ. Эти риски различаются применительно к разным элементам системы цифровой идентификации, но могут иметь более разрушительные последствия по сравнению с нарушениями, связанными с традиционными системами идентификации, вследствие потенциального масштаба совершаемых атак. Развитие технологий, а также тщательно проработанные процессы проверки и подтверждения подлинности личности и аутентификации могут содействовать снижению этих рисков, как указано в Разделе IV и рассматривается более подробно в Разделе V.

39. Признавая потенциальные риски и преимущества систем цифровой идентификации, ФАТФ разработала настоящее Руководство для разъяснения того, как системы цифровой идентификации могут использоваться для выполнения конкретных требований ПОД/ФТ, установленных в Стандартах ФАТФ.

Назначение и целевая аудитория

40. Настоящее Руководство предназначено для оказания содействия государственным органам в более чётком понимании того, как функционируют системы цифровой идентификации, и разъяснения того, как они могут использоваться в рамках глобальных стандартов ПОД/ФТ. К числу таких государственных органов относятся: органы, занимающиеся выработкой политики; органы, отвечающие за регулирование, надзор и контроль за деятельностью регулируемых субъектов; органы, отвечающие за обеспечение неприкосно-

[11] Для удобства чтения в некоторых случаях термин «достоверный» используется в качестве синонима термина «надёжный независимый».

[12] Рекомендация 15 (для финансовых учреждений и провайдеров услуг в сфере виртуальных активов) и Рекомендация 22 для УНФПП.

[13] Информация, позволяющая установить личность, включает в себя любую информацию, которая сама по себе или в сочетании с другой информацией позволяет установить личность конкретного человека.

венности личной жизни, защиту данных и кибербезопасность (в части, касающейся их компетенции); а также другие государственные органы, преследующие связанные с этим политические цели (например, расширение доступности финансовых услуг).

41. Настоящее Руководство также предназначено для оказания содействия участникам частного сектора, в том числе регулируемым субъектам и провайдерам услуг цифровой идентификации. Оно также является актуальным для международных организаций, неправительственных организаций (НПО) и других организаций, участвующих в предоставлении и использовании систем цифровой идентификации для оказания финансовых услуг и гуманитарной помощи.

Предмет Руководства

42. Настоящее Руководство посвящено вопросам, касающимся применения Рекомендации 10 (надлежащая проверка клиентов) в контексте использования систем цифровой идентификации в целях идентификации/верификации клиентов при приёме на обслуживание (открытие счётов), предусмотренной в Рекомендации 10(a). В нём также рассматриваются возможности использования цифровой идентификации в целях содействия осуществлению постоянной надлежащей проверки (в том числе мониторинга операций) в соответствии с Рекомендацией 10(d). Кроме того, в Руководстве рассматривается применение Рекомендации 17 (возможность полагаться на третьи стороны) в ситуациях, когда регулируемые субъекты предоставляют системы цифровой идентификации другим регулируемым субъектам для проведения идентификации/верификации клиентов.

43. В соответствии с принципом технологической непредвзятости, требования Рекомендации 11 (хранение данных и документов) в равной степени распространяются на хранение документов как в цифровой, так и в физической (документарной) форме. В практическом плане, при использовании систем цифровой идентификации могут возникнуть актуальные вопросы, касающиеся того, как следует хранить и предоставлять доступ к требуемой информации по результатам НПК с тем, чтобы регулируемые субъекты могли выполнять требования Рекомендации 11. Подходы к хранению данных и документов в контексте цифровой идентификации будут различаться в зависимости от вида и структуры систем цифровой идентификации, видов и правовых обязанностей провайдеров таких систем, а также нормативно-правовой и договорной базы, существующей в юрисдикции. Например, когда государственные органы предоставляют системы цифровой идентификации, они собирают или создают соответствующие удостоверяющие личность свидетельства (первичные исходные документы, информацию и данные) для проверки и подтверждения подлинности личности/регистрации, и в этой связи ожидается, что они будут иметь доступ к этой информации в регулятивных и правоохранительных целях, что соответствует целям Рекомендации 11. Если регулируемые субъекты используют системы цифровой идентификации, предоставленные негосударственными субъектами, то соответствующие удостоверяющие личность свидетельства могут храниться, целиком или частично, провайдерами услуг цифровой идентификации и/или другими субъектами. Кроме того, частные провайдеры услуг цифровой идентификации могут получать/подтверждать некоторые или все базовые идентификационные данные напрямую из цифрового источника (такого как, например, государственные базы данных или реестры предоставления и оплаты коммунальных услуг, ведущиеся компаниями частного сектора). В этом случае, также имеется вероятность того, что цифровые записи с указанием видов доказательств идентичности, используемых в качестве свидетельств в конкретных целях, включая источник данных, дату/время и средства доступа к нему, могут соответствовать требованиям Рекомендации 11. Эти вопросы соответствующим образом решаются государственными органами в рамках нормативно-правовой базы в сфере ПОД/ФТ и цифровой идентификации, а также регулируемыми субъектами в рамках стандартных договорных отношений с агентами и провайдерами финансовых услуг. Поэтому требования, касающиеся хранения данных и документов, и аналогичные требования не рассматриваются более подробно в настоящем Руководстве.

44. В настоящем Руководстве рассматриваются вопросы идентификации клиентов, являющихся физическими лицами. В Руководстве не исследуются вопросы использования систем цифровой идентификации в целях

содействия установлению и проверке личности представителя (представителей) юридического лица в рамках идентификации/верификации клиентов, являющихся юридическими лицами; или в целях реализации других элементов процесса НПК – в частности, в целях установления и проверки личности бенефициарного собственника (собственников) в соответствии с Рекомендацией 10(b) или для понимания и получения информации о цели и предполагаемом характере деловых отношений в соответствии с Рекомендацией 10(c). Однако надёжные независимые системы цифровой идентификации важны для выполнения всех этих функций, связанных с процессом надлежащей проверки клиентов.

45. В настоящем Руководстве рассматриваются системы цифровой идентификации, предоставляемые правительством или от лица правительства[14], а также системы цифровой идентификации, предоставляемые участниками частного сектора. Что касается правительственных систем цифровой идентификации, то в Руководстве рассматриваются, главным образом, системы цифровой идентификации общего назначения (т.е. цифровые идентификационные данные, применимые для официального удостоверения личности во всех или в большинстве целей в юрисдикции). При этом, в Руководстве также рассматриваются системы цифровой идентификации, используемые в узкоспециализированных целях (т.е. цифровые идентификационные данные, применимые для конкретных целей), таких как регистрация в системе социального обеспечения или в других базах данных, когда правительство разрешает их использовать для проведения НПК и предоставляет доступ к ним регулируемым субъектам и провайдерам услуг цифровой идентификации. Дополнительная информация, касающаяся видов систем цифровой идентификации, рассматриваемых в настоящем Руководстве, приведена в Разделе II.

46. В настоящем Руководстве не устанавливаются механизмы надежности или технические стандарты для оценки независимости или надёжности систем цифровой идентификации в части используемых технологий, процессов и архитектуры. Вместо этого, в нём используются технические стандарты и механизмы надежности цифровой идентификации (далее по тексту стандарты и механизмы надежности цифровой идентификации), которые разработаны или разрабатываются другими организациями и в разных юрисдикциях. Разъяснение технических стандартов приведено в Разделе II, а дополнительная информация по этому вопросу содержится в Разделе V и в Приложении «E».

47. Настоящее Руководство включает в себя пять приложений и глоссарий, в которых содержится дополнительная актуальная информация:

* *Приложение A: Описание базовой системы цифровой идентификации и её участников* – в этом Приложении содержится более подробный обзор концепций и понятий, касающихся элементов системы цифровой идентификации, приведённых в Разделе V.

* *Приложение B: Примеры* – в этом Приложении приведены примеры использования цифровых идентификационных данных в разных юрисдикциях, в том числе в целях НПК и получения доступа к финансовым услугам.

* *Приложение C: Принципы идентификации в целях устойчивого развития* – в этом Приложении освещены вопросы управления/отчётности, конфиденциальности и другие оперативные вопросы, решаемые разными юрисдикциями и организациями[15].

* *Приложение D: Организации, устанавливающие технические стандарты и механизмы надежности цифровой идентификации* – в этом Приложении перечислен ряд организаций, устанавливающих стандарты

[14] Система цифровой идентификации предоставляется «от лица правительства» в случае, когда правительство заключает договор или иным образом договаривается или предоставляет право международной организации, такой, например, как Управление Верховного комиссара ООН по делам беженцев, или иному субъекту предоставить и управлять системой цифровой идентификации. В этом случае неправительственный субъект занимает место правительства в части выполнения этих функций.

[15] Эти Принципы были совместно разработаны и одобрены 25 участниками Инициативы устойчивого развития, международными организациями, НПО, ассоциациями частного сектора и правительственными структурами.

(не включая национальные или региональные организации), которые разрабатывают соответствующие механизмы или стандарты надежности цифровой идентификации.

* *Приложение E: Обзор технических стандартов и механизмов надежности цифровой идентификации в США и ЕС* – В этом Приложении приведено, в качестве примера, описание национальных и региональных механизмов надежности цифровой идентификации в Соединённых Штатах Америки и в Европейском союзе.

* *Глоссарий* – в Глоссарии приведено разъяснение терминов, касающихся цифровой идентификации, которые используются в настоящем Руководстве.

РАЗДЕЛ II: ТЕРМИНОЛОГИЯ И КЛЮЧЕВЫЕ ХАРАКТЕРИСТИКИ ЦИФРОВОЙ ИДЕНТИФИКАЦИИ

Что означает «личность» в целях настоящего Руководства?

Понятие «официальной идентичности»

48. Личность – это сложное понятие, имеющее множество значений. В целях ФАТФ, применительно к Рекомендации 10(a) (т.е. в целях «идентификации клиента и проверки личности этого клиента»), «личность» означает официальную идентичность, которая отличается от более широких понятий персональной и социальной идентичности, которые могут быть актуальными для неофициальных целей (например, для нерегулируемого коммерческого или социального взаимодействия между физическими лицами в личном порядке или через Интернет). Настоящее Руководство посвящено использованию систем цифровой идентификации в целях подтверждения подлинности «официальной идентичности» для получения доступа к финансовым услугам.

49. В целях настоящего Руководства[16] **официальная идентичность** является характеристикой конкретного физического лица, которая:

a. основана на характеристиках (атрибутах или идентификаторах) данного физического лица, которые определяют уникальность этого лица в рамках группы населения или определённой ситуации (ситуаций): и

b. признаётся государством в регулятивных и других официальных целях.

Подтверждение официальной идентичности

50. **Подтверждение официальной идентичности,** как правило, зависит от формы обеспечиваемой или предоставляемой правительством регистрации, документации или сертификации (например, свидетельство о рождении, удостоверение личности или учетные цифровые идентификационные данные), которые подтверждают основные атрибуты (например, имя дату и место рождения) для установления и проверки личности.

51. Критерии подтверждения «официальной идентичности» могут различаться в разных юрисдикциях. В рамках осуществления своего права суверенитета национальные правительства определяют необходимые атрибуты, удостоверяющие свидетельства и процедуры для подтверждения «официальной идентичности». При этом такие факторы могут меняться с течением времени. По мере развития технологий, а также культурных понятий и концепций личности государственные органы могут санкционировать использование различных атрибутов. При определении критериев подтверждения «официальной идентичности» государственные органы могут использовать либо жёсткий директивный нормативно-ориентированный подход, либо подход, в основе которого лежат определённые принципы, показатели и/или результаты. При этом второй подход является более гибким. С учётом стремительного развития технологий и стандартов цифровой идентификации, он позволяет юрисдикциям устанавливать перспективные требования в целях подтверждения «официальной идентичности» и продвижения ответственных инноваций.

Использование ориентированного на результат подхода для определения идентификационных атрибутов позволяет юрисдикциям устанавливать перспективные требования в целях подтверждения «официальной идентичности».

52. В ЕС использование общих механизмов надежности позволяет государствам-членам ЕС устанавливать и применять разные национальные требования, например, касающиеся признания различных видов официальных документов и процедур удостоверения личности, существующих в странах ЕС, при условии, что их результаты отвечают требованиям, установленным в Регламенте ЕС об электронной идентификации. В зависимости от обстоятельств, в которых необходимо проверить тот или иной аспект удостоверяющего личность свидетельства, используемые достоверные источники могут существовать во множестве разных форм, таких как, например, реестры, документы, соответствующие органы и т.д. Достоверные источники могут различаться в разных государствах-членах ЕС даже в аналогичных обстоятельствах, но механизм, установленный в Регламенте ЕС об электронной идентификации, предусматривает возможность гармонизации и взаимного признания этих источников. В настоящее время Международная организация по стандартизации (ISO)[17] работает над созданием глобальных стандартов по идентификации физических лиц в целях предоставления финансовых услуг, в том числе в цифровом контексте.

---

[16] Использование ФАТФ этого определения в целях настоящего Руководства никоим образом не ограничивает использование альтернативных определений другими организациями, разрабатывающими и устанавливающими стандарты.

[17] Консультативная группа по стандартам ИСО Технического комитета 68, Рабочая группа 7

53. Во многих странах подтверждение «официальной идентичности» обеспечивается в рамках систем идентификации **общего назначения** (которые иногда также называются базовыми системами идентификации), таких как систем национальных удостоверений личности и систем регистрации актов гражданского состояния. Такие системы обычно предусматривают оформление документарных и/или цифровых учётных данных, которые повсеместно признаются и принимаются государственными органами и частными провайдерами услуг в качестве подтверждения «официальной идентичности» в разных целях. Однако не во всех юрисдикциях имеются такие системы идентификации общего назначения.

54. В юрисдикциях также, как правило, имеются разнообразные системы идентификации **ограниченного назначения** (которые также называются функциональными системами идентификации). Такие системы разрабатываются в целях обеспечения идентификации, аутентификации и авторизации для конкретных услуг или секторов, например, в целях сбора налогов; доступа к конкретным государственным программам социального обеспечения и услугам; предоставления права для голосования; выдачи разрешений на управление автотранспортными средствами; и (в некоторых юрисдикциях) для доступа к финансовым услугам и т.д. Примеры удостоверяющих личность свидетельств и документов, используемых в ограниченных целях, включают в себя: индивидуальные номера налогоплательщиков, водительские удостоверения, паспорта, карты регистрации избирателей, номера социального страхования, идентификационные документы беженцев и т.д. В некоторых случаях, особенно в странах, в которых отсутствуют системы идентификации общего назначения, такие функциональные системы и учётные данные могут также использоваться в целях подтверждения «официальной идентичности».

55. Как правило, свидетельства и документы, удостоверяющие «официальную идентичность», выдаются государственными органами или от их лица. Однако в цифровую эру стали появляться новые модели, в рамках которых цифровые учётные данные, предоставляемые частным сектором или в партнёрстве с частным сектором, признаются государственными органами в качестве официального удостоверения личности в онлайновой среде (например, NemID в Дании), наряду с более традиционными цифровыми удостоверениями, выдаваемыми государственными органами (такими как, например, национальные электронные удостоверения личности).

56. В случае беженцев свидетельства, подтверждающие их личность, могут также предоставляться международно признанными организациями, обладающими такими полномочиями[18]. См. Вставку 8.

Что представляет собой система цифровой идентификации в целях настоящего Руководства?

57. В рамках систем цифровой идентификации используются электронные средства для удостоверения и подтверждения «официальной идентичности» лица в режиме онлайн (в цифровом режиме) и/или при личном присутствии с различными уровнями надежности.

58. В настоящем Руководстве рассматриваются комплексные системы цифровой идентификации (т.е. системы, охватывающие процессы проверки, подтверждения подлинности личности/регистрации и аутентификации). В системах цифровой идентификации могут использоваться разные операционные модели, в них могут быть задействованы разные субъекты, и они могут быть основаны на разных видах технологий, процессов и архитектурных решений. Когда в настоящем Руководстве говорится о системах цифровой идентификации, то речь идёт о комплексной системе, а не о её отдельных составных элементах.

[18] См. Статьи 25 и 27 Конвенции о статусе беженцев от 1951 года и Устав Управления Верховного комиссара ООН по делам беженцев от 1950 года.

59. Не все элементы системы цифровой идентификации непременно являются цифровыми. Некоторые элементы проверки, подтверждения подлинности личности и регистрации могут быть либо цифровыми, либо документарными или сочетать цифровую и документарную форму, но **привязка, выпуск учётных данных, аутентификация и механизмы переноса/интеграции (где применимо) обязательно должны быть цифровыми.** Более подробное описание этих понятий приведено в подразделах ниже.

60. В рамках систем цифровой идентификации цифровые технологии могут использоваться различными способами и путями, что включает в себя, например:

* Использование электронных баз данных, включая распределённые реестры, для получения, подтверждения, хранения и/или управления удостоверениями личности;
* Использование цифровых учётных данных в целях удостоверения личности для доступа к мобильным, онлайновым и оффлайновым приложениям;
* Использование биометрических характеристик для содействия в идентификации и/или аутентификации физических лиц; и
* Использование цифровых интерфейсов прикладного программирования, платформ и протоколов, содействующих идентификации/верификации и удостоверения личности в режиме онлайн.

Каковы ключевые элементы системы цифровой идентификации?

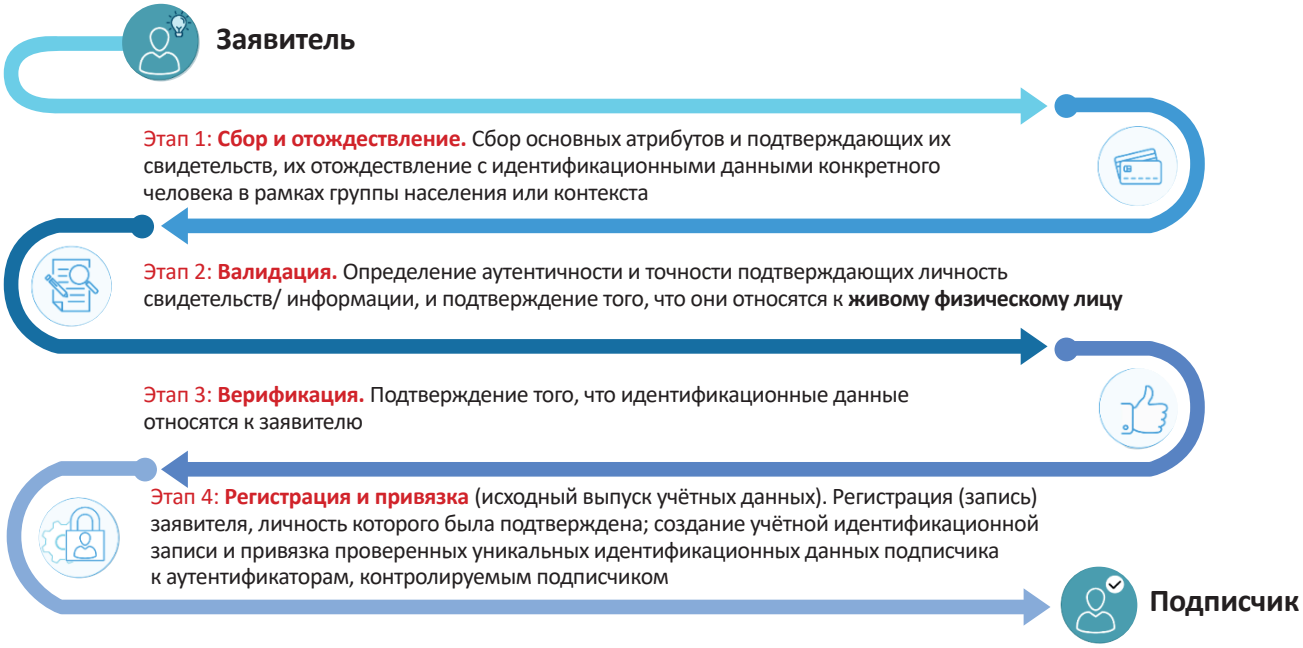
61. Как указано в Руководствах по цифровой идентификации, выпущенных Национальным институтом стандартов и технологий США (NIST), **системы цифровой идентификации** включают в себя два основных элемента и необязательный третий элемент (указано ниже). За обеспечение функционирования составных частей этих элементов могут отвечать разные субъекты, в том числе это может обеспечиваться совместно государственными органами и субъектами частного сектора. Терминология, используемая разными юрисдикциями и организациями, может несколько отличаться, в зависимости от конкретных описываемых систем. Более подробное описание каждого этапа работы системы приведено в ***Приложении «А»: Описание базовой системы цифровой идентификации и её участников.***

Элемент 1: Проверка и подтверждение подлинности личности, регистрация (с первичной привязкой и выпуском учётных данных) *(обязательный элемент)*

62. Этот элемент отвечает на вопрос: ***Кто вы такой?*** Он включает в себя: сбор, валидацию и проверку подтверждающих личность свидетельств и информации о физическом лице; создание учётной идентификационной записи (регистрация); и привязку уникальных идентификационных данных лица к аутентификаторам, принадлежащим или контролируемым этим лицом.

63. Этот элемент прямо и непосредственно связан (пересекается) с требованиями по идентификации/ верификации, установленными в Рекомендации 10(а) (см. Раздел III).

Рисунок 2: Проверка и подтверждение личности, регистрация



Примечание: Данная схема приведена только для наглядности. Этапы проверки, подтверждения подлинности личности и регистрации могут следовать в ином порядке. Цель состоит в идентификации, верификации лица и привязке его личности к аутентификатору. Дополнительное разъяснение ключевых терминов, используемых в этой схеме, приведено в Приложении «А».

64. Некоторые примеры действий, осуществляемых в рамках Элемента 1 (которые приведены исключительно для наглядности), могут включать в себя следующее:

* Сбор: Представление и сбор атрибутов и подтверждающих личность свидетельств либо в личном присутствии, либо в режиме онлайн (например, путём заполнения онлайновой формы, направления фотографии самого себя, загрузки фотографий документов, таких как паспорт, водительское удостоверение и т.д.).

* Валидация: Цифровая или физическая проверка, осуществляемая для того, чтобы удостовериться в аутентичности (подлинности) документа и точности содержащихся в нём данных и сведений (например, проверка защитных свойств, дат истечения сроков действия, а также проверка атрибутов по другим источникам).

* Исключение дубликатов: Определение того, что атрибуты и подтверждающие личность свидетельства относятся к определённому (уникальному) физическому лицу в системе цифровой идентификации (например, путём поиска возможных дублирующих записей, использования систем биометрического распознавания и/или алгоритмов исключения дубликатов).

* Верификация: Привязка физического лица к предоставленным свидетельствам, подтверждающим его личность (например, путём использования биометрических технологий, таких как распознавание черт лица и подтверждение того, что человек является живым).

* Занесение в учётную идентификационную запись и привязка: Создание учётной идентификационной записи, а также создание одного или нескольких аутентификаторов и их привязка к учётной идентификационной записи (например, пароли, генератор одноразовых кодов/ паролей на смартфоне, смарт-карты PKI[19], сертификаты FIDO и т.д.). Это процесс позволяет проводить аутентификацию (см. ниже).

[19] Инфраструктура открытых ключей

Элемент 2: Аутентификация и управление жизненным циклом идентификационных данных (обязательный элемент)

65. Этот элемент отвечает на вопрос: ***Являетесь ли вы лицом, чья личность была установлена и проверена?*** Это включает определение, на основании владения и контроля аутентификаторами, того, что лицо, заявляющее свою личность (принятый на обслуживание клиент или заявитель), является тем лицом, личность которого была подтверждена, и которое было зарегистрировано.

66. Имеется три вида факторов, которые могут использоваться в целях удостоверения личности какого-либо человека (см. Рисунок 3 ниже): (1) факторы владения (что-либо, чем вы обладаете, например, криптографические ключи); (2) факторы знания (что-либо, что вы знаете, например, пароль); и (3) присущие факторы (что-либо, кем вы являетесь, например, биометрические характеристики)[20].

67. В рамках аутентификации могут использоваться различные виды факторов аутентификации, протоколы или процессы. Такие факторы аутентификации характеризуются разными уровнями безопасности – анализ рисков, связанных с аутентификацией, приведён в Разделе V. Одиночный фактор аутентификации, как правило, не считается заслуживающим полного доверия. Процесс удостоверения личности обычно считается более глубоким и надёжным при использовании множества видов факторов аутентификации[21].

[20] Когда в настоящем Руководстве речь идёт о составных элементах аутентификации, то это не то же самое, что «усиленная аутентификация клиентов», предусмотренная в нормативно-правовой базе ЕС. Что является, а что не является применимыми факторами для усиленной аутентификации клиентов в целях Директивы (ЕС) 2015/2366 (Вторая Директива о платёжных услугах), должно оцениваться в соответствии со Второй Директивой о платёжных услугах и Регулятивными техническими стандартами по усиленной аутентификации клиентов и безопасной связи, а не в рамках Руководства ФАТФ.

[21] По мере развития систем цифровой аутентификации это понимание становится более конкретным и детальным. Если процесс аутентификации является активным и постоянным, то надёжность аутентификации иногда оценивается не с точки зрения количества различных факторов аутентификации и их видов, а в плане общей надёжности и достоверности, обусловленной использованием множества источников динамичных цифровых данных о клиентах, включая ожидаемые каналы подключения, данные геолокации, частоту использования, виды использования, IP-адреса и модели поведения, основанные на биомеханической биометрии.

Рисунок 3: Общие факторы аутентификации

Источник: Инициатива «Идентификация в целях Развития» Всемирного банка

Вставка 1: Роль аутентификации в осуществлении надлежащей проверки клиентов и реализации других мер в целях ПОД/ФТ

- После того, как личность человека была подтверждена и человек был зарегистрирован в системе цифровой идентификации, он может использовать учётные данные и аутентификаторы, привязанные к его идентификационным данным, для того, чтобы «предъявить» эти идентификационные данные третьей «полагающейся стороне» (например, регулируемому субъекту). Хотя надёжность проверки, подтверждения личности и регистрации даёт полагающейся стороне определённую степень уверенности в достоверности идентификационных данных (например, то, что такие атрибуты, как имя и возраст, являются правильными и связаны с реальным человеком), процесс аутентификации гарантирует полагающейся стороне, что человек, предоставивший учётные данные, является именно тем, кому они принадлежат, а не вором или самозванцем. В этой связи возможности систем цифровой идентификации подтверждать личность человека являются важной составной частью их функционала и могут использоваться регулируемыми субъектами для идентификации/верификации в рамках НПК при открытии счёта.

- Следует отметить, что «аутентификация» существующих клиентов также является важной мерой для обеспечения безопасности в процессе проведения постоянной надлежащей проверки и санкционирования доступа к счетам. В некоторых случаях для санкционирования доступа к счетам регулируемые субъекты могут использовать те же самые учётные цифровые идентификационные данные и услуги аутентификации, которые они используют при открытии счёта, но это не обязательно. Например, многие регулируемые субъекты предоставляют свои собственные учётные данные/аутентификаторы (например, ПИН-коды и токены для доступа к онлайн счетам) и/или привязывают их к установленным на устройствах аутентификаторам, интегрированным в мобильные телефоны или браузеры (например, используя стандарты FIDO).

68. ***Управление жизненным циклом идентификационных данных*** означает действия, которые необходимо предпринимать в ответ на события, которые могут произойти в течение жизненного цикла идентификационных данных и повлиять на использование, безопасность и надёжность аутентификаторов, например, в случае кражи, утери, несанкционированного дублирования, истечения срока действия и аннулирования **аутентификаторов** и/или **учётных данных.**

Элемент 3: Механизмы переносимости и функциональной совместимости (необязательный элемент)

69. Системы цифровой идентификации могут включать в себя элемент, обеспечивающий переносимость подтверждающих личность свидетельств. «Переносимая идентичность» означает, что учётные цифровые идентификационные данные физического лица могут использоваться для подтверждения его личности («официальной идентичности») в рамках новых клиентских отношений с несвязанными субъектами из частного или государственного сектора, без необходимости с их стороны каждый раз получать и проверять персональные данные и проводить идентификацию/ верификацию клиента. Возможности такого переноса могут поддерживаться различными архитектурными решениями и протоколами цифровой идентификации. В Европе Регламент ЕС об электронной идентификации предусматривает механизм взаимного признания систем цифровой идентификации.

70. Так называемая «интеграция» является одним из способов обеспечения переносимости «официальной идентичности». Интеграция означает использование взаимосвязанной архитектуры и удостоверяющих протоколов для передачи идентификационных данных и аутентификаторов в *рамках объединённых в сеть систем.* Это позволяет обеспечить функциональную совместимость отдельных сетей. В Соединенном Королевстве портал «GOV.UK. Verify» является примером интегрированной системы цифровой идентификации – см. Вставку 16.

Технические стандарты и механизмы надежности цифровой идентификации

71. Механизмы надежности и технические стандарты по обеспечению надёжности технологий, процессов и архитектуры цифровой идентификации разработаны или разрабатываются следующими субъектами:

    * Различными юрисдикциями и наднациональными юрисдикциями (например, Европейским союзом, Канадой и Австралией);

    * Международными или отраслевыми организациями по стандартизации, такими как Международная организация по стандартизации (ISO), Международная электротехническая комиссия (МЭК), альянс «Fast Identity Online Alliance» (FIDO), Организация «OpenID Foundation» (OIDF), Международный союз электросвязи (МСЭ) и Ассоциация «GSMA».

72. Общий обзор этих организаций приведён в ***Приложении D: Организации, устанавливающие технические стандарты и механизмы надежности цифровой идентификации.***

73. В механизмах и стандартах надежности цифровой идентификации, разработанных на данный момент на уровне юрисдикций, используется разное количество и/или разные наименования уровней надежности, но, по своей сути, они в значительной степени схожи. В данное время юрисдикции работают над приведением своих соответствующих технических стандартов цифровой идентификации в соответствие друг с другом для устранения остающихся расхождений. В 2018 году Международная организация по стандартизации выпустила совместно с Международной электротехнической комиссией международный стандарт по проверке, подтверждению личности и регистрации физических лиц (ISO/МЭК 29003:2018). В настоящее время Международная организация по стандартизации пересматривает свой ранее выпущенный стандарт, касающийся механизма надежности аутентификации (ISO/МЭК 29115:2013), и уточняет свое Руководство по управлению рисками (ISO 3100:2018) для его применения в целях снижения рисков, связанных с идентификацией. Кроме того, Международная организация по стандартизации проводит работу по обновлению, систематизации и гармонизации всех других стандартов серии ISO для создания комплексного международного механизма надежности цифровой идентификации.

74. С учётом разрабатываемых стандартов, в настоящем Руководстве приводится много ссылок на Руководства по цифровой идентификации Национального института стандартов и технологий США (NIST) и Регламент ЕС об электронной идентификации. Государственным органам, отвечающим за вопросы ПОД/ФТ, следует тесно взаимодействовать со своими партнёрами в сфере цифровой идентификации и кибербезопасности, а также с другими соответствующими государственными ведомствами для определения подходящих механизмов и стандартов надежности цифровой идентификации.

75. По мере развития технологий, архитектуры и процессов цифровой идентификации потребуется совершенствование самих механизмов надежности и технических стандартов для систем цифровой идентификации, которые, вероятно, будут отставать от развития систем цифровой идентификации. В этой связи государственным органам и участникам частного сектора настоятельно рекомендуется тщательно отслеживать появление новых технологий/процессов цифровой идентификации, обеспечивающих более надёжную проверку и подтверждение подлинности личности или аутентификации. Им также рекомендуется рассматривать механизмы и стандарты в качестве полезного инструмента для оценки, а не использовать существующие повышенные уровни надежности для установления предельных параметров.

РАЗДЕЛ III: СТАНДАРТЫ ФАТФ, КАСАЮЩИЕСЯ НАДЛЕЖАЩЕЙ ПРОВЕРКИ КЛИЕНТОВ

76. Для рассмотрения вопросов, затрагиваемых в данном Разделе, требуется базовое понимание того, как системы цифровой идентификации работают на практике. В этой связи читателям рекомендуется ознакомиться с кратким обзором и описанием основных этапов обобщённой системы цифровой идентификации, которые приведены в Разделе II и Приложении «А». Это необходимо в качестве основы для анализа того, как это относится к Рекомендации 10 и, в частности, к установленным в ней критериям «надёжности и независимости», о чём идёт речь в данном Разделе.

77. Рекомендация 10 требует от юрисдикций установить для регулируемых субъектов обязательство по проведению надлежащей проверки клиентов (НПК). Ниже разъясняется применение требований Рекомендации 10(a) в контексте цифровых систем идентификации. От подотчётных субъектов требуется определить степень и объём необходимых мер НПК, используя риск-ориентированный подход в соответствии с положениями Пояснительных записок к Рекомендации 10 и к Рекомендации 1. В настоящем Разделе также кратко рассматривается то, как надёжные системы цифровой идентификации могут содействовать выполнению других требований ПОД/ФТ, установленных в Рекомендации 10(d).

Требования об идентификации/верификации (при приёме клиентов на обслуживание)

78. При установлении деловых отношений с клиентом (т.е. при приёме клиента на обслуживание) регулируемые субъекты обязаны идентифицировать клиента и проверить его личность, «*используя документы, данные или информацию из надёжных независимых источников*» (Рекомендация 10, подпункт (a)).

Документарная или цифровая форма свидетельства удостоверения личности и процесса подтверждения личности

79. Рекомендация 10 является непредвзятой в плане использования различных технологий. Рекомендация 10(a) разрешает финансовым учреждениям использовать «документы», а также «информацию или данные» при осуществлении идентификации и верификации клиентов. В Рекомендации 10(a) не установлены никакие ограничения в части формы (документарной/бумажной или цифровой) свидетельств, используемых для проверки и подтверждения подлинности личности, т.е. «исходных документов, информации или данных».

80. Более того, хотя в соответствии с Рекомендацией 10(a) финансовые учреждения должны привязывать проверенную личность клиента к конкретному человеку каким-либо «надёжным» способом, никакие положения Стандартов ФАТФ не устанавливают требования относительно того, каким именно образом проверенная личность клиента должна привязываться к конкретному живому человеку в процессе проведения идентификации/верификации при приёме на обслуживание. Таким образом, Рекомендация 10 не устанавливает ограничения на использование систем цифровой идентификации в этих целях. Стандарты ФАТФ оставляют этот вопрос на усмотрение юрисдикций, которые самостоятельно определяют в рамках своего национального законодательства способы и методы проверки и подтверждения подлинности личности («официальной идентичности») в процессе проведения НПК.

«Надёжные независимые» свидетельства, удостоверяющие личность

81. Ключевым условием для определения того, как системы цифровой идентификации могут использоваться в целях идентификации/верификации клиентов, является понимание того, что именно требование Рекомендации 10, касающееся «использования документов, данных или информации из надёжных независимых источников», означает в цифровом контексте. В механизмах и стандартах надежности цифровой идентификации используется термин «гарантия» для описания надёжности системы. Таким образом, уровни надежности являются полезным инструментом для определения того, является ли конкретная система цифровой идентификации «надёжной и независимой» в целях ПОД/ФТ.

82. Ниже рассматривается развитие и изменение действующего требования ФАТФ, касающегося «надёжности и независимости», для лучшего понимания его значения и целей.

83. В исходных 40 Рекомендациях ФАТФ (утверждённых в июле 1990 года) в Рекомендации 12 было установлено требование, согласно которому регулируемые субъекты были обязаны идентифицировать своих клиентов (т.е. устанавливать личность) «на основании официальных или иных надёжных

документов, удостоверяющих личность»[22]. Эта формулировка оставалась неизменной при пересмотре Рекомендаций в июне 1996 года и в июне 2003 года и продолжала оставаться в силе до утверждения нынешней версии Рекомендаций в феврале 2012 года. В 2012 году ФАТФ добавила требование о «верификации (проверке) личности» и требование о том, чтобы удостоверяющие личность свидетельства были «независимыми» в дополнении к тому, что они должны быть «надёжными». Одновременно с этим, изменения, внесённые в 2012 году, предусматривают более гибкий и широкий подход к видам удостоверяющих личность свидетельств – исходные документы, цифровые данные или информация – которые могут использоваться для идентификации/верификации клиентов. Кроме того, было удалено прямое указание на «официальные документы, удостоверяющие личность», которое присутствовало в предыдущих версиях Рекомендаций.

84. В контексте цифровой идентификации требование о том, чтобы цифровые «исходные документы, данные или информация» были «надёжными и независимыми», означает, что в основе системы цифровой идентификации, используемой для проведения НПК, лежат технологии, надлежащее управление, процессы и процедуры, которые обеспечивают надлежащий уровень уверенности в том, что система выдаёт точные результаты. Это означает наличие мер для снижения видов и типов рисков, указанных в Разделе IV.

Риск-ориентированный подход к надлежащей проверке клиентов

Применение риск-ориентированного подхода к реализации мер НПК для содействия достижению целей, касающихся расширения доступности финансовых услуг.

85. Согласно требованиям, установленным в Рекомендации 10, регулируемые субъекты должны использовать риск-ориентированный подход для определения степени применяемых мер НПК, в том числе для идентификации/верификации клиентов. В соответствии с Рекомендацией 10 и Пояснительной запиской к ней регулируемые субъекты обязаны выявлять, оценивать и применять эффективные меры для снижения своих рисков ОД/ФТ (связанных с клиентами, странами или географическими регионами, а также с продуктами, услугами, операциями или каналами поставки). Усиленные меры должны приниматься в ситуациях, характеризующихся повышенным риском, а упрощённые меры могут быть подходящими в случаях, когда установлен низкий риск. ФАТФ опубликовала Руководство для разъяснения того, как юрисдикции/регулируемые субъекты могут принимать меры НПК с использованием риск-ориентированного подхода для содействия достижению целей, касающихся расширения доступности финансовых услуг[23].

86. Как подробно рассматривается в Разделе V, в соответствии с требованиями Рекомендаций 1 и 10 и Пояснительных записок к ним, регулируемые субъекты должны принимать меры НПК, соответствующие виду и уровню рисков ОД/ФТ. В Пояснительной записке к Рекомендации 1

[22] В исходных 40 Рекомендациях ФАТФ (от июля 1990 года) для финансовых учреждений были установлены требования по идентификации клиентов для усиления их роли в противодействии легализации доходов от незаконного оборота наркотиков. В Рекомендации 12 (от 1990 года), в части, касающейся этих требований (выделено курсивом нами, а пунктуация сохранена), было установлено следующее: *Финансовым учреждениям* не следует вести анонимных счетов или счетов, открытых на явно вымышленные имена: *они должны быть обязаны* (в соответствии с законом, нормативным актом, соглашениями между надзорными органами и финансовыми учреждениями или саморегулируемыми договорённостями между финансовыми учреждениями) *идентифицировать, на основании официального или иного надежного документа, удостоверяющего личность,* и регистрировать личность *своих клиентов,* как разовых, так и постоянных, *при установлении деловых отношений или проведении операций (особенно при открытии счетов или сберегательных книжек, заключении фидуциарных сделок, сдачи в аренду сейфовых ячеек, осуществлении операций с наличными деньгами на крупные суммы).*

[23] ФАТФ (2013-2017), «Меры по противодействию отмыванию денег и финансированию терроризма и доступность финансовых услуг – с дополнением, касающимся надлежащей проверки клиентов», Париж, https://www.fatf-gafi.org/fr/publications/inclusionfinanciere/documents/financial-inclusion-cdd-2017.html?hf=10&b=0&s=desc(fatf_releasedate).

подчеркивается, что при оценке риска регулируемые субъекты должны рассмотреть все факторы риска, прежде чем определить уровень общего риска и надлежащую степень мер, направленных на снижение риска. Наряду с Рекомендацией 10 и Пояснительной запиской к ней, в Пояснительной записке к Рекомендации 1 конкретно указано, что регулируемые субъекты могут дифференцировать степень и объем принимаемых мер, в зависимости от вида и уровня рисков, связанных с различными факторами риска (например, в определенной ситуации они могут использовать обычные меры НПК, применяемые при приёме клиентов на обслуживание, но при этом применять усиленные меры НПК при осуществлении постоянного мониторинга, или наоборот).

Деловые отношения и операции без личного контакта

87. ФАТФ использует термины «при личном присутствии» и **«без личного присутствия»** для классификации деловых отношений (включая приём на обслуживание) и операций. В целях ФАТФ взаимодействие при личном присутствии осуществляется в личном присутствии – то есть, это означает, что стороны, участвующие во взаимодействии/операции, находятся в одном и том же «физическом» месте и осуществляют деятельность путём «физического» взаимодействия друг с другом. **Взаимодействие без личного присутствия** осуществляется дистанционно – то есть, это означает, что стороны не находятся в одном и том же «физическом» месте и осуществляют деятельность посредством цифровых или иных физически неосязаемых средств, например, по (электронной) почте или по телефону[24].

88. В Пояснительной записке к Рекомендации 10 «деловые отношения или операции без личного контакта» приведены в качестве *одного из примеров ситуации, потенциально* представляющей повышенный риск при проведении НПК. По своему определению это заявление не требует от соответствующих государственных органов и регулируемых субъектов всегда относить деловые отношения или финансовые операции без личного контакта к категории повышенного риска в целях ПОД/ФТ. Скорее, деловые отношения и операции без личного контакта являются примерами обстоятельств, при которых риск ОД и ФТ может *потенциально* являться повышенным.

89. С учётом развития технологий, архитектуры и процессов цифровой идентификации, а также появления открытых согласованных технических стандартов цифровой идентификации, важно разъяснить, что дистанционная идентификация клиентов и операции без личного контакта, осуществляемые с использованием надёжных независимых систем цифровой идентификации, в которых предусмотрены надлежащие меры по снижению рисков, могут представлять стандартный уровень риска или даже пониженный риск в случае обеспечения повышенных уровней надежности и/или применения надлежащих мер контроля рисков ОД/ФТ таких, как ограничение функциональных возможностей продуктов и других мер, указанных в Пояснительной записке к Рекомендации 10 и в Руководстве ФАТФ по доступности финансовых услуг. (См. также подразделы настоящего Руководства, посвящённые вопросам расширения доступности финансовых услуг, дистанционной проверки, подтверждения личности и регистрации).

[24] Определение взаимодействия при личном присутствии и без личного контакта может различаться в зависимости от национальной нормативно-правовой базы. Например, в некоторых юрисдикциях видеоидентификация считается взаимодействием при личном присутствии.

Постоянная надлежащая проверка деловых отношений

90. Помимо других мер, в соответствии с требованиями Рекомендации 10(d) регулируемые субъекты должны проводить «постоянную надлежащую проверку деловых отношений и тщательный анализ операций, осуществляемых в рамках таких отношений, для того, чтобы убедиться в том, что проводимые операции соответствуют сведениям учреждения о клиенте, его хозяйственной деятельности и характере рисков, в том числе об источнике средств, при необходимости».

91. Как указано в Разделе II выше и более подробно описано в Приложении «А», **аутентификация** проводится с использованием системы цифровой идентификации и обеспечивает уверенность в том, что физическое лицо является именно тем человеком, личность которого была подтверждена, и которому были выданы соответствующие учётные данные. Тем регулируемым субъектам, которые используют системы цифровой идентификации для аутентификации личности своих клиентов в рамках санкционирования доступа к счетам, настоятельно рекомендуется использовать данные, генерируемые в процессе аутентификации, а также другую соответствующую информацию[25] для содействия проведению постоянной надлежащей проверки и мониторинга операций. Сбор такой информации, как правило, осуществляется в целях защиты регулируемых субъектов от мошенничества. Однако, учитывая ускоряющиеся темпы перехода к цифровым финансовым системам и сопутствующее этому расширение использования механизмов аутентификации цифровых идентификационных данных для санкционирования доступа к счетам, эта информация также может оказаться актуальной для целей ПОД/ФТ.

92. Постоянная аутентификация принятых на обслуживание клиентов даёт регулируемым субъектам разумную, основанную на оценке риска, гарантию (т.е. уверенность) в том, что лицо, которое сегодня предоставляет свои идентификационные данные, является тем же самым человеком, который ранее открыл счёт или заключил договор на оказание других финансовых услуг, и, в самом деле, является тем же самым физическим лицом, в отношении которого была проведена «надёжная независимая» идентификация и верификация при приёме на обслуживание. Постоянная цифровая аутентификация личности клиента обеспечивает привязку такого физического лица к осуществляемой им финансовой деятельности. Таким образом, это может дополнительно повысить возможности для проведения полноценной надлежащей проверки на постоянной основе и осуществления мониторинга операций в соответствии с требованиями Рекомендации 10(d).

Требования, касающиеся возможности полагаться на третьи стороны

93. В данном подразделе разъясняется, каким образом субъект, чья деятельность регулируется в целях ПОД/ФТ, может: (1) полагаться на результаты идентификации/верификации, проведённой другим регулируемым субъектом в контексте цифровой идентификации (в рамках требований Рекомендации 17); и (2) выступать в качестве агента другого регулируемого субъекта или в качестве субъекта, которому делегированы полномочия по идентификации/верификации другим регулируемым субъектом (вне рамок требований Рекомендации 17).

[25] Аутентификация является лишь одним из элементов процедуры санкционирования доступа к счёту. Регулируемые субъекты также могут собирать другие дополнительные данные (такие, как данные геолокации, IP-адреса и т.д.) для принятия решений о предоставлении права доступа к счетам.

94. В соответствии с Рекомендацией 17 страны могут позволить регулируемым субъектам[26] полагаться на третьи стороны в части осуществления идентификации/верификации клиентов при приёме на обслуживание[27], при соблюдении следующих условий:

* Третья сторона должна также являться регулируемым субъектом, на которого распространяются требования о проведении надлежащей проверки клиентов в соответствии с Рекомендацией 10, и, в отношении которого должен осуществляться надзор или контроль на предмет соблюдения установленных требований и обязательств.

* Регулируемый субъект должен:

  ○ Незамедлительно получать необходимую информацию, касающуюся идентификации/ верификации клиентов;

  ○ Принимать надлежащие меры для того, чтобы иметь возможность без задержки по запросу получить от третьей стороны копии идентификационных данных и другую соответствующую документацию, попадающую под действие требований Рекомендации 10(a);

  ○ Убедиться в том, что в отношении третьей стороны осуществляется регулирование, надзор или контроль, и что такая третья сторона принимает меры по выполнению требований, касающихся НПК и хранения данных и документов, в соответствии с Рекомендациями 10 и 11; и

  ○ Учитывать информацию об уровне страновых рисков при определении стран, в которых может находиться третья сторона, отвечающая вышеуказанным условиям.

95. В случае разрешения полагаться на третьи стороны, конечная ответственность за меры НПК остается лежать на регулируемом субъекте, полагающемся на третью сторону.

Возможность полагаться на третьи стороны в контексте цифровой идентификации (в случаях, когда регулируемые субъекты также выступают в качестве провайдеров услуг цифровой идентификации)

96. В тех случаях, когда это разрешено в юрисдикции, регулируемый субъект может полагаться на другого субъекта, отвечающего вышеперечисленным критериям, в части проведения идентификации/верификации клиентов с использованием системы цифровой идентификации при приёме их на обслуживание, при условии, что система цифровой идентификации такой третьей стороны позволяет полагающемуся субъекту:

* Незамедлительно получать необходимую информацию, касающуюся личности клиента (включая уровни надежности (доверия), где применимо). Например, система цифровой идентификации может дать потенциальному клиенту возможность заявить свою личность полагающемуся регулируемому субъекту и позволить третьей стороне подтверждать личность такого человека и предоставить сведения, такие как имя и дата рождения этого человека, присвоенный государством уникальный идентификационный номер или иные атрибуты, требуемые для подтверждения «официальной идентичности» в целях установления деловых отношений в юрисдикции.

---

[26] В Рекомендации 22 установлено, что требования, касающиеся возможности полагаться на третьи стороны, установленные в Рекомендации 17, распространяются на УНФПП.

[27] Рекомендация 17 позволяет полагаться на третьи стороны в части реализации мер НПК, определённых в подпунктах (a)-(c) Рекомендации 10, но не даёт право полагаться на третьи стороны для осуществления постоянной надлежащей проверки деловых отношений. В настоящем Руководстве рассматриваются положения Рекомендации 17 только в части, касающейся требований об идентификации/верификации клиентов, установленных в Рекомендации 10(a).

* Принимать надлежащие меры для того, чтобы иметь возможность без задержки по запросу получать имеющиеся копии или другие соответствующие формы доступа к удостоверяющим личность свидетельствам (документам, данным и другой соответствующей информации), относящимся к требованиям Рекомендации 10(a). Например, полагающийся субъект может принять соответствующие меры для того, чтобы: (1) убедиться в том, что в рамках проверки, подтверждения подлинности личности и регистрации третья сторона создала учётную цифровую идентификационную запись идентифицированного лица, в которой содержатся надлежащие подтверждения атрибутов и другие идентификационные данные и сведения; и (2) убедиться в том, что порядок и процедура аутентификации, проводимой третьей стороной, позволяет ей безотлагательно предоставлять эту информацию полагающейся стороне по её запросу.

Регулируемые субъекты, выступающие в качестве провайдеров услуг цифровой идентификации вне рамок требований Рекомендации 17

97. Те регулируемые субъекты, которые разработали свои собственные системы цифровой идентификации, могут стать провайдерами услуг цифровой идентификации, выступая в качестве агентов или третьих сторон для других регулируемых субъектов. В тех случаях, когда это разрешено, это будет включать в себя делегирование полномочий на осуществление идентификации/ верификации клиентов при приёме на обслуживание, а также на проведение аутентификации клиентов. В этих обстоятельствах требования Рекомендации 17, касающиеся возможности полагаться на третьи стороны, не будут действовать, поскольку Рекомендация 17 не охватывает отношения аутсорсинга или агентские отношения.

98. Как и другие провайдеры услуг цифровой идентификации, выступающие в качестве агентов или третьих сторон для других регулируемых субъектов, регулируемые субъекты, действующие в качестве провайдеров услуг цифровой идентификации, будут использовать свои системы цифровой идентификации для осуществления идентификации/верификации (и аутентификации) клиентов от лица регулируемых субъектов, делегировавших им такие полномочия. Кроме того, как и другие провайдеры услуг цифровой идентификации, они могут обращаться за сертификацией своих систем в соответствии с действующими в их юрисдикциях нормативно-правовыми актами, регулирующими вопросы государственной проверки и сертификации, если такие акты имеются, либо обращаться за проверкой и сертификацией своих систем к авторитетным сертифицирующим организациям из частного сектора.

99. В любом случае, будучи поручителем, установленный субъект будет продолжать отвечать за проведение *эффективной* идентификации/верификации клиентов и их *эффективной* аутентификации с использованием системы цифровой идентификации, предоставленной провайдером услуг цифровой идентификации, и ему потребуется применять риск-ориентированный подход к использованию систем цифровой идентификации для идентификации/верификации и аутентификации клиентов, как указано в Разделе V.

РАЗДЕЛ IV: ПРЕИМУЩЕСТВА И РИСКИ ИСПОЛЬЗОВАНИЯ СИСТЕМ ЦИФРОВОЙ ИДЕНТИФИКАЦИИ В ЦЕЛЯХ ОБЕСПЕЧЕНИЯ ВЫПОЛНЕНИЯ ТРЕБОВАНИЙ ПОД/ФТ И СОПУТСТВУЮЩИЕ ВОПРОСЫ

100. В данном Разделе рассматриваются некоторые потенциальные преимущества, которые системы цифровой идентификации дают регулируемым субъектам, их клиентам и государственным органам. В нём также рассматриваются некоторые потенциальные риски, представляемые системами цифровой идентификации, которые необходимо выявлять, понимать и контролировать, а также принимать надлежащие меры для управления или снижения этих рисков. Такие преимущества и риски относятся как к реализации мер контроля в целях ПОД/ФТ, так и к осуществлению мер, направленных на расширение доступности финансовых услуг.

101. Данный Раздел предназначен для повышения осведомлённости заинтересованных сторон о потенциальных рисках, присущих технологиям цифровой идентификации, с тем, чтобы они могли предупреждать или эффективно управлять этими рисками, применяя при этом риск-ориентированный подход, как указано в Разделе V. Приведённый ниже анализ рисков никоим образом не направлен на воспрепятствование использованию надёжных независимых систем цифровой идентификации – то есть систем, обеспечивающих надлежащие уровни надежности (т.е. соответствующих государственным нормативам и техническим стандартам), и позволяющих надлежащим образом снижать потенциальные риски. Он также не подразумевает, что применение систем цифровой идентификации, особенно в целях идентификации/верификации клиентов, непременно обусловливает большую степень уязвимости в плане их использования в незаконных целях, нежели традиционные методы документарной идентификации и проверки личности.

102. В данном Разделе также отмечен ряд более широких проблем, представляемых системами цифровой идентификации. Реагирование на эти проблемы, как правило, не относится к прямой компетенции государственных органов, отвечающих за вопросы ПОД/ФТ, но эти проблемы могут оказывать косвенное влияние на усилия и меры, принимаемые в целях противодействия отмыванию денег и финансированию терроризма.

103. Хотя в данном Разделе и приведён общий обзор некоторых рисков и проблем, именно механизмы и стандарты надежности цифровой идентификации обеспечивают основу для оценки мер по снижению рисков, заложенных в системы цифровой идентификации. В этой связи юрисдикциям рекомендуется проанализировать такие стандарты, касающиеся более широкого спектра существующих рисков (связанных с технологиями и с другими вопросами, касающимися организации и управления), и определить способы и методы снижения этих рисков.

Потенциальные преимущества систем цифровой идентификации

Усиление надлежащей проверки клиентов

104. Системы цифровой идентификации обладают потенциалом для повышения надёжности, безопасности, конфиденциальности, удобства и эффективности идентификации физических лиц в процессе предоставления финансовых услуг, что идёт на пользу клиентам и регулируемым субъектам, а также способствуют укреплению целостности финансового сектора. Как указано ниже, надёжные независимые системы цифровой идентификации могут принести значительную пользу в плане повышения надёжности идентификации/верификации клиентов при приёме на обслуживание и аутентификации личности клиентов при санкционировании доступа к счетам. Более того, точная идентификация клиентов может обеспечить эффективную реализацию других мер НПК, в том числе проведение эффективной постоянной надлежащей проверки деловых отношений и осуществление мониторинга операций.

Минимизация слабых мест в ручных мерах контроля

105. Традиционно документарные методы проведения идентификации/верификации клиентов в значительной степени основывались на ручных мерах контроля – например, сравнение фотографии в официальном документе, удостоверяющем личность, с человеком, обратившимся с просьбой открыть счёт, и суждение о том, является ли документ подлинным. Однако у сотрудников, непосредственно обслуживающих клиентов, может не иметься инструментов, технологий, подготовки, навыков и опыта для надёжного выявления поддельных, видоизменённых или краденых документов.

106. Применение надёжных независимых систем цифровой идентификации может потенциально снизить возможность человеческой ошибки в процессе установления и проверки личности человека.

*Во - первых, когда элемент системы цифровой идентификации, касающийся проверки и подтверждения личности, проводится при личном присутствии[28] и основывается на человеческом суждении, этот процесс обычно осуществляется специалистами, имеющими доступ к передовым техническим инструментам для выявления поддельных и краденых документов, удостоверяющих личность. Например, при дистанционной проверке и подтверждении подлинности личности (по крайней мере при повышенных уровнях надежности), как правило, применяются всё более современные и эффективные технологии цифровой идентификации для определения того, что документарное удостоверение личности является подлинным, а не поддельным, а также используются дополнительные данные и сведения, помогающие надёжно подтвердить личность человека[29].

[28] Как указано в Разделе II и Приложении «А», в рамках системы цифровой идентификации проверка и подтверждение личности являются одним элементом, который может иметь место при личном присутствии (т.е. такая проверка необязательно должна проводиться дистанционно для того, чтобы считаться элементом системы цифровой идентификации).

[29] В настоящее время может оказаться затруднительно или вообще невозможно дистанционно проверить и подтвердить достоверность защитных функций, которые считываются только в ультрафиолетовом свете или являются элементами структуры документа, такие как, например, защитные ныряющие нити, водяные знаки или сплошная перфорация страниц, но большинство идентификационных документов обладают надежными защитными функциями, которые можно эффективно проверять дистанционно.

*Во - вторых, элемент системы цифровой идентификации, касающийся аутентификации, в значительной степени снижает роль человеческого суждения при определении того, что клиенты являются именно теми людьми, кем они представляются. Системы цифровой идентификации с многофакторной аутентификацией и защищёнными процессами могут оказаться неизменно надёжными при определении того, что лицо, желающее открыть счёт или получить доступ к счёту, на самом деле является тем человеком, которому были изначально выданы идентификационные учётные данные.

Повышение функциональных возможностей для клиентов и снижение издержек

107. Надёжные независимые системы цифровой идентификации могут также обеспечить более эффективные и удобные возможности для потенциальных клиентов при приёме на обслуживание, а также впоследствии для уже принятых на обслуживание клиентов при получении ими доступа к своим счетам. Приемлемость и удобство для клиентов являются важными движущими факторами для обработки заявлений, осуществления операций и удержания клиентов. Удобство использования для клиентов, наряду с потенциальным повышением эффективности для регулируемых субъектов, может способствовать снижению затрат и издержек при приёме на обслуживание. В одном отчёте отмечено, что регулируемые субъекты, которые используют системы цифровой идентификации, могут почти на 90 процентов снизить издержки, связанные с приёмом клиентов на обслуживание, благодаря тому, что время на идентификацию/верификацию и на другие меры НПК сокращается с дней или недель до нескольких минут[30]. Такое снижение затрат и издержек может позволить регулируемым субъектам перераспределить ресурсы, выделяемые на обеспечение соблюдения установленных требований НПК, а также на исполнение других комплаенс функций в сфере ПОД/ФТ. Это может также содействовать расширению охвата финансовыми услугами тех слоёв населения, которые не имеют или имеют ограниченный доступ к финансовому обслуживанию, благодаря снижению затрат, связанных с приёмом на обслуживание.

Мониторинг операций

108. Как отмечено выше, надёжная цифровая аутентификация личности клиентов для регулярного предоставления им доступа к счетам может содействовать выявлению подозрительных операций и направлению сообщений о таких операциях. Это обусловлено тем, что такая цифровая аутентификация помогает регулируемому субъекту установить, что человек, получающий доступ к счёту и осуществляющий операции, является тем же самым лицом, которое получало доступ к счёту ранее, и на самом деле является идентифицированным/верифицированным клиентом, которому принадлежит счёт. Кроме того, в зависимости от операционной модели и других факторов, таких как согласие пользователей и законодательство о защите данных/конфиденциальности, цифровая аутентификация личности в целях санкционирования доступа к счёту может позволить регулируемым субъектам получать дополнительную информацию, такую как данные геолокации, IP-адреса или идентификационные номера цифровых устройств, используемых для осуществления операций. Эти сведения могут помочь регулируемым субъектам лучше понять поведение клиента для определения того, когда его финансовые операции выглядят необычными или подозрительными, а также могут содействовать правоохранительным органам в расследовании преступлений. Например, дополнительные сведения, получаемые регулируемыми субъектами с помощью разных средств и каналов (включая Интернет и мобильные телефоны) в соответствии с местными нормативно-законодательными актами, в том числе в соответствии с правилами о защите данных и неприкосновенности личной жизни, могут оказаться весьма полезными для определения того, кто контролирует счёт; выяснения того, контролирует ли это лицо другие счета; и установления сети физических и юридических лиц, участвовавших в финансовых операциях, проведённых через эти счета.

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

Расширение доступности финансовых услуг

109. Стремительная цифровизация финансовых услуг существенно повысила роль надёжных независимых систем цифровой идентификации в целях расширения доступа к финансовым услугам, особенно в развивающихся странах[31], где появляющиеся системы цифровой идентификации и цифровые финансовые услуги являются определяющими факторами, способствующими охвату финансовыми услугами всех слоёв населения[32]. Разработка гибких ориентированных на результат механизмов и стандартов надежности цифровой идентификации может позволить финансово изолированным людям, у которых нет официальных удостоверяющих личность документов, таких как паспорта и водительские удостоверения, получить цифровое удостоверение в рамках пониженного уровня надежности (требующего менее надёжные удостоверяющие личность свидетельства и менее жёсткой проверки) и использовать его для получения доступа к финансовым услугам в соответствующих ситуациях, представляющих пониженный риск. Механизмы и стандарты надежности идентификации также позволяют людям, не имеющим доступ к финансовым услугам, использовать альтернативные свидетельства своей личности (например, доверенных поручителей, чье поручительство является своеобразной формой удостоверения личности) для получения цифрового удостоверения. Кроме того, системы цифровой идентификации могут использоваться для предоставления доступа к финансовым услугам населению в удалённых районах путём обеспечения надёжной проверки и подтверждения личности/регистрации без личного контакта в целях идентификации/верификации таких клиентов. Эти вопросы рассматриваются более подробно в подразделе ниже, посвящённому вопросам, касающимся расширения доступности финансовых услуг.

110. В развивающихся странах государственные выплаты населению, включая переводы социальных пособий (например, переводы денежных пособий при соблюдении определённых условий, пособий на детей и студенческих стипендий), выплаты государственной заработной платы, пенсий и возврат переплаченных налогов, а также коммерческие операции и розничные платежи потребителей всё в большей степени осуществляются в цифровой форме. В контексте гуманитарной деятельности жизненно необходимая помощь также всё в больших масштабах оказывается путём цифрового перевода наличных денег. Для всей этой деятельности требуется доступ к счетам для осуществления соответствующих операций и платежей, и системы цифровой идентификации могут содействовать обеспечению такого доступа.

111. Использование надёжных независимых систем цифровой идентификации может снизить издержки, связанные с НПК, и предоставить гораздо большему количеству людей, не имеющих или имеющих ограниченный доступ к финансовому обслуживанию, возможность использовать регулируемые финансовые услуги. (См. Вставку 4, в которой рассматривается уникальный идентификационный номер (Aadhaar), используемый в Индии, и Вставку 5, в которой описан Национальный реестр удостоверений личности и актов гражданского состояния в Перу). Всё это содействует охвату финансовыми услугами всех слоёв населения и, вместе с тем, расширяет охват и повышает эффективность режимов ПОД/ФТ.

---

[31] Исследование, посвящённое глобальному охвату населения финансовыми услугами (Global Findex Survey), проведённое в 2017 году, показало, что 26 процентов населения, не имеющего доступа к банковскому обслуживанию в странах с низким уровнем доходов, указали отсутствие официальных документов, удостоверяющих личность, в качестве основного препятствия, не дающего им возможность получить доступ к финансовым услугам.

[32] ФАТФ (2013-2017), «Меры по противодействию отмыванию денег и финансированию терроризма и доступность финансовых услуг – с дополнением, касающимся надлежащей проверки клиентов», Париж, http://www.fatf-gafi.org/publications/financialinclusion/documents/financial-inclusion-cdd-2017.html

Риски и затруднения, представляемые системами цифровой идентификации

112. В настоящем Руководстве рассматриваются вопросы применения систем цифровой идентификации для осуществления некоторых элементов надлежащей проверки клиентов, а не использование традиционных систем документарного удостоверения личности. При этом рассматриваемые ниже риски не предполагают, что риски систем цифровой идентификации перевешивают их преимущества, или, что системы цифровой идентификации представляют в целом большие риски, нежели традиционные системы документарного удостоверения личности.

113. Как и любые другие системы идентификации, надёжность систем цифровой идентификации зависит от надёжности документов, процессов, технологий и мер безопасности, используемых для проверки и подтверждения личности, регистрации, аутентификации и постоянного управления идентификационными данными. Например, надёжность как систем документарного удостоверения личности, так и систем цифровой идентификации может быть снижена вследствие хищения идентификационных данных или использования исходных документов, которые можно легко подделать или видоизменить. Вероятность некоторых видов мошенничества может быть более низкой в случае взаимодействия при личном присутствии или при осуществлении процессов, требующих человеческого вмешательства. Например, «массовые мошеннические атаки» с большей вероятностью будут осуществляться дистанционно. Хотя системы цифровой идентификации обеспечивают определённые элементы безопасности, например, надёжную аутентификацию, что позволяет снять некоторые проблемы, возникающие в случае использования «бумажных» систем, они также повышают некоторые риски, такие как, например, риски, связанные с утерей данных, искажением данных или незаконным использованием данных вследствие несанкционированного доступа.

114. Системы цифровой идентификации представляют различные технические проблемы и риски, поскольку они часто связаны с проверкой/подтверждением личности и аутентификацией людей по открытым сетям связи (по Интернету). По этой причине процессы и технологии, используемые в системах цифровой идентификации, предоставляют массу возможностей для осуществления кибератак в процессе взаимодействия между сторонами (провайдером идентификационных услуг, клиентом и полагающейся стороной). Без тщательного учёта соответствующих факторов риска, а также без реализации надлежащих технологических мер безопасности и эффективных мер управления и отчётности, направленных на устранение этих рисков, преступники, лица, занимающиеся отмыванием денег, и другие злоумышленники могут незаконным образом использовать системы цифровой идентификации для создания поддельных идентификационных данных или воспользоваться (в результате хакерских или спуфинг-атак) аутентификаторами, привязанными к законным идентификационным данным.

115. Механизмы и стандарты надежности цифровой идентификации являются ключевыми инструментами для выявления и оценки некоторых из этих рисков и их снижения с помощью технологий и процессов цифровой идентификации, обеспечивающих надлежащую гарантию каждого компонента цифровой идентификации[33]. Ниже рассматриваются риски, связанные с системами цифровой идентификации, которые *не являются* достаточно надёжными в части механизмов управления рисками, установленных в нормативах и стандартах надежности цифровой идентификации. В подразделах ниже также затрагиваются более широкие проблемы, касающиеся совместимости, кибербезопасности и конфиденциальности в цифровом пространстве, которые могут повлиять на целостность или доступность использования систем цифровой идентификации в целях проведения надлежащей проверки клиентов.

[33] В Приложении «Е» содержится более подробное описание уровней гарантии идентификации (IAL); уровней гарантии аутентификации (AAL); и уровней гарантии интеграции (FAL), используемых для оценки и снижения рисков на этих основных этапах.

116. Ниже рассматриваются риски, связанные как с проверкой и подтверждением личности/ регистрацией, так и риски, связанные с аутентификацией. Риски на этапе проверки и подтверждения личности могут привести к появлению «фальшивых» цифровых идентификационных данных (т.е., которые были получены обманным путём в результате совершения злоумышленных действий), которые могут использоваться для содействия незаконной деятельности. Снижение этих рисков обеспечивается за счёт надлежащего уровня надежности идентификации. При этом риски, связанные с проверкой и подтверждением личности, отличаются от рисков, связанных с аутентификацией, при которых имеет место раскрытие законно выданного цифрового удостоверения, а связанные с ним учётные данные или аутентификаторы находятся во владении или под контролем неправомочного лица. Снижение этих рисков обеспечивается за счёт надлежащего уровня надежности аутентификации.

Риски, связанные с проверкой и подтверждением личности и регистрацией

117. На этапе регистрации имеются два основных источника угроз: (1) кибератаки и нарушения в системе безопасности, которые приводят к раскрытию информации, позволяющей установить личность, и предоставлению фальшивых доказательств либо в результате хищения идентификационных данных реального человека (имперсонации), либо создания синтетических идентификационных данных; и (2) раскрытие или нарушение, допущенное провайдером идентификационных услуг, или несанкционированное раскрытие более широкой инфраструктуры цифровой идентификации. В данном подразделе рассматривается первая категория угроз, поскольку снижение угроз, связанных с раскрытием/нарушениями со стороны провайдеров идентификационных услуг, кибербезопасностью и более широкой инфраструктурой, непосредственно предусмотрено в рамках более широких требований, касающихся управления/ организации, установленных в правовых механизмах и стандартах надежности цифровой идентификации, а также в рамках традиционных мер обеспечения компьютерной безопасности (например, касающихся защиты от несанкционированного проникновения, хранения записей, проведения независимых аудитов), которые выходят за рамки настоящего Руководства.

Риски, связанные с имперсонацией и созданием синтетических идентификационных данных (включая кибератаки, нарушения в системе защиты данных и/или в системе безопасности)

118. В определённом отношении риски, связанные с предоставлением фальшивых доказательств (которые либо украдены, либо подделаны) в системах цифровой идентификации, могут проявляться в гораздо больших масштабах[34]. Имперсонация означает ситуацию, когда какое-либо лицо выдает себя за обладателя идентификационных данных другого человека либо с использованием украденного документа кого-то с похожей внешностью, либо в сочетании с использованием фальшивого или поддельного удостоверения личности (например, замена фотографии в паспорте на изображение самозванца). **Синтетические идентификационные данные** создаются преступниками путем объединения реальной (обычно украденной) и поддельной информации для создания новой (синтетической) идентификационной информации, которую можно использовать для открытия мошеннических счетов и совершения мошеннических покупок. В отличие от имперсонации, преступник притворяется тем, кого не существует в реальном мире, а не маскируется под обладателя существующих идентификационных данных. Например, преступные группировки могут совершать хищения персональных и создавать большое количество синтетических цифровых идентификаци-

[34] В результате поиска «поддельных удостоверяющих личность документов» в Интернете были обнаружены сотни сайтов, предлагающих поддельные водительские удостоверения, паспорта, свидетельства о рождении, иммиграционные документы и другие официальные документы, которые очень сложно отличить от законно выдаваемых документов.

онных данных, которые частично основаны на атрибутах идентификационных данных реальных людей, которые были похищены в ходе осуществления операций в режиме онлайн или в результате взлома баз данных в Интернете, и частично основаны на полностью сфабрикованной информации. Синтетические идентификационные данные могут использоваться для получения кредитных карт или онлайновых кредитов с последующим снятием средств, после чего соответствующие счета больше не используются. По мнению экспертов в области цифровой идентификации, использование синтетических идентификационных данных представляет наибольший риск на этапе проверки и подтверждения подлинности личности и регистрации с использованием систем цифровой идентификации в США[35].

119. Для наглядности в приведённой ниже Таблице указаны эти риски и представлены стратегии снижения угроз для процесса проверки и подтверждения личности и регистрации, предусмотренные в Руководствах Национального института стандартов и технологий США (NIST).

Таблица 1: Национальный институт стандартов и технологий США – стратегии снижения рисков, связанных с проверкой и подтверждением личности/регистрацией

Виды рисков	Описание	Возможные стратегии снижения рисков
Поддельные удостоверяющие личность свидетельства и документы	Заявитель представляется под другим именем, используя поддельное водительское удостоверение	Провайдер идентификационных услуг (провайдер учётных данных) должен проверить подлинность физических элементов защиты в предъявленном документе Провайдер идентификационных услуг (провайдер учётных данных) должен проверить подлинность личных данных, содержащихся в предъявленном документе, у органа, выдавшего этот документ, или из другого достоверного источника
Мошенническое использование идентификационных данных другого человека	Заявитель использует паспорт, имеющий отношение к другому человеку	Провайдер идентификационных услуг (провайдер учётных данных) должен проверить удостоверяющий личность документ и биометрические данные заявителя на основании информации, полученной от органа, выдавшего документ, или из другого достоверного источника

Источник: Руководство NIST 800-63A

[35] Встреча проектной группы ФАТФ с экспертами в области цифровой идентификации, состоявшаяся в сентябре 2019 года

Риски, связанные с аутентификацией и управлением жизненным циклом идентификационных данных

120. Уязвимости, связанные с видами и количеством различных факторов аутентификации, могут привести к возникновению не выявленных и нежелательных рисков, которые могут позволить злоумышленникам предъявить законные идентификационные данные другого человека (например, клиента) полагающейся стороне для открытия счёта или получения несанкционированного доступа к продуктам, услугам и данным.

121. Ниже приведены, исключительно в качестве примера, некоторые из таких уязвимостей:

* Атака с подстановкой учётных данных (credential stuffing) (также называемая повторным воспроизведением утечки (breach replay) или очисткой списка (list cleaning)): Вид кибератаки, при которой украденные учётные данные (часто из-за утечки данных) проверяются на совпадения в других системах. Этот тип атаки на учётную запись может быть успешным, если жертва использовала этот же пароль (который был украден при утечке данных) для другой учетной записи.

* Фишинг: Мошенническая попытка сбора учётных данных не подозревающих об этом жертв с использованием методов социальной инженерии, таких как обманные электронные письма, телефонные звонки, текстовые сообщения или Интернет-сайты. Например, преступник пытается обманным путём заставить свою жертву указать имена, пароли, государственные идентификационные номера или учётные данные для, казалось бы, заслуживающего доверия источника.

* Атака посредника или перехват учётных данных: Попытка достичь ту же самую цель, что и в случае фишинга, или это может быть инструментом фишинга, но данные похищаются путем перехвата сообщений между жертвой и провайдером услуг.

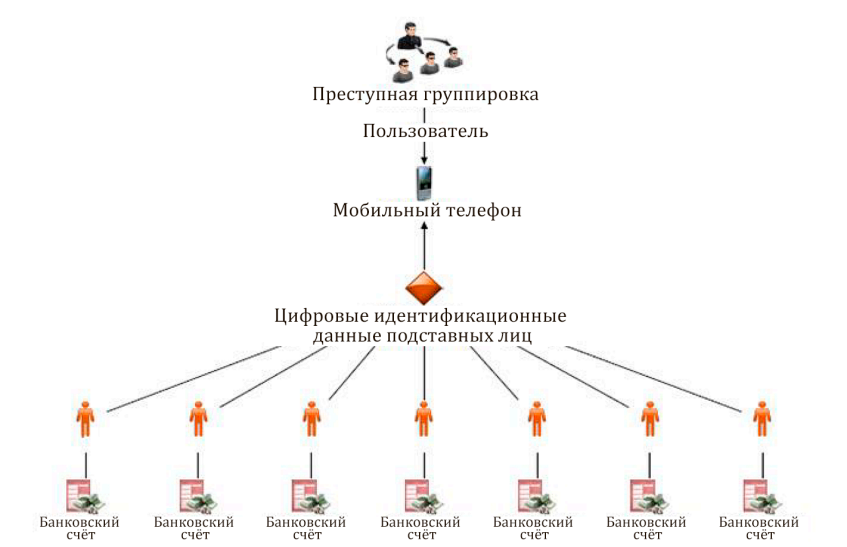
* Перехват и воспроизведение ПИН-кода: Это включает в себя перехват ПИН-кода, введенного на клавиатуре ПК, с помощью перехватчика данных ввода и незаметно для пользователя, а также использование перехваченного ПИН-кода, когда смарт-карта вставляется в считывающее устройство, для доступа к услугам.

122. Большинство уязвимостей, связанных с аутентификацией, используются злоумышленниками таким образом, что владельцы идентификационных данных даже не подозревают об этом, но такое незаконное использование может также иметь место при соучастии подписчиков или провайдеров идентификационных услуг. Например, совместно используемые аутентификаторы, такие как пароли, могут похищаться и использоваться злоумышленниками, но также могут преднамеренно раскрываться владельцами учётных данных в незаконных целях.

123. Например, преступные организации могут покупать цифровые учётные идентификационные данные у физических лиц, что позволяет им получать доступ к счетам этих лиц, открытых в регулируемых учреждениях, превращая, таким образом, этих лиц в «цифровых мулов». Такие лица могут уже иметь открытый счёт либо согласиться открыть его в рамках продажи своих учётных идентификационных данных (см. пример ниже).

Вставка 2: Незаконное использование цифровых идентификационных данных подставными лицами

Шведские власти отметили риски ОД/ФТ, связанные с систематическим использованием преступниками цифровых идентификационных данных подставных лиц в целях легализации преступных доходов. Этот риск также может иметь место при осуществлении операций при личном присутствии, но он приведён для иллюстрации того, как такие атаки могут совершаться в цифровом мире. Услуги провайдеров платёжных услуг, предусматривающие проведение операций в режиме реального времени, являются особенно привлекательными для преступников, поскольку, наряду с незаконным использованием цифровых идентификационных данных, они также позволяют быстро переводить деньги между разными счетами.



Когда преступная группировка хочет отмыть деньги путём незаконного использования цифровых идентификационных данных, ей, прежде всего, необходимо открыть банковские счета, что делается подставными лицами. Роль подставного лица заключается в том, чтобы открыть банковский счёт, получить цифровые идентификационные данные и код безопасности и передать свои учётные данные преступной группировке за вознаграждение. Множество цифровых идентификационных данных может использоваться на одном мобильном телефоне или портативном компьютере (см. схему выше). После этого банковские счета контролируются преступной группировкой. При этом следует отметить, что подавляющее большинство цифровых идентификационных данных, незаконным образом используемых преступными группировками, оформлено на основании законных удостоверений личности (т.е. удостоверяющих личность документов).

Источник: Швеция

124. Ниже рассмотрены некоторые из наиболее известных рисков, связанных с конкретными видами аутентификаторов/процессов, которые являются особенно актуальными для целей ПОД/ФТ.

125. **Уязвимости, связанные с многофакторной аутентификацией:** Пароли или секретные коды, которые, по сути, представляют собой совместно используемые аутентификаторы, являются уязвимыми к атакам с использованием полного перебора логинов, фишинговым атакам и массовым утечкам данных в Интернете, а также легко поддаются взлому. Украденные и ненадёжные пароли,

а также пароли, присваиваемые по умолчанию, фигурируют в 81 проценте случаев утечки данных[36]. Решения, используемые в многофакторной аутентификации, такие как одноразовые коды, отправляемые в виде текстовых SMS-сообщений на мобильные телефоны, обеспечивают дополнительный уровень защиты паролей/секретных кодов, но они также могут быть уязвимыми для фишинговых и иных атак. Аутентификаторы, защищённые от фишинговых атак, в которых, по крайней мере, в одном факторе используется шифрование с открытым ключом[37] (например, аутентификаторы, разработанные на основании сертификатов инфраструктуры открытых ключей (PKI) или стандартов FIDO), могут помочь устранить эти уязвимости.

126. **Биометрические аутентификаторы:** Биофизические аутентификаторы, такие как отпечатки пальцев и радужная оболочка глаз, в большей степени защищены от подделки и взлома по сравнению с традиционными аутентификаторами, и получают повсеместное распространение. В большинстве смартфонов имеются встроенные сканеры отпечатков пальцев; в некоторых смартфонах имеются встроенные сканеры радужной оболочки глаз; а функции распознавания лица встроены во многие персональные компьютеры и современные смартфоны.

127. Однако могут происходить массовые хищения биометрических данных из центральных баз данных[38]. Их также можно получить, делая снимки (фотографии) с высоким разрешением; путём снятия отпечатков пальцев с объектов, к которым прикасался человек (например, невидимые отпечатки пальцев); или делая снимки с высоким разрешением радужной оболочки глаз (например, узора радужной оболочки глаз), а затем использовать в качестве поддельных аутентификаторов. Однако в настоящее время такие атаки являются трудноосуществимыми и/или крайне ресурсозатратными, и поэтому не проводятся в больших масштабах. Например, биометрические аутентификаторы, требующие проверки совпадения на устройстве, не могут использоваться мошенническим образом в больших масштабах, поскольку для этого требуется доступ к устройству клиента.

128. Биометрические данные имеют ряд других слабых мест, что вызывает озабоченность в плане их надёжности при использовании в целях аутентификации. В этой связи в некоторых технических стандартах использование биометрических данных в целях аутентификации ограничено (в отличие от возможности их использования в целях проверки и подтверждения личности)[39]. Отпечатки пальцев могут не считываться или считываться неточно. Факторы, касающиеся распознавания черт лица, могут оказаться ненадёжными вследствие изменения выражения лица при различных настроениях, изменения волос на лице, макияжа и разных условий освещения. По причине неполных наборов данных, распознавание черт лица являлось менее надёжным в случае людей, имеющих тёмный цвет кожи и определённые этнические черты, хотя в последнее время надёжность такого распознавания повышается. В отличие от аутентификаторов, которые человек знает, или которые находятся в его владении, краденые биометрические аутентификаторы гораздо труднее аннулировать или заменить[40].

---

[36] Отчёт о расследованиях утечек данных от 2018 года доступен по адресу: https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf.

[37] **Шифрование с открытым ключом** - шифрование, при котором для объекта (человека, системы или устройства) генерируется пара ключей, и этот объект надёжно хранит секретный ключ, при этом свободно предоставляя открытый ключ другим лицам. Любой человек, имеющий открытый ключ, может затем использовать его для шифрования и отправки сообщения владельцу секретного ключа, зная, что только он сможет открыть это сообщение.

[38] В результате атаки на Управление кадровой службы США (OPM) в 2015 году было похищено 5,6 миллионов комплектов изображений отпечатков пальцев.

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

[40] Хотя существуют способы аннулирования биометрических учётных данных, на сегодняшний день доступность этих способов ограничена, а технические стандарты для их тестирования всё ещё находятся в процессе разработки.

129. **Риски, связанные с жизненным циклом идентификационных данных:** Неудовлетворительное управление жизненным циклом и доступом к идентификационным данным может, вольно или невольно, нарушить целостность аутентификаторов и позволить неуполномоченным лицам получить доступ к клиентским счетам и использовать их в незаконных целях. А это, в свою очередь, подрывает цели, заложенные в требованиях об идентификации/ верификации клиентов, постоянной надлежащей проверке и мониторинге операций для защиты финансовой системы от противоправного использования.

130. **Неизвестные риски:** Системы цифровой идентификации постоянно развиваются и совершенствуются. Во многих случаях изменения в технической конструкции и структуре обеспечивают операционные улучшения, но также влекут за собой уязвимости, которые являются неочевидными до тех пор, пока они не будут использованы злоумышленниками таким образом, что станет очевидным, как была нарушена целостность системы цифровой идентификации.

Потенциальные препятствия для доступа к идентификационным данным в целях осуществления постоянной надлежащей проверки и мониторинга операций

131. Аутентификация в сфере цифровой идентификации может способствовать проведению постоянной надлежащей проверки и осуществлению мониторинга операций. Если регулируемый субъект использует стороннюю систему цифровой идентификации и сам не осуществляет сбор информации, такой как схемы операций, местонахождение, доступ к устройствам и т.д., то он может не иметь доступ к информации, являющейся важной в целях анализа поведения клиентов и схем их операций, для определения того, соответствуют ли проводимые операции сведениям учреждения о клиенте, его хозяйственной деятельности и характере рисков, в том числе, когда необходимо, об источнике средств. Если сбор такой информации осуществляется для предупреждения мошенничества, то эти сведения могут также использоваться в целях ПОД/ФТ. Регулируемые субъекты могут рассмотреть целесообразность получения доступа к данным об аутентификации клиентов при предоставлении им доступа к счетам (или стороннего анализа таких данных), что позволит им выявлять случаи систематического незаконного использования цифровых идентификационных данных, в том числе раскрытых, украденных или проданных цифровых идентификационных данных. Эта информация может использоваться для выявления подозрительной деятельности и принятия решения о направлении сообщений о такой деятельности. Одним из существенных преимуществ интегрированной модели идентификации является то, что в случае выявления мошенничества с идентификационными данными, эти сведения могут передаваться по сети другим провайдерам идентификационных услуг и полагающимся сторонам.

Более широкие вопросы, связанные с системами цифровой идентификации, которые могут повлиять на деятельность в сфере ПОД/ФТ

Вопросы, связанные с подключением

132. Отсутствие развитой и надёжной инфраструктуры может не позволить использовать системы цифровой идентификации в определённых юрисдикциях или в определённых географических районах в течение значительного периода времени. Однако системы цифровой идентификации могут быть разработаны для поддержки операций, осуществляемых как в режиме онлайн, так и традиционным способом, что позволяет им функционировать как при наличии, так и при отсутствии доступа к Интернету или сетям мобильной связи. Регулируемым субъектам следует учитывать такую гибкость при принятии решения о том, следует ли использовать систему цифровой идентификации в целях проведения надлежащей проверки клиентов.

Национальные системы удостоверения личности

133. Если в системах цифровой идентификации используются официальные удостоверяющие личность документы для проверки и подтверждения личности, недостаточная надёжность документарных удостоверяющих личность свидетельств может иметь эффект домино для рисков, представляемых системами цифровой идентификации. «Надёжность и независимость» в случае чисто документарного подхода может быть снижена вследствие кражи идентификационных документов и широко распространённой подделки официальных документов, удостоверяющих личность, в том числе, если такие официальные удостоверения личности не имеют надлежащих элементов защиты для недопущения искажений и подделки, или выдаются без надлежащей проверки и подтверждения личности. Кража идентификационных данных из баз данных в Интернете обусловливает одинаковые риски как в случае систем цифровой идентификации, так и в случае использования документарного подхода.

134. Система цифровой идентификации, разработанная для конкретной ограниченной цели, не связанной с проведением НПК в финансовым секторе, может оказаться неприспособленной или ограниченно приспособленной для использования в других ситуациях. Она также может привести к большим издержкам для регулируемых субъектов или оказаться непригодной для использования в целях НПК (см., например, Вставку 7 в Приложении II)

Вопросы, касающиеся защиты данных и неприкосновенности личной жизни

135. Использование цифровой идентификации включает в себя сбор и обработку персональных данных, в том числе биометрических данных. Важно отметить, что механизмы и стандарты надежности цифровой идентификации включают в себя требования о защите данных и неприкосновенности личной жизни, которые могут основываться на отдельных стандартах, установленных юрисдикцией и/или международной организацией, занимающейся разработкой стандартов. Кроме того, разрабатываются инновационные высокотехнологичные решения (например, децентрализованная цифровая идентификация), которые предоставят лицам больше возможностей для контроля того, как и в каких целях осуществляется сбор, обработка и передача их персональных данных другим лицам, что позволит дополнительно решить проблемные вопросы, касающиеся неприкосновенности личной жизни и защиты данных.

136. На правительство возложена основная обязанность по созданию режима защиты данных и обеспечения неприкосновенности личной жизни в юрисдикции. Такие требования, обеспечивающие конфиденциальность, точность и целостность данных, как правило, будут распространяться на провайдеров услуг цифровой идентификации. Согласно этим требованиям, они будут обязаны, например, проводить оценку воздействия на защиту данных для выявления потенциальных проблемных вопросов, а также для определения надлежащих мер управления рисками. Меры по защите данных и обеспечению неприкосновенности личной жизни являются важными для снижения рисков хищения идентификационных данных и рисков, связанных с кибербезопасностью, которые могут серьёзно подорвать и снизить надёжность системы цифровой идентификации. В этой связи, в соответствии с Рекомендацией 2 ФАТФ органы, отвечающие за вопросы ПОД/ФТ, и органы, отвечающие за обеспечение защиты данных и неприкосновенности личной жизни, должны сотрудничать и взаимодействовать для обеспечения совместимости соответствующих требований и правил.

Вопросы, касающиеся финансовой изоляции

137. Если системы цифровой идентификации не охватывают всё или большинство населения в юрисдикции или не распространяются на определённые слои населения, то они могут способствовать (или, по крайней мере, препятствовать снижению) финансовой изоляции определённых групп

населения, что представляет риск для ПОД/ФТ. Обязательное использование конкретных цифровых идентификационных данных, которые не являются общедоступными в целях проведения НПК, представляют такие же трудности, как и директивное использование бумажных документов, удостоверяющих личность, которые имеются не у всех граждан. Отсутствие доступа к цифровым технологиям или низкий уровень технологической грамотности могут усугубить риск финансовой изоляции. Например, недоступность мобильных телефонов, смартфонов или других цифровых устройств, отсутствие покрытия и/или ненадёжное подключение может лишить возможности доступа к финансовым услугам бедное и сельское население, женщин, а также людей, живущих в нестабильных и охваченных конфликтами районах, таких как беженцы и перемещённые лица. Кроме того, системы цифровой идентификации могут также способствовать финансовой изоляции, если в них используется только биометрическая аутентификация без возможности применения альтернативных механизмов аутентификации. Это обусловлено более высоким процентом сбоев в случае определённых биометрических характеристик. Например, люди, занимающиеся ручным трудом, как правило, имеют мозолистые отпечатки пальцев, которые не распознаются биометрическими считывателями. В случае пожилых людей может иметь место частое несовпадение по причине изменяющихся черт лица, выпадения волос и других признаков старения, болезней или иных факторов. Несоразмерно большой процент сбоев и ошибок распознавания может иметь место в случае определённых этнических групп и лиц, имеющих определённые внешние данные, связанные с более тёмным цветом кожи, разрезом глаз или растительностью на лице.

РАЗДЕЛ V: ОЦЕНКА ДОСТАТОЧНОСТИ СТЕПЕНИ НАДЁЖНОСТИ И НЕЗАВИСИМОСТИ СИСТЕМ ЦИФРОВОЙ ИДЕНТИФИКАЦИИ В РАМКАХ РИСК-ОРИЕНТИРОВАННОГО ПОДХОДА К НПК

138. Как отмечено в Разделе III, в контексте цифровой идентификации требование о том, чтобы идентификация/верификация клиентов проводилась с использованием «документов, данных или информации из надёжных независимых источников», означает, что системы цифровой идентификации должны быть основаны на технологиях, надлежащем управлении, процессах и других мерах, обеспечивающих надлежащий уровень достоверности. Это означает наличие необходимого уровня уверенности (надежности) в том, что система цифровой идентификации работает как надо и выдаёт точные результаты. Она также должна быть защищена от внутреннего или внешнего манипулирования или фальсификаций в целях создания и оформления ложных идентификационных данных или аутентификации неправомочных пользователей, в том числе путём осуществления кибератак или совершения внутренних должностных преступлений.

139. Для определения того, соответствует ли использование системы цифровой идентификации требованиям Рекомендации 10 (a) и (d), государственные органы, финансовые учреждения и другие заинтересованные стороны должны провести следующие оценки:

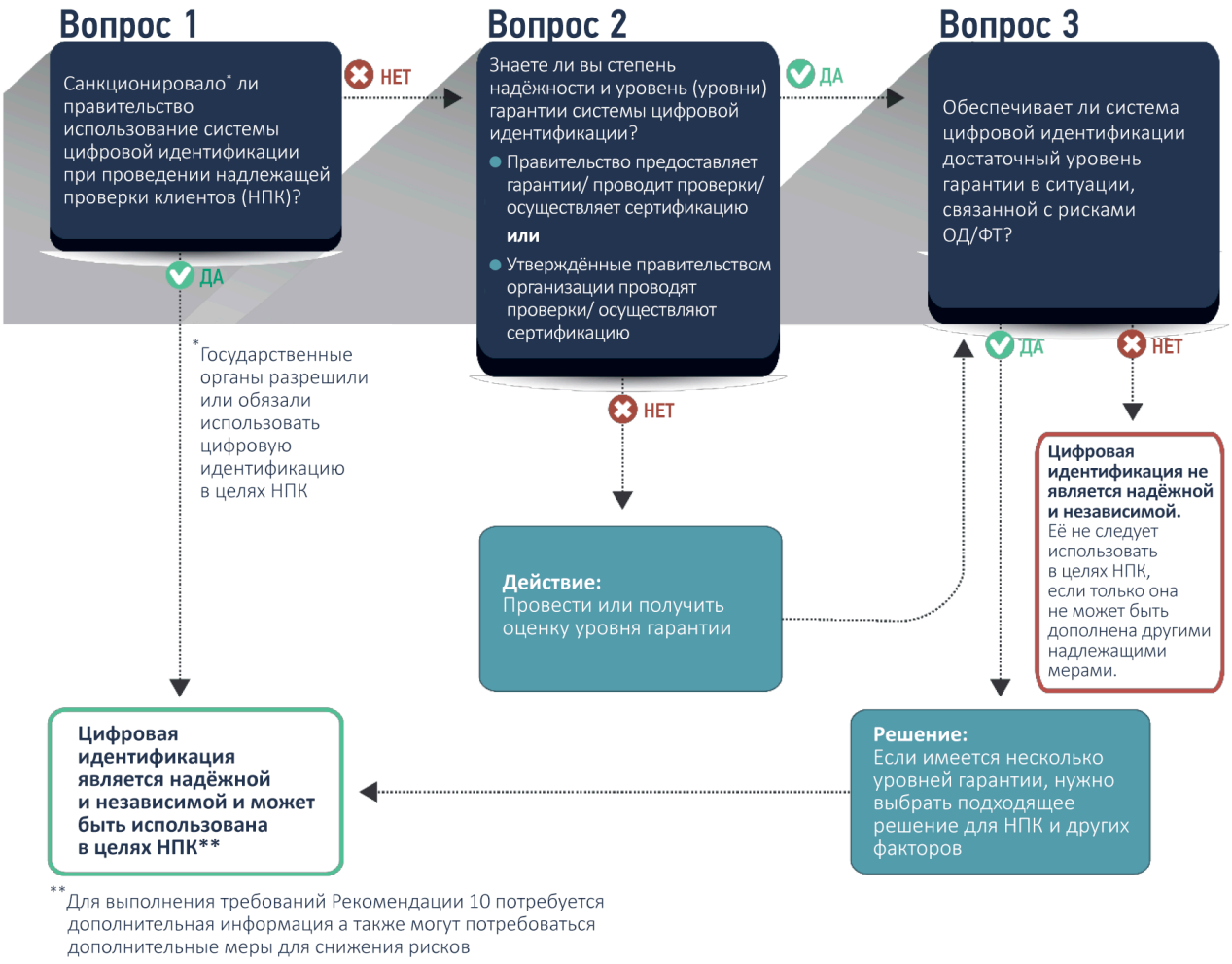
    a. Необходимо понять, какие уровни надежности обеспечивает система цифровой идентификации с учётом используемых в ней технологий, архитектуры и методов управления для определения её надёжности/независимости; и

    b. Учитывая уровни надежности цифровой идентификации, им необходимо определить, исходя из оценки рисков, является ли система цифровой идентификации достаточно надёжной и независимой в свете потенциальных рисков, связанных с отмыванием денег, финансированием терроризма, мошенничеством и другой незаконной финансовой деятельностью.

140. В зависимости от системы (систем) цифровой идентификации и нормативно-правовой базы, имеющейся в конкретной юрисдикции, государственные органы и регулируемые субъекты могут выполнять разные функции и обязанности в процессе оценки уровней надежности, обеспечиваемых системой идентификации, и её пригодности для целей НПК, как указано на приведённой ниже диаграмме принятия решений для регулируемых субъектов.

141. На приведённой схеме показан порядок принятия регулируемыми субъектами решения о том, можно ли использовать систему цифровой идентификации в целях проведения идентификации и верификации клиентов и осуществления постоянной надлежащей проверки. Две указанные выше оценки отражены во втором и третьем вопросе соответственно.

Рисунок 4: Процесс принятия решений для регулируемых субъектов



Первый вопрос: Санкционировало ли правительство использование системы цифровой идентификации при проведении надлежащей проверки клиентов (НПК)?

142. В рамках Первого вопроса, если правительство поддерживает систему цифровой идентификации и считает её подходящей для использования в процессе надлежащей проверки клиентов, то регулируемые субъекты могут использовать такую систему цифровой идентификации без проведения оценки по Второму и Третьему вопросу. Это означает, что правительство фактически провело оба этапа рекомендуемой оценки (по крайней мере, стандартных рисков, связанных с НПК) за регулируемых субъектов, и поэтому остальные этапы процесса принятия решения не применимы. Однако, в зависимости от действующего законодательства в области ПОД/ФТ и общей системы цифровой идентификации, существующей в юрисдикции, от регулируемых субъектов может потребоваться принятие дополнительных мер (см. пункты 147 и 148 ниже).

143. Правительства могут однозначно счесть целесообразным использование систем цифровой идентификации для проведения надлежащей проверки клиентов, выпустив для регулируемых субъектов нормативные акты или руководства, *разрешающие или обязывающие* их применять систему (системы) цифровой идентификации в целях выполнения определённых элементов НПК. Такое прямое разрешение может быть дано, например, когда правительство само разработало и осуществляет эксплуатацию системы (систем) цифровой идентификации и, поэтому доверяет им, или когда у правительства имеется механизм для получения проверенной сертифицированной информации об уровнях гарантий, обеспечиваемых системой цифровой идентификации другого провайдера.

144. Правительства могут также опосредованно поддерживать систему цифровой идентификации и в неявно выраженной форме считать её подходящей для использования регулируемыми субъектами в процессе надлежащей проверки клиентов. Это может иметь место, когда, например, правительство ввело систему цифровой идентификации общего назначения, которая в требуемых случаях используется для официального удостоверения личности в юрисдикции. Государственные органы должны открыто и чётко разъяснить, как работает их система цифровой идентификации, и какие уровни надежности она обеспечивает. То же самое относится к системам идентификации ограниченного назначения, которые разрешено использовать в финансовом секторе.

145. В зависимости от действующих в юрисдикции законов и нормативных актов в сфере ПОД/ФТ, регулируемым субъектам потребуется применять дополнительные меры при использовании разрешённых систем цифровой идентификации в определённых обстоятельствах, например, в ситуациях, характеризующихся повышенным риском, а также собирать информацию, касающуюся других аспектов НПК, не рассматриваемых в рамках настоящего Руководства (т.е. для понимания цели и предполагаемого характера деловых отношений). В некоторых юрисдикциях могут действовать нормативные акты, разрешающие использовать системы цифровой идентификации только в ситуациях и обстоятельствах, представляющих пониженный риск.

146. Помимо выполнения нормативных требований, действующих в их юрисдикциях, регулируемым субъектам рекомендуется рассмотреть необходимость принятия дополнительных мер для снижения рисков, связанных с цифровой идентификацией (если она используется). Такие меры могут включать в себя введение дополнительных единиц данных идентификационных атрибутов, дополнительных аутентификаторов и/или меры для снижения рисков ОД/ФТ, в зависимости от внутренней политики финансового учреждения, касающейся ПОД/ФТ, противодействия мошенничеству и управления общими рисками.

Второй вопрос: Знаете ли вы уровень (уровни) надежности системы цифровой идентификации?

147. В случае, если правительство не санкционировало, прямо или косвенно, применение конкретных систем цифровой идентификации в целях НПК, регулируемому субъекту необходимо, в первую очередь, определить уровни надежности[41], обеспечиваемые любой системой цифровой идентификации, которую он собирается использовать.

148. Если государственные органы предоставляют надежности, осуществляют проверки или проводят сертификацию систем цифровой идентификации (своими силами или силами назначенных организаций, действующих от их имени[42]), то регулируемые субъекты могут полагаться на такие оценки при ответе на Второй вопрос в рамках процесса принятия решения. Аналогичным образом, правительство может назначить национальную или зарубежную экспертную организацию для тестирования/проверки и сертификации уровней надежности, обеспечиваемых системами цифровой идентификации, на которые регулируемые субъекты могут полагаться. Краткий обзор некоторых из таких экспертных организаций приведён в Приложении «D». Системы цифровой идентификации могут быть сертифицированы на соответствие минимальному уровню надежности или иметь разные по степени надежности уровни надежности (либо единые, либо отдельные для каждого составного элемента), но достоверная информация должна быть общедоступной.

149. Если правительство официально не санкционировало использование системы (систем) цифровой идентификации при проведении надлежащей проверки клиентов и не предоставило механизм для получения достоверной информации об уровне (уровнях) надежности, обеспечиваемых системой (системами) цифровой идентификации, регулируемые субъекты должны самостоятельно определить надёжность и независимость системы:

    a. либо путём проведения оценки уровня надежности самостоятельно;

    b. либо путём использования информации о проверке или сертификации уровней надежности, проведённой экспертной организацией (пусть даже не утверждённой официально правительством).

150. Если регулируемый субъект проводит оценку уровня надежности самостоятельно, он должен осуществить надлежащую проверку провайдера системы цифровой идентификации, в том числе проверить наличие у него надлежащих систем управления и принять дополнительные меры предосторожности.

151. Регулируемый субъект должен использовать информацию, полученную от другой экспертной организации только, если у него имеются разумные основания считать, что такая организация применяет надлежащие открытые механизмы и стандарты надежности цифровой идентификации. Например, такая организация может быть назначена для исполнения аналогичных функций правительством другой страны или быть признана в качестве надёжной соответствующими национальными, региональными или международными экспертами.

---

[41] Как указано выше в настоящем Руководстве, термин «уровень гарантии» означает степень доверия или уверенности в надёжности каждого составного элемента процесса цифровой идентификации.

[42] Это может осуществляться не силами национальных органов, отвечающих за регулирование в целях ПОД/ФТ, поскольку возможности для определения того, применяет ли субъект надлежащие открытые механизмы и технические стандарты гарантии идентификации, будут, вероятно, иметься у других государственных органов. Но в любом случае выбор компетентного органа для исполнения этой функции отдаётся на усмотрение каждой отдельной юрисдикции. Например, в США Управление служб общего назначения (GSA) утвердило нескольких провайдеров удостоверительных услуг для сертификации систем цифровой идентификации, используемых в государственных целях.

Третий вопрос: Является ли система цифровой идентификации подходящей для использования в ситуации, связанной с рисками ОД/ФТ?

152. После того, как регулируемый субъект удостоверился (используя порядок, описанный в рамках Второго вопроса) в том, что он знает уровни надежности, обеспечиваемые системой цифровой идентификации, ему необходимо проанализировать, подходит ли система цифровой идентификации в контексте соответствующих рисков, связанных с незаконной финансовой деятельностью, для использования риск-ориентированного подхода к проведению НПК, определённого ФАТФ. Иными словами, принимая во внимание уровень (уровни) надежности, подходит ли система цифровой идентификации для использования в процессе идентификации/верификации клиентов и проведения постоянной надлежащей проверки в свете потенциальных рисков ОД/ФТ, связанных с клиентами, продуктами и услугами, географической зоной деятельности и т.д. Регулируемым субъектам необходимо проанализировать, является ли система цифровой идентификации, с учётом обеспечиваемого ей уровня надежности, подходящей для использования в ситуации, характеризующейся соответствующими рисками незаконной финансовой деятельности. В зависимости от установленных в юрисдикции требований ПОД/ФТ и имеющихся систем цифровой идентификации, у регулируемых субъектов может иметься возможность выбора из нескольких систем цифровой идентификации с разными уровнями надежности для проверки и подтверждения личности и аутентификации. В такой ситуации регулируемым субъектам следует сравнить и сопоставить надёжность проверки и подтверждения личности и/или аутентификации, обеспечиваемую системой, с видами возможной незаконной деятельности и уровнем рисков ОД/ФТ.

153. В некоторых странах государственные органы установили обязательный (единый) уровень надежности для ситуаций, характеризующихся стандартным или высоким риском ОД/ФТ. Тем не менее, у регулируемых субъектов всё равно может иметься возможность выбора из нескольких систем цифровой идентификации, обеспечивающих требуемый уровень надежности. У регулируемых субъектов также может иметься возможность выбора из различных уровней удостоверяющих личность свидетельств и/или конкретных учётных данных или аутентификаторов, предусмотренных в одной и той же системе. В этом случае при выборе подходящего варианта (вариантов) им следует учитывать особенности своих рисков ОД/ФТ в части проверки и подтверждения личности и аутентификации. У регулируемых субъектов также может иметься возможность выбора соответствующих систем цифровой идентификации для ситуаций, характеризующихся пониженным риском (см. также подраздел ниже, посвящённый вопросам расширения доступности финансовых услуг).

Использование правовых механизмов и технических стандартов надежности цифровой идентификации для применения риск-ориентированного подхода

154. Как указано выше, государственные органы (выступающие в качестве провайдеров идентификационных услуг и/или органов регулирования, надзора и выработки политических решений) и регулируемые субъекты (выступающие в качестве полагающихся сторон) должны надлежащим образом рассмотреть и учесть соответствующие факторы риска и уровни надежности цифровой идентификации, применительно к соответствующим факторам риска ОД/ФТ и мерам по снижению этих рисков. Как более подробно описано ниже, **механизмы и стандарты надежности цифровой идентификации** являются полезным инструментом для проведения такой оценки.

155. В этой связи государственным органам и регулируемым субъектам рекомендуется учитывать информацию, содержащуюся в нормативах и стандартах надежности идентификации, при оценке того, отвечает ли система цифровой идентификации критериям «надёжности и независимости», предусмотренным в Рекомендации 10(а). Им также рекомендуется рассмотреть надёжность каждого отдельного составного

элемента системы цифровой идентификации. Это обусловлено тем, что, в зависимости от факторов потенциального риска ОД/ФТ и имеющихся мер, направленных на снижение этого риска, одинаковая степень надёжности может не требоваться для каждого элемента системы цифровой идентификации (проверки и подтверждения личности/регистрации, аутентификации и, в соответствующих случаях, интеграции).

156. Понимание уровня надежности, обеспечиваемого каждым составным элементом системы цифровой идентификации, может помочь регулируемым субъектам применять более выверенный риск-ориентированный подход к НПК при использовании цифровой идентификации. Последовательный поэтапный подход к оценке уровня надежности является особенно актуальным в контексте расширения доступности финансовых услуг. В технических стандартах на портале «GOV.UK Verify» и в окончательной версии Руководства NIST по цифровой идентификации 800-63-3 установлены отдельные «уровни надежности» для каждого основного этапа, осуществляемого в рамках системы идентификации[43]. В случае правовых механизмов и стандартов надежности идентификации, в которых предусмотрен единый уровень надежности для всей системы цифровой идентификации в целом (таких как, например, Регламент ЕС об электронной идентификации), последовательный поэтапный подход может применяться путём рассмотрения того, насколько каждый элемент и этап процесса отвечает требованиям, установленным для каждого уровня надежности.

157. Технологии и архитектура цифровой идентификации, а также механизмы и стандарты надежности цифровой идентификации являются динамичными и постоянно развиваются[44]. Стандарты сами по себе являются гибкими и ориентированными на результат в целях содействия внедрению инноваций. В настоящее время они дают возможность использовать разные технологии и архитектурные решения для выполнения требований, установленных для отдельных уровней надежности, а их структура позволяет в максимально возможной степени использовать их в будущем. Юрисдикциям следует избегать использования жестко регламентированных подходов, в рамках которых действующие на сегодняшний момент требования к уровню надежности рассматриваются в качестве «крыши», а не одного из возможных «этажей» в плане надёжности.

Использование стандартов и механизмов надежности цифровой идентификации

158. Механизмы и стандарты надежности цифровой идентификации, как правило, предусматривают различные, всё более надёжные уровни надежности и устанавливают всё более жёсткие технические требования для каждого из трёх этапов, реализуемых в рамках системы цифровой идентификации.

159. Также как в Пояснительной записке к Рекомендации 10 приведены примеры факторов потенциально повышенного и пониженного риска ОД/ФТ, в технических стандартах предусмотрены факторы *надёжности* идентификации в виде уровней надежности для основных этапов и составных элементов системы цифровой идентификации. Каждый уровень надежности отражает степень уверенности или доверия к рассматриваемому этапу или процессу. Процесс с более высоким уровнем надежности является более надёжным, тогда как процесс с меньшим уровнем надежности представляет повышенный риск сбоя и является менее надёжным. Государственные органы и регулируемые субъекты могут ис-

[43] Например, в Руководствах Национального института стандартов и технологий США (NIST) предусмотрены три (1-3) уровня гарантии для каждого из этапов цифровой идентификации: уровень гарантии идентификации (IAL); уровень гарантии аутентификации и управления жизненным циклом учётных данных (ALA); и уровень доверия к федеративной интеграции (FAL).

[44] Следует признать, что стандарты цифровой идентификации не всегда поспевают за развитием технологий. Например, на момент завершения подготовки настоящего Руководства механизмы и стандарты гарантии цифровой идентификации ещё не охватывали вопросы непрерывной аутентификации. В них также не содержались положения, касающиеся прогрессивной идентификации в части постоянной динамичной проверки подлинности и подтверждения личности.

пользовать уровни надежности для оценки надёжности конкретной системы цифровой идентификации. Настоящее Руководство не устанавливает и не рекомендует какие-либо конкретные уровни надежности.

160. Некоторые технические стандарты предусматривают проведение последовательной поэтапной оценки надёжности и допускают, что различные процессы и этапы цифровой идентификации могут, но не обязательно, обеспечивать один и тот же уровень надежности. Однако, если смотреть глубже, то в рамках риск-ориентированного подхода требуется определить, какие уровни надежности подходят для разных процессов и этапов с учётом существующих рисков, связанных с отмыванием денег, финансированием терроризма, мошенничеством и другой незаконной финансовой деятельностью. Даже если в рамках механизма установлен единый уровень надежности, регулируемые субъекты всё равно могут проанализировать, в какой степени каждый элемент и этап процесса соответствует отдельным требованиям, установленным для каждого уровня надежности.

161. Для иллюстрации факторов, которые соответствующие государственные органы, финансовые учреждения и другие заинтересованные стороны могут использовать для оценки надёжности и независимости цифровой идентификации, а также степени гибкости, предусмотренной в механизмах и стандартах надежности цифровой идентификации, в ***Приложении «E»: Обзор технических стандартов и механизмов надежности цифровой идентификации в США и ЕС*** приведены в качестве примеров уровни надежности, установленные в США и Европейском союзе. В этом Приложении в общих чертах описываются технические требования к проверке и подтверждению личности (что является первым этапом в рамках системы цифровой идентификации). В нём также кратко выделены некоторые ключевые вопросы, связанные с уровнями надежности аутентификации.

Специальные вопросы, касающиеся расширения доступности финансовых услуг

Взаимосвязь между управлением рисками цифровой идентификации, риск-ориентированным подходом в сфере ПОД/ФТ и мерами по снижению рисков ОД/ФТ

162. В идеале, внедрение систем цифровой идентификации позволит физическим лицам подтвердить свою «официальную идентичность» с более высоким уровнем надежности (достоверности) – особенно в тех странах, в которых государство ещё не обеспечило всех граждан надёжными официальными удостоверениями личности. Однако, поскольку цифровая идентификация часто основана на документарных удостоверениях личности, в тех странах, в которых лишь небольшое число граждан имеет официальные удостоверяющие личность документы, некоторые слои населения могут, по-прежнему, не иметь возможность получить цифровые удостоверения личности с повышенным уровнем надежности по причине трудностей, связанных с проверкой и подтверждением их личности.

163. Как подчёркнуто выше в настоящем Руководстве, юрисдикциям, испытывающим трудности с охватом всех слоёв населения финансовыми услугами, следует использовать гибкий подход при определении требуемых атрибутов, доказательств и процессов идентификации в целях проверки и подтверждения подлинности «официальной идентичности». Это даст возможность распространить требования, касающиеся проверки и подтверждения личности, на граждан, не имеющих доступ к финансовым услугам (например, путём включения адреса постоянного местожительства в качестве возможного атрибута или, разрешив пользующимся доверием лицам удостоверять личность другого человека). В рамках более широких международных, правительственных или неправительственных инициатив, направленных на решение этих вопросов (в том числе путём расширения доступа к удостоверяющим личность свидетельствам) государственным органам, отвечающим за ПОД/ФТ,

и регулируемым субъектам следует рассмотреть и проанализировать, как риск-ориентированный подход к НПК сообразуется с системами цифровой идентификации, особенно в юрисдикциях или среди слоёв населения, в которых финансовая изолированность была определена в качестве риска ОД/ФТ.

164. В 2017 году ФАТФ опубликовала дополнение к Руководству по мерам ПОД/ФТ и доступности финансовых услуг (от 2013 года), специально посвящённое вопросам НПК и доступности финансовых услуг[45]. В этом документе подчёркивается, что меры по снижению риска, которые обязаны применять регулируемые субъекты, должны соответствовать характеру и уровню выявленных рисков. В нём также представлены разные подходы к проведению НПК, которые могут устранить препятствия для доступа к финансовым услугам, связанные с верификацией личности клиента. Это включает, например, расширенное понимание надёжного и независимого источника информации или упрощённые меры надлежащей проверки. В указанном Руководстве также отмечено, что в ряде стран поэтапный многоуровневый подход к проведению НПК способствовал расширению доступности цифровых финансовых услуг. Например, в рамках этого подхода людям, которые раньше не имели или имели ограниченный доступ к финансовым услугам, открывается счёт, в котором изначально заложены меры, направленные на снижение рисков ОД/ФТ. Такие меры включают в себя, например, лимиты на общую сумму денежных средств, которая может находиться на счёте, и/или ограничения на сумму и количество операций, которые можно осуществить в установленный период времени, а верификация личности клиента откладывается до того момента, когда эти пороговые значения будут достигнуты.

165. Применение уроков, извлечённых из Руководства о доступности финансовых услуг от 2017 года, к системам цифровой идентификации означает, что, когда риски ОД/ФТ, связанные с приёмом на обслуживание конкретного потенциального клиента, являются низкими, система цифровой идентификации с более низким уровнем надежности в части проверки и подтверждения личности может быть вполне приемлема в этой ситуации. При этом могут потребоваться дополнительные меры для обеспечения снижения риска ОД/ФТ, в том числе, например, установление ограничений на использование счёта, как описано выше. Также могут иметь место ситуации, когда риски незаконной финансовой деятельности, связанные с несанкционированным доступом к счетам, являются повышенными (например, по причине широкого использования краденых имён пользователей и паролей в юрисдикции), но при этом сам клиент представляет низкий риск. В этом случае для недопущения использования счёта неправомочными лицами может быть использована система цифровой идентификации с более низким уровнем надежности в части проверки и подтверждения личности (в целях идентификации/верификации клиента при приёме на обслуживание), но с повышенным уровнем надежности в части аутентификации клиента. Аутентификация личности клиента для санкционирования доступа к счёту в целях проведения операций (даже в случае счетов с небольшими суммами) является важной мерой для борьбы с мошенническими операциями. Такая аутентификация также необходима для недопущения обхода требований, касающихся сумм, частоты и объёмов операций, установленных в рамках многоуровневой НПК.

166. Способность использовать гибкий подход к применению систем цифровой идентификации в рамках Стандартов ФАТФ имеет важные последствия для обеспечения доступности финансовых услуг. Такой подход может способствовать внедрению практики поэтапной многоуровневой НПК и отложенной проверки личности, поскольку в рамках механизмов и стандартов надежности цифровой идентификации системы цифровой идентификации с более низким уровнем надежности в части проверки и подтверждения личности/регистрации предусматривают использование менее строгих удостоверяющих личность свидетельств или менее жёсткой проверки личности человека (см. Приложение «Е»).

[45] ФАТФ (2013-2017), «Меры по противодействию отмыванию денег и финансированию терроризма и доступность финансовых услуг – с дополнением, касающимся надлежащей проверки клиентов», Париж, http://www.fatf-gafi.org/publications/financialinclusion/documents/financial-inclusion-cdd-2017.html

Это означает, что человек, который ранее не имел или имел ограниченный доступ к финансовым услугам (вследствие отсутствия определённых документов для подтверждения своей личности при приёме на обслуживание), всё равно может быть зарегистрирован в системе цифровой идентификации. После этого такой человек может использовать цифровые идентификационные аутентификаторы в целях установления его личности при открытии счёта без проведения проверки его личности при условии соблюдения установленных мер контроля и лимитов.

167. Кроме того, системы цифровой идентификации могут позволить людям, которые ранее не имели или имели ограниченный доступ к финансовым услугам, создать со временем более чёткий «цифровой след» и «профиль риска», что даст им возможность получить доступ к более широкому спектру финансовых услуг. В зависимости от используемого в юрисдикции подхода к требованиям, касающимся подтверждения личности, системы цифровой идентификации могут потенциально трансформировать само понятие «официальной идентичности» от чего-то, что является неизменным, к чему-то, что может развиваться со временем, то есть, к так называемой «прогрессивной идентичности». В случае прогрессивной идентичности, по мере того как человек (например, клиент) осуществляет цифровую финансовую деятельность и другую деятельность в режиме онлайн и наращивает свое цифровой присутствие, появляются дополнительные атрибуты его личности и факторы аутентификации, которые могут расширить цифровую идентичность этого человека и, таким образом, повысить степень уверенности в личности клиента.

168. Прогрессивная идентичность также содействует расширению доступности финансовых услуг, даже если системы цифровой идентификации не обладают функциональной совместимостью, а цифровые идентификационные данные не могут переноситься, поскольку она позволяет конкретному регулируемому субъекту лучше понять отдельного клиента и повысить уверенность в деловых отношениях для предоставления более широкого спектра финансовых услуг. Однако значение прогрессивной идентичности значительно возрастает, в том числе в целях расширения доступности финансовых услуг, в том случае, когда она является переносимой. В этом случае более надёжные идентификационные данные, основанные на поведенческих характеристиках человека, сведениях о его операциях и на связанных с ними данных аутентификации, собираемых одним регулируемым субъектом, могут «сопровождать» этого человека и использоваться в целях его идентификации/верификации другим регулируемым субъектом. В отсутствие такой переносимости клиентам приходится заново формировать свою прогрессивную идентичность в каждом регулируемом субъекте в течение определённого периода времени, на протяжении которого они могут получать доступ только к продуктам и услугам, позволяющим осуществлять операции на ограниченные суммы и представляющим низкий риск.

Вставка 3: Пример того, как использование цифровых идентификационных данных в рамках поэтапной многоуровневой НПК может содействовать расширению доступности финансовых услуг

Человек, не имеющий доступа к финансовым услугам, обращается с просьбой открыть ему ограниченный банковский счёт, предоставив свои цифровые идентификационные данные, полученные без предъявления доказательств, подтверждающих его личность. Такие цифровые идентификационные данные имеют пониженный уровень надежности в части проверки и подтверждения личности, но обеспечивают уровень надежности в части аутентификации, дающий уверенность в том, что заявитель контролирует аутентификатор (аутентификаторы), привязанный (привязанные) к идентифицированному человеку.

Регулируемый субъект принимает клиента на обслуживание и открывает ему банковский счёт, представляющий низкий риск, с очень ограниченными лимитами на суммы, объёмы и частоту операций и отсутствием возможности осуществлять трансграничные операции (эти меры по снижению рисков основаны на анализе рисков). Клиент использует этот счёт для приобретения мобильного телефона по договору и, помимо всего прочего, получает заработную плату прямо на банковский счёт.

Регулируемый субъект использует данные, связанные с прямым перечислением заработной платы, социальных выплат или пособий, для проверки занятости, рода деятельности и источника средств клиента. Регулируемый субъект также использует данные о регулярных платежах с банковского счета за мобильный телефон и коммунальные услуги для определения шаблона ответственного финансового поведения клиента. Кроме того, регулируемый субъект осуществляет сбор информации о других осуществляемых операциях и связанных с ними данных аутентификации для проверки и подтверждения адреса клиента. Со временем регулируемый субъект использует постоянную финансовую деятельность клиента и моделей его поведения (например, время проведения операций, типичные суммы операций, цели операций/получатели платежей и данные геолокации) для повышения надёжности аутентификации в целях предоставления доступа к счёту и принятия мер для недопущения мошенничества.

В юрисдикции действует нормативно-правовая база в сфере ПОД/ФТ, в основе которой лежат определённые принципы, показатели и результаты. Согласно действующим нормативным актам, регулируемые субъекты должны иметь разумные основания для того, чтобы считать, что они знают, кем являются их клиенты, но в этих нормативных актах жестко не предписано, каким именно образом они должны достигнуть этого. Регулируемый субъект рассматривает данные, генерируемые в процессе деятельности клиента со временем, в качестве подтверждающих личность свидетельств и использует их для укрепления своей уверенности в том, что он знает, кем является клиент, и знает профиль риска этого клиента. Когда такая уверенность позволяет регулируемому субъекту считать, что он выполнил свои обязательства, касающиеся идентификации/верификации клиента, а также удовлетворены все условия, касающиеся допустимого уровня риска, порядка и процедур управления рисками, связанными с другими финансовыми услугами, регулируемый субъект предлагает стандартный банковский счёт с более высокими лимитами и большими функциональными возможностями. Позднее регулируемый субъект предоставляет небольшую ссуду, которую клиент использует для открытия своего собственного дела.

Такой подход к цифровой идентификации является зеркальным отражением аналогичного процесса, описанного в Руководстве ФАТФ о НПК и доступности финансовых услуг от 2017 года. В рамках этого процесса лица, не имеющие удостоверяющих личность документов, могут проходить поэтапную многоуровневую надлежащую проверку, а также постепенно расширять и повышать свой уровень доступа к финансовым услугам, начиная с открытия ограниченного счета, представляющего низкий риск.

Источник: министерство финансов США

Возможности механизмов и стандартов цифровой идентификации содействовать доступности финансовых услуг

«Доверенные поручители»

169. Одним из примеров этого являются механизмы и стандарты надежности цифровой идентификации, которые позволяют людям, не имеющим традиционные документы, удостоверяющие личность, использовать доверенных лиц – таких как старост деревень, местных чиновников, судей, работодателей, других лиц, пользующихся хорошей репутацией в местной общине (например, бизнесменов, юристов, нотариусов) или других обученных, утверждённых или уполномоченных лиц – для того, чтобы они поручились за заявителя для удостоверения его личности[46] в соответствии с действующими в юрисдикции законами, нормативными актами или ведомственными правилами.

170. Например, в соответствии с Руководством Национального института стандартов и технологий США (NIST), в случае использования доверенных поручителей провайдеры идентификационных услуг обязаны:

* Разработать письменную политику и процедуры, устанавливающие порядок определения доверенного поручителя (критерии выбора) и срок действия статуса доверенного поручителя в качестве действующего поручителя, включая любые требования об ограничении, отзыве и приостановке такого статуса.

* Провести проверку и подтвердить личность доверенного поручителя на том же самом уровне, что и заявителя, и определить минимальные доказательства личности, требуемые для установления отношений между доверенным поручителем и заявителем.

Дистанционная проверка, подтверждение личности и приём на обслуживание без личного контакта

171. Как отмечено выше, системы цифровой идентификации могут позволить осуществлять дистанционную идентификацию/верификацию клиентов и обеспечить возможность дистанционного проведения финансовых операций с обеспечением стандартного или даже пониженного уровня риска. Технические стандарты допускают дистанционную проверку, подтверждение личности и регистрацию даже при установленных повышенных уровнях надежности. См. Приложение «E».

[46] Руководство NIST 800-63A, пункт 4.4.2 - Уровень гарантии идентификации 2: Требования к удостоверению личности доверенными поручителями

ПРИЛОЖЕНИЕ А: ОПИСАНИЕ БАЗОВОЙ СИСТЕМЫ ЦИФРОВОЙ ИДЕНТИФИКАЦИИ И ЕЕ УЧАСТНИКОВ

В данном Приложении приводится более подробное объяснение основных элементов общей системы цифровой идентификации, с более полным изложением сведений, приведенных в разделе II. Описание очень обобщенное. Вниманию читателя предлагаются некоторые примеры технологий или процессов, исключительно в качестве иллюстрации. Мы не призываем и не одобряем использование какой-либо конкретной технологии, архитектуры или процесса идентификации, таких как биометрия или мобильные технологии. Таким образом, информация относится к широкому спектру систем цифровой идентификации. В данном Приложении основное внимание уделяется первым двум элементам системы цифровой идентификации, поскольку они имеют самое непосредственное отношение к применению требований Рекомендации 10 в отношении идентификации/верификации клиента при принятии его на обслуживание и для аутентификации клиента с целью доступа к учетной записи. Настоящее приложение предназначено для описания общей ситуации и не предусматривает определение технических или организационных требований к приемлемой цифровой идентификации в рамках системы ПОД/ФТ.

Краткое описание процесса цифровой идентификации

Как отражено в стандартах цифровой идентификации Национального института стандартов и технологий США, процесс цифровой идентификации включает в себя два основных элемента и третий необязательный элемент:

- **Элемент 1: Проверка и подтверждение личности, регистрация (с первичной привязкой/выпуском учётных данных)** (обязательный элемент);
- **Элемент 2: Аутентификация и управление жизненным циклом идентификационных данных** (обязательный элемент);
- **Элемент 3: Механизмы переносимости и функциональной совместимости** (необязательный элемент).

Проверка и подтверждение личности/регистрация могут быть цифровыми или документарными, с личным присутствием (очные) или без личного присутствия (удаленные)[47]. В системе цифровой идентификации привязка/выпуск учетных данных, аутентификация и переносимость/федеративная интеграция всегда цифровые, в обязательном порядке.

Терминология, используемая различными юрисдикциями и организациями, может незначительно различаться в зависимости от описываемой системы. Более подробное описание каждого из этапов приводится ниже.

Элемент 1: Проверка и подтверждение личности, регистрация

Проверка и подтверждение личности, регистрация (с первичной привязкой/выпуском учётных данных) совместно составляют первый этап системы цифровой идентификации.

Проверка и подтверждение личности дает ответ на вопрос: «Кто вы такой?» и относится к процессу, посредством которого провайдер идентификационных услуг (IDSP) собирает, валидирует, проверяет информацию о человеке и отождествляет ее с уникальным физическим лицом в рамках данной группы населения или контекста.

Ниже описывается процесс идентификации, который включает в себя три этапа: сбор/отождествление, (2) валидация и (3) верификация.

[47] Более подробное объяснение этих терминов приводится в Руководстве.

(1) Сбор и отождествление предполагают получение атрибутов, сбор подтверждений атрибутов и отождествление доказательств и атрибутов идентичности с единственной уникальной личностью в рамках данной группы населения или контекста. Процесс отождествления доказательств и атрибутов идентичности с единственной уникальной личностью в рамках данной группы населения или контекста называется **исключением дубликатов**. В некоторых предоставляемых правительством решениях цифровой идентификации процесс исключения дубликатов является частью проверки и подтверждения личности, которая может включать в себя проверку конкретных биографических атрибутов соискателя (таких как имя, возраст и пол), биометрических данных (таких как отпечатки пальцев, радужная оболочка глаз и распознанное изображение лица) и присвоенных правительством атрибутов (таких как номера водительских прав и/или паспорта или идентификационный номер налогоплательщика) по базе данных зарегистрированных в системе идентификации пользователей и их соответствующих атрибутов и доказательств идентичности, в целях предотвращения создания дубликатов при регистрации.

- **Подтверждение атрибута** может быть либо физическим (документарным), либо чисто цифровым, либо являться цифровым представлением физического подтверждения атрибута (например, цифровым представлением бумажных или пластиковых водительских прав). Традиционно доказательства идентичности имеют физическую форму, такую как (для физических лиц) выданный государством документ (предпочтительно, для надежности, с фотографией и голограммой или аналогичными средствами защиты) — например, свидетельство о рождении, национальное удостоверение личности, водительские права или паспорт. Кроме того, традиционно заявитель физически предъявлял провайдеру идентификационных услуг документарное доказательство идентичности. С развитием цифровых технологий стало возможно цифровое доказательство идентичности (или преобразование доказательств из физической в цифровую форму) и хранение в электронных базах данных, что позволяет *получать удаленный доступ* к доказательствам и/или атрибутам идентификации и к другой информации для удаленной проверки и подтверждения по цифровой(-ым) базе(- ам) данных.

- Атрибуты также могут быть свойственными, т.е. основанными на личных биометрических (биологических или поведенческих) характеристиках человека[48]. Биометрия быстро эволюционировала от статической к динамической, что привело к появлению различных технологий биометрической идентификации с различными рисками снижения надежности и конфиденциальности. С учетом технологической отработанности и масштабов коммерческого внедрения, а также серьезности потенциальных угроз конфиденциальности, системы цифровой идентификации могут включать использование следующих элементов:
  - атрибуты биофизической биометрии, такие как отпечатки пальцев, радужная оболочка глаз, спектрограммы голоса и распознанные изображения лиц; все они не меняются со временем;
  - атрибуты биомеханической биометрии, такие как механика нажатия клавиш, которые являются результатом уникальных взаимодействий мышц, скелетной и нервной систем человека; все они динамичны;
  - атрибуты поведенческой биометрии, основанные на новой вычислительной общественной науке — социальной физике, которые состоят из различных схем движения человека и использования им *геопространственных временных данных*, которые включают в себя, например, схемы электронных писем или текстовых сообщений человека, использование мобильного телефона, геолокационные схемы и журнал регистрации доступа к файлам (включая ожидаемые способы входа в систему, геолокацию, время, частоту и тип использования (остаток на счете, а также обзор активности и операций)[49].

[48] Важно отличать использование биометрических данных в качестве атрибутов идентичности, а также при идентификации или исключении дубликатов (т.е. для установления идентичности и уникальности физического лица) от их использования в качестве аутентификаторов. Технические стандарты цифровой идентификации (например, Стандарты Национального института стандартов и технологий США) предусматривают только ограниченное использование биометрических данных в целях аутентификации и устанавливают строгие требования и указания в отношении такого использования для решения различных проблем.

[49] См. Д. Шрайер, Т. Харджоно и А. Пентланд, «Поведенческая биометрия», глава 12, «Новые решения для кибербезопасности» (под ред. Х. Шробе; Д. Шрайер и А. Пентланд (MIT Connection Science and Engineering, MIT Press 2017)

– Обязательные (основные) официальные атрибуты идентичности различаются в зависимости от юрисдикции и могут включать в себя: полное официальное имя, дату рождения, место рождения, домашний адрес и уникальный выданный правительством идентификационный номер. Однако правительства обладают значительной степенью свободы при определении атрибутов и доказательств, необходимых для проверки подлинности официальной идентичности в юрисдикции. Подход правительства к определению обязательных атрибутов идентичности может со временем меняться по мере развития технологий и сопутствующего укрепления уверенности в надежности различных типов атрибутов идентичности[50]. Кроме того, при определении обязательных атрибутов идентичности правительства могут учитывать ситуацию в стране и цели расширения доступности финансовых услуг. Например, особенно в развивающихся странах со значительной долей скитающегося или бездомного населения и людей без официальных адресов, правительство может исключить требование об обязательном использовании адреса в качестве основного идентификатора при проверке подлинности официальной идентичности.

(2) ***Валидация*** предполагает определение того, что доказательства являются подлинными (не поддельными или незаконно присвоенными), и что информация, содержащаяся в доказательствах, является точной. Для этого информация об идентичности/доказательства идентичности проверяются по приемлемым (достоверным/надежным) источникам, что позволяет установить, что информация соответствует данным/записям из надежных независимых источников. Например, провайдер идентификационных услуг может (1) проверить физическое доказательство идентичности (документ, удостоверяющий личность), такое как водительские права и/или паспорт или цифровые изображения удостоверения личности соискателя, (a) определить, что изменения отсутствуют, идентификационные номера соответствуют стандартным форматам, физические и цифровые элементы защиты являются действительными и неповрежденными; (b) направить запрос в государственный орган, выдавший водительские права и/или паспорт, о валидации (подтверждении) совпадения информации.

(3) ***Верификация*** предполагает подтверждение того, что валидированная идентичность относится к физическому лицу (соискателю), подлинность личности которого была проверена. Например, провайдер идентификационных услуг может попросить соискателя сделать с помощью мобильного телефона и отправить видео или фотографию, затем сравнить предоставленную соискателем фотографию с фотографией в паспорте или с фотографией, хранящейся в государственной базе данных паспортов или водительских прав, и установить их совпадение с заданным уровнем достоверности. Чтобы привязать доказательство идентичности к реальному человеку-соискателю, провайдер идентификационных услуг может затем отправить код регистрации на подтвержденный номер телефона соискателя, который привязан к его идентичности, потребовать от соискателя предоставить код регистрации провайдеру идентификационных услуг и подтвердить, что представленный код регистрации соответствует коду, отправленному провайдером идентификационных услуг; тем самым будет подтверждено, что соискатель является реальным человеком, во владении и под контролем которого находится подтвержденный номер телефона. После этого соискатель считается идентифицированным.

Регистрация — это процесс, посредством которого провайдер идентификационных услуг регистрирует идентифицированного соискателя в качестве «подписчика» и создает его учетную идентификационную запись. В рамках этого процесса уникальная установленная личность подписчика (то есть атрибуты подписчика) достоверно **привязываются** к одному или нескольким аутентификаторам, которые находятся во владении и под контролем подписчика, с использованием соответствующего **протокола связываний.** Процесс привязки идентификационных данных подписчика к аутентификатору(-ам) также называется «выпуском учетных данных».

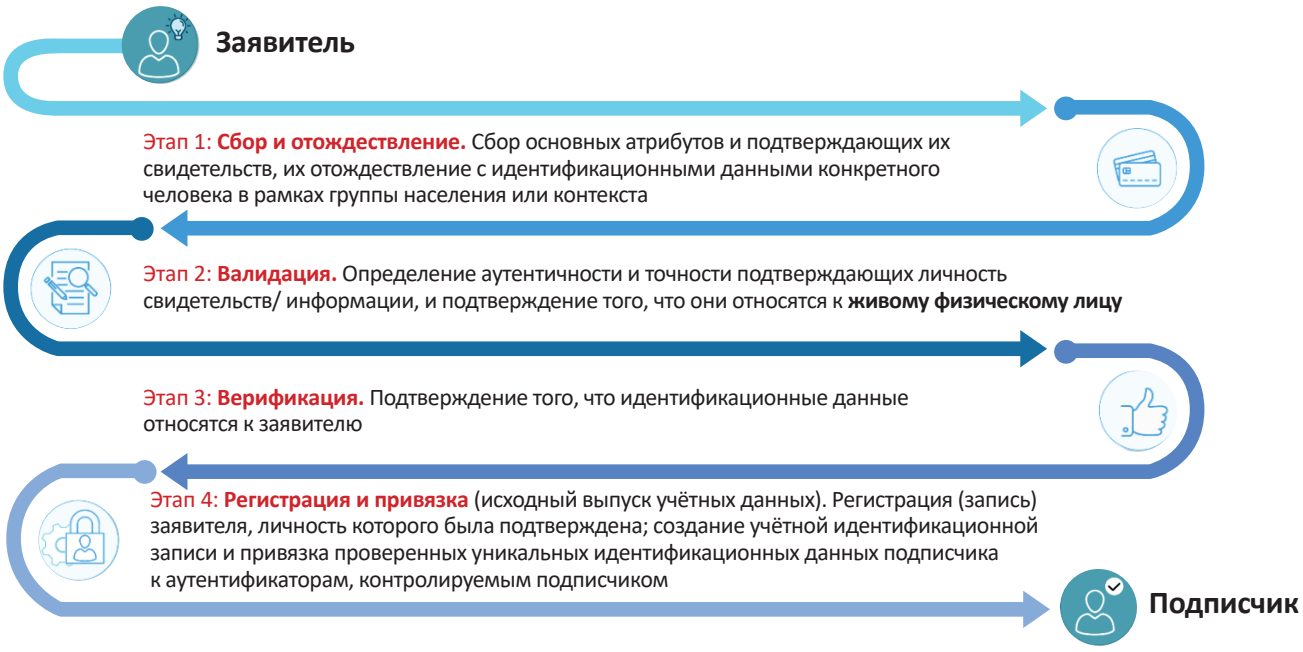
[50] Например, развитие технологии человеко-машинного интерфейса (HCI) (например, комбинирование движения глаз и использования мыши) или тактильных интерфейсов может привести к тому, что правительства некоторых стран в конечном итоге заменят использование традиционных идентификаторов на использование биомеханических атрибутов. В разделе V описывается изменение роли поведенческих биометрических атрибутов в цифровой идентификации/проверке и аутентификации.

Аутентификатор — это то, что находится во владении и под контролем заявителя; как правило, это криптографический модуль, генератор одноразовых кодов или пароль, который используется для аутентификации (подтверждения) соискателя. А точнее, аутентификатор — это то, что находится во владении и под контролем заявителя и используется для аутентификации (подтверждения) того, что заявитель является физическим лицом, которому были выданы учетные данные, и, следовательно (в зависимости от строгости аутентификации системы цифровой идентификации), является (с разной степенью вероятности, определяемой уровнем надежности аутентификации) фактическим подписчиком и владельцем учетной записи. **Учетные данные** — это физический объект или цифровая структура, которая достоверно привязывает установленную личность подписчика, посредством идентификатора(-ов), по крайней мере к одному аутентификатору, который находится во владении и под контролем подписчика. Когда цифровой провайдер идентификационных услуг (действующий в качестве провайдера учетных данных (CSP)) выдает аутентификатор(-ы) и достоверно привязывает аутентификатор(-ы) к личности подписчика, возникший в результате физический объект или цифровая структура является учетными данными.

Обычно провайдер идентификационных услуг выдает аутентификатор(-ы) подписчику и регистрирует аутентификатор(-ы) с привязкой к установленной личности подписчика при регистрации. Однако провайдер идентификационных услуг может также привязать учетную запись подписчика к аутентификаторам, предоставленным подписчиком, приемлемым для провайдера идентификационных услуг (действующего в качестве провайдера учетных данных). Более того, хотя привязка является важной частью надежной регистрации, провайдер идентификационных услуг также может привязывать учетные данные подписчика к дополнительным или альтернативным аутентификаторам на более позднем этапе, в рамках управления жизненным циклом идентификационных данных, о котором речь пойдет ниже.

Проверка и подтверждение личности может осуществляться одним или несколькими провайдерами услуг (см. сводную информацию об участниках системы цифровой идентификации ниже). В первом случае возможно осуществление процесса проверки и подтверждения личности одним учреждением, процессом, методом или технологией. Аналогичным образом, привязка установленных идентификационных данных во время регистрации может быть выполнена одним провайдером услуг или отдельным провайдером услуг, который не осуществляет проверку и подтверждение личности.

Рисунок 5. Проверка и подтверждение личности/регистрация



Элемент 2: Аутентификация

Аутентификация отвечает на вопрос: ***«Являетесь ли вы идентифицированным/проверенным физическим лицом?»*** Она устанавливает, что физическое лицо, которое хочет получить доступ к учетной записи (или к другим услугам или ресурсам) — заявитель — это то же самое лицо, личность которого была проверена, подтверждена и зарегистрирована, оно получило учетные данные и в его владении и под его контролем находятся привязанные учетные данные и, в соответствующих случаях, другие аутентификаторы (т.е. это клиент, принятый на обслуживание). Аутентификация может опираться на факторы и процессы аутентификации разного типа, как описано ниже. Надежность аутентификации зависит от типа используемых факторов аутентификации и безопасности процессов аутентификации[51].

Факторы аутентификации

Традиционно существуют три основных категории факторов аутентификации:

- факторы знания: что-то, что вы знаете — общая неразглашаемая информация (например, имя пользователя, пароль или парольная фраза), персональный идентификационный номер (PIN) или ответ на заранее выбранный секретный вопрос;

- факторы владения: что-то, что вы имеете — криптографические ключи, хранящиеся в аппаратном обеспечении (например, в мобильном телефоне, планшете, компьютере или USB-адаптере) или в программном обеспечении, которым управляет подписчик, одноразовый пароль, сгенерированный аппаратным устройством, или программный генератор одноразовых паролей, установленный на цифровом устройстве, таком как мобильный телефон;

- факторы свойства: что-то, что является частью вас — биофизическая биометрия, такая как распознанное изображение лица и отпечаток пальца или рисунок сетчатки глаза; биомеханическая биометрия, основанная на уникальном способе взаимодействия человека с цифровыми устройствами, например, на манере человека держать мобильный телефон, водить пальцем по экрану, скорости печати на клавиатуре или использовании определенных сочетаний клавиш или жестов; а также расширенная поведенческая биометрия.

Как излагается ниже, в системе цифровой идентификации не обязательно используются все эти типы факторов. Например, несмотря на то что во многих современных системах цифровой идентификации используется биометрия, не следует полагать, что она используется во всех системах цифровой идентификации.

Факторы знания, используемые при аутентификации (что-то, что вы знаете), на самом деле могут не являться секретной информацией. Аутентификация на основе знаний, при которой заявителю предлагается ответить на вопросы, которые предположительно известны только заявителю, не является приемлемой секретной информацией для цифровой аутентификации в соответствии со Стандартами Национального института стандартов и технологий США. Аналогичным образом, фактор свойства, относящийся к биофизической биометрии, не является секретной информацией, и поэтому Стандарты Национального института стандартов и технологий США разрешают использовать биофизическую биометрию для аутентификации только тогда, когда она строго привязана к физическому аутентификатору.

[51] Элементы аутентификации, описанные в данном Руководстве — не то же самое, что «усиленная аутентификация клиентов (SCA)» в соответствии с правовой базой ЕС. То, что является или не является эффективным фактором SCA для целей второй Директивы ЕС о платежных услугах, должно оцениваться в соответствии со второй Директивой ЕС о платежных услугах и Нормативно-техническими стандартами по усиленной аутентификации клиентов и защищенной связи, а не в соответствии с Руководством ФАТФ.

Важно отметить, что новые виды аутентификаторов, основанных на технологиях, и связанных с владением и свойствами (в том числе расширенные аутентификаторы для цифровых устройств, биомеханические биометрические характеристики и **поведенческие биометрические схемы**), многие из которых разрабатывались и использовались или разрабатываются и используются главным образом для борьбы с мошенничеством, потенциально могут значительно усилить процессы аутентификации цифровых удостоверений в целях соблюдения установленных требований ПОД/ФТ[52].

Традиционно (и как отражено в стандартах цифровой идентификации Национального института стандартов и технологий США) аутентификация цифровых удостоверений проводится в определенный момент времени: когда заявитель подтверждает личность клиента/подписчика и запрашивает разрешение на начало цифрового (онлайн-сеанса) или личного взаимодействия для доступа к счету клиента или другим финансовым услугам или ресурсам. Однако в настоящее время многие регулируемые субъекты, в частности, более крупные финансовые учреждения в развитых странах, дополняют традиционную аутентификацию в начале интерактивного взаимодействия решениями «непрерывной аутентификации», в которых используется биомеханическая биометрия, поведенческие биометрические схемы и/или динамический **анализ риска операций.** Вместо того, чтобы, опираясь на комбинацию чего-то, что заявитель имеет/знает или чем он является, установить в начале взаимодействия, что заявитель является клиентом, с которым уже установлены отношения и что он контролирует аутентификаторы/учетные данные, выданные этому клиенту, непрерывная аутентификация направлена на обеспечение того, чтобы определенные данные, собранные в ходе интерактивного взаимодействия, такие как данные геолокации, MAC-адреса и IP-адреса, скорость набора текста и угол наклона мобильного устройства, соответствовали «тому, что следует ожидать», в течение всего сеанса.

Способы измерения влияния (эффективности) технологии непрерывной аутентификации на снижение рисков аутентификации не до конца отлажены, и технические стандарты цифровой идентификации, такие как стандарты Национального института стандартов и технологий США, в настоящее время не учитывают их. Делегированный регламент Европейской Комиссии (ЕС) 2018/389 (Нормативно-технические стандарты усиленной аутентификации клиентов (SCA) и защищенной связи) в соответствии со второй Директивой ЕС о платежных услугах предписывает провайдерам платежных сервисов (ППС) иметь механизмы мониторинга операций, которые позволяют обнаруживать несанкционированные или мошеннические платежные операции с целью выполнения требований в отношении усиленной аутентификации клиентов, изложенных во второй Директиве ЕС о платежных услугах (ст. 2 «Нормативно-технические стандарты»). Кроме того, ППС, которые хотят воспользоваться преимуществами исключения усиленной аутентификации клиентов из «Анализа риска операций» по ст. 18 Нормативно-технических стандартов, должны иметь механизмы мониторинга рисков в режиме реального времени в соответствии со ст. 2 Нормативно-технических стандартов и продемонстрировать, что у них уровни мошенничества ниже конкретных пороговых значений, определенных в Нормативно-технических стандартах[53].

Описание ниже относится к статическим методам аутентификации в конкретный момент времени, к которым применяются Стандарты цифровой идентификации Национального института стандартов и технологий США.

[52] Как отмечено в самом Руководстве, системы цифровой идентификации также представляют значительные риски (включая риски конфиденциальности) и дают возможности для злоупотреблений (например, предвзятости или нарушения прав человека), которые выходят за рамки данного Руководства, но должны эффективно устраняться.

[53] Текст Нормативно-технических стандартов доступен по ссылке: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R0389

Процессы аутентификации

Процессы аутентификации обычно классифицируются по количеству и типу факторов аутентификации, которые необходимы для этого процесса, при этом чем больше факторов используется в процессе аутентификации, тем более надежна система аутентификации. По мере развития технологии/процессов аутентификации это понятие пересматривается и дополняется в соответствии с более современным подходом, основанным на результатах, при котором предполагается многофакторная аутентификация, но степень надежности элемента аутентификации не зависит от *количества* и типов используемых факторов, зато она зависит от устойчивости процессов аутентификации к распространенным и новым типам атак, таким как фишинг и атака через посредника. (Этот более целостный подход, основанный на результатах, должен лучше согласовываться с появлением непрерывной аутентификации.)

Типы протоколов/процессов аутентификации по возрастанию уровней безопасности включают в себя:

- **однофакторную аутентификацию,** при которой для аутентификации личности человека используется только один аутентификатор;

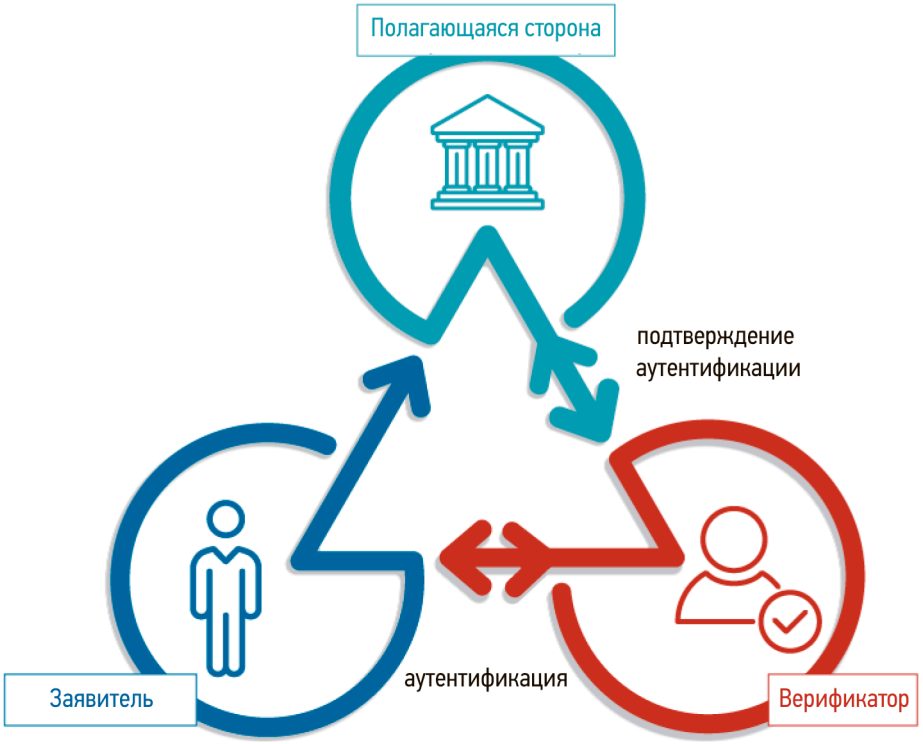
- **многофакторную аутентификацию,** при которой для аутентификации личности заявителя используются два или несколько независимых аутентификатора по крайней мере из двух разных категорий факторов аутентификации (факторы знания/владения/свойства). Например, когда заявитель пытается войти в учетную запись онлайн-банка, используя аутентификатор на основе знаний (например, имя пользователя и пароль), для успешного получения доступа заявителю также необходимо ввести дополнительный фактор аутентификации из другой категории факторов аутентификации. Заявитель может использовать фактор аутентификации на основе владения, такой как секретный ключ, сгенерированный сертифицированным FIDO устройством, встроенным в его мобильный телефон для этой цели. Многофакторная аутентификация может быть реализована с использованием либо нескольких аутентификаторов из разных категорий, которые в комбинации предъявляются непосредственно верификатору, либо одного аутентификатора, в котором присутствует несколько типов факторов, как в случае, когда в аутентификаторе используется один или несколько факторов для защиты фактора другого типа, который, в свою очередь, предъявляется непосредственно верификатору[54].

На приведенном ниже рисунке изображен процесс аутентификации на примере типичной финансовой операции. На этой диаграмме существующий клиент хочет инициировать финансовую операцию и должен сначала доказать с помощью одного или нескольких аутентификаторов, что он/она является тем, за кого себя выдает, т.е. владельцем счета. Клиент (заявитель) подтверждает свое владение аутентификаторами и контроль над ними, связываясь с провайдером идентификационных услуг (верификатором) по защищенному протоколу аутентификации. Верификатор подтверждает (проверяет) аутентификаторы у провайдера учетных данных (CSP) и предоставляет подтверждение аутентификации финансовому учреждению, которое в этой ситуации является полагающейся стороной (ПС).

Примечание: CSP, верификатор и ПС могут быть одним и тем же учреждением (простая двусторонняя аутентификация, состоящая только из заявителя и ПС).

[54] В соответствии со Стандартами Национального института стандартов и технологий США, для усиленной аутентификации требуется либо двухфакторная аутентификация, либо многофакторная аутентификация (MFA), при которой используются два или несколько взаимно независимых фактора аутентификации разных типов, по крайней мере один из которых не подлежит повторному использованию и повторному воспроизведению и не может быть тайно украден через Интернет. Как говорится во 2-й Директиве ЕС о платежных услугах и повторяется в Нормативно-технических стандартах, «усиленная (строгая) аутентификация клиентов» определяется как «аутентификация, основанная на использовании двух или более элементов, классифицированных как знания (что-либо, известное только пользователю), владение (что-либо, чем владеет только пользователь) и свойство (то, чем является пользователь), которые являются независимыми в том смысле, что нарушение одного элемента не ставит под угрозу надежность других и которые разработаны таким образом, чтобы обеспечить конфиденциальность данных аутентификации». В Приложении Е содержится более подробное описание технических стандартов.

Рисунок 6. Цифровая аутентификация



Традиционно, и как отражено в Стандартах Национального института стандартов и технологий США, аутентификация цифровых удостоверений проводится в определенный момент времени: когда заявитель подтверждает личность и запрашивает разрешение на начало цифрового (онлайн-сеанса) или личного взаимодействия, а также доступ к счету или другим финансовым услугам. Однако в настоящее время многие регулируемые субъекты, в частности, более крупные финансовые учреждения в развитых странах, дополняют традиционную аутентификацию в начале интерактивного взаимодействия решениями «непрерывной аутентификации», в которых используется биомеханическая биометрия, поведенческие биометрические схемы и/или «Анализ риска операций».

Управление жизненным циклом идентификационных данных

Управление жизненным циклом идентификационных данных относится к действиям, которые провайдеры идентификационных услуг должны предпринимать в ответ на события, которые могут произойти в течение жизненного цикла аутентификатора подписчика и которые влияют на использование, безопасность и надежность аутентификатора. К таким событиям относятся: выдача и привязка аутентификаторов к учетным данным, при регистрации либо после регистрации, потеря, кража, несанкционированное дублирование, истечение срока действия и аннулирование аутентификаторов и/или учетных данных.

Атрибуты, связанные с удостоверением личности, могут меняться из года в год. Аналитические системы могут обнаруживать сигналы риска, свидетельствующие о том, что удостоверение используется способом, похожим на мошенничество или компрометацию учетной записи (как отмечалось ранее при обсуждении «непрерывной аутентификации»). Некоторые коммерческие системы управления определением идентичности предусматривают функции анализа возможности и способа изменения удостоверения в течение его жизненного цикла.

В приведенном ниже описании используется основанный на функциях термин, провайдер учетных данных, при описании действий, которые следует предпринять в ответ на конкретное событие из жизненного цикла аутентификатора, даже несмотря на то, что один провайдер идентификационных услуг может управлять жизненным циклом аутентификатора, а также осуществлять проверку, подтверждение личности, регистрацию и/или аутентификацию.

- **Выдача и запись учетных данных:** провайдер учетных данных выдает, записывает и хранит учетные данные и связанные с ними данные регистрации в учетной идентификационной записи подписчика на протяжении всего жизненного цикла учетных данных. Как правило, подписчик владеет учетными данными, но провайдер учетных данных/верификатор также может владеть учетными данными. Во всех случаях подписчик в обязательном порядке владеет аутентификатором(-ами), который(-ые), как описывалось выше, используется(-ются) для заявления прав на идентификацию при взаимодействии с Полагающейся стороной.

- **Привязка (выпуск учетных данных):** на протяжении жизненного цикла цифровых идентификационных данных провайдер учетных данных также должен фиксировать все аутентификаторы, которые связаны или были связаны с учетной идентификационной записью каждого из подписчиков, а также информацию, необходимую для контроля попыток аутентификации. Когда провайдер учетных данных привязывает (то есть выдает учетные данные, которые привязывают) новый аутентификатор к учетной записи подписчика после прохождения регистрации, он должен потребовать, чтобы подписчик сначала прошел аутентификацию с таким уровнем надежности аутентификации (или более высоким уровнем), при котором будет использоваться новый аутентификатор.

- **Скомпрометированные аутентификаторы — потеря, кража, повреждение, несанкционированное дублирование:** если подписчик теряет (или иным образом компрометирует) фактор аутентификации, необходимый для многофакторной аутентификации, и его личность была проверена и подтверждена с уровнем надежности идентификации 2 или 3, то подписчик должен повторить процесс проверки и подтверждения личности, подтверждающий привязку аутентификаторов заявителя к ранее подтвержденным доказательствам, прежде чем провайдер учетных данных привяжет замену утраченного аутентификатора к идентичности/учетной записи подписчика. Если подписчик использует многофакторную аутентификацию и теряет один аутентификатор, провайдер учетных данных должен требовать от заявителя аутентификации с использованием оставшихся факторов аутентификации.

- **Истечение срока действия и продление:** провайдер учетных данных может выдавать аутентификаторы, срок действия которых истекает и которые больше не могут использоваться для аутентификации. Провайдер учетных данных должен привязать обновленный аутентификатор до истечения срока действия существующего аутентификатора, посредством процесса, аналогичного начальному процессу и протоколу привязки аутентификатора, а затем отозвать аутентификатор, срок действия которого истекает.

- **Аннулирование (отзыв):** провайдер учетных данных должен незамедлительно аннулировать привязку аутентификаторов, когда удостоверение личности прекращает существование (например, по причине смерти подписчика или из-за обнаружения, что он мошенник); по запросу подписчика; или когда провайдер учетных данных определяет, что подписчик больше не соответствует его квалификационным требованиям.

Элемент 3: Механизмы переносимости и функциональной совместимости (необязательные)

Системы цифровой идентификации могут включать в себя, но не обязательно, элемент, обеспечивающий переносимость официальной процедуры проверки и подтверждения личности. Переносимость идентичности означает, что цифровые идентификационные учетные данные физического лица могут

использоваться для проверки и подтверждения официальной личности при установлении новых клиентских отношений в несвязанных учреждениях частного сектора или государственных учреждениях без необходимости каждый раз получать и проверять информацию, позволяющую установить личность и осуществлять идентификацию/проверку клиента. Переносимость требует разработки совместимых продуктов, систем и процессов цифровой идентификации. Переносимость/ функциональная совместимость может обеспечиваться различными архитектурами и протоколами цифровой идентификации.

Федеративная интеграция — один из способов обеспечения переносимости официальной идентичности. Федеративная интеграция означает использование федеративной цифровой архитектуры и протоколов подтверждения для передачи идентичности и аутентификационной информации по сетевым системам. Архитектура федеративных удостоверений обеспечивает совместимость отдельных сетей, т.е. инфраструктуру, которая связывает отдельные системы в сеть с возможностью взаимодействия. Интерфейс прикладного программирования, который не использует федеративную архитектуру и протоколы подтверждения, является еще одним способом обеспечения переносимости.

Архитектура и протоколы федеративных цифровых удостоверений также разрабатываются и утверждаются в различных юрисдикциях для обеспечения совместимости и переносимости идентичности в многочисленных национальных системах идентификации ограниченного назначения.

Надежная федеративная интеграция и другие подходы к обеспечению переносимости систем цифровой идентификации частного сектора могут иметь много значимых преимуществ. Например, переносимость/ совместимость могут потенциально сэкономить полагающимся сторонам (например, финансовым учреждениям и государственным организациям) время и ресурсы на идентификацию, проверку удостоверений клиентов и управление ими, в том числе на открытие счета и авторизацию доступа к счету клиента. Решения для обеспечения переносимости на основе федеративной интеграции или интерфейса прикладного программирования также могут избавить клиентов от неудобств, связанных с необходимостью проведения процедуры проверки и подтверждения идентификации для каждого несвязанного финансового учреждения или государственной службы, а также снизить риск кражи личных данных, возникающий в результате повторного подвергания риску информации, позволяющей установить личность.

Например, система совместимости в соответствии с Регламентом eIDAS обеспечивает международное сотрудничество и совместимость национальных систем цифровой идентификации. Инфраструктура совместимости, установленная системой eIDAS, создала технические интерфейсы на основе узлов eIDAS, которые играют центральную роль для взаимосвязи между полагающимися сторонами и различными национальными схемами цифровой идентификации, подключенными к этим узлам.

Участники системы цифровой идентификации

Как отмечалось выше, системы цифровой идентификации могут включать в себя разные операционные модели с различными ролями правительства и частного сектора в разработке и эксплуатации системы и/или предоставлении конкретных компонентов, подкомпонентов или процессов.

В таблице ниже описаны основные участники типичной системы цифровой идентификации и их роли. Несмотря на то, что в таблице описывается каждый тип участника в зависимости от его конкретной функции, следует понимать, что в предоставленных правительством системах цифровой идентификации общего или ограниченного назначения правительство напрямую осуществляет (или поручает другому учреждению(-ям) осуществлять от своего имени) все основные функции провайдера/оператора. Аналогичным образом, в системах цифровой идентификации частного сектора одно или несколько учреждений могут выполнять все или некоторые функции провайдера/оператора.

Таблица 2. Участники системы цифровой идентификации

ПРОВАЙДЕРЫ УСЛУГ ИДЕНТИФИКАЦИИ	
Провайдер идентификационных услуг (IDSP)	Обобщающий собирательный термин, который относится ко всем типам учреждений, участвующих в обеспечении и эксплуатации процессов и элементов системы цифровой идентификации. IDSP предоставляют системы цифровой идентификации пользователям и полагающимся сторонам. Как отмечалось выше, одно учреждение может выполнять роли одного или нескольких IDSP.
Провайдер услуг по верификации идентичности (IVSP)	Учреждение, которое осуществляет проверку и подтверждение идентичности (валидирует доказательство и верифицирует привязку подтверждаемого доказательства к соискателю).
Поставщик идентификационных данных (IDP)	Учреждение, которое управляет учетными данными первичной аутентификации подписчика и выдает полагающимся сторонам подтверждения на основе этих учетных данных. Обычно IDP также являются провайдерами учетных данных (CSP), но они могут полагаться на третьи стороны при проверке и подтверждении идентичности и выпуске учетных данных.
Провайдер учетных данных (CSP)	Учреждение, которое выдает подписчикам и/или регистрирует аутентификаторы и соответствующие электронные учетные данные (привязывая аутентификаторы к проверенным удостоверениям) подписчиков. CSP отвечает за хранение идентификационных учетных данных подписчика и всех связанных учетных данных в течение всего жизненного цикла учетных данных, а также за предоставление верификаторам информации о статусе учетных данных. Обычно CSP также выступает в качестве Органа регистрации и Верификатора, но может делегировать определенные процессы регистрации, проверки и подтверждения личности и выдачи учетных данных/ аутентификаторов независимому учреждению, называемому Органом регистрации или Менеджеру идентификации — т.е. CSP может состоять из нескольких независимо функционирующих коммерческих организаций, имеющих разных владельцев. CSP может быть независимым сторонним провайдером или выдавать учетные данные для собственного использования (например, крупное финансовое учреждение или государственная организация). CSP также может оказывать другие услуги, помимо услуг цифровой идентификации, такие как обеспечение выполнения дополнительных мер НПК/ «Знай своего клиента» от имени Полагающейся стороны (ПС).
Орган регистрации (или Менеджер идентификации)	Учреждение, отвечающее за регистрацию. Орган регистрации регистрирует (записывает) соискателя и [учетные данные и] аутентификаторы соискателя после проверки и подтверждения идентичности.

ПРОВАЙДЕРЫ УСЛУГ ИДЕНТИФИКАЦИИ

Верификатор	Учреждение, которое проверяет идентификационные данные Заявителя для Полагающейся стороны (ПС), подтверждая, с использованием протокола аутентификации, что один или несколько аутентификаторов находятся во владении и под контролем Заявителя. Верификатор подтверждает действительность аутентификаторов, взаимодействуя с провайдером учетных данных (CSP), и предоставляет подтверждение по протоколу аутентификации Полагающейся стороне (ПС). В таком подтверждении для ПС содержатся результаты аутентификации и, опционально, информация о Подписчике. Чтобы подтвердить, что заявитель владеет действительными аутентификаторами и контролирует их, Верификатору, возможно, понадобится подтвердить действительность учетных данных, привязывающих аутентификатор(ы) к учетной записи Подписчика. Верификатор должен предоставить механизм, посредством которого ПС может подтвердить достоверность подтверждения, которое Верификатор передает ПС. Функции Верификатора часто реализуется в сочетании с функциями CSP, ПС или их обоих.

ПОЛЬЗОВАТЕЛЬ

Пользователь	Уникальный живой человек, который идентифицирован, зарегистрирован, получил учетные данные и аутентифицирован в системе цифровой идентификации и использует ее, чтобы подтвердить свое (юридическое) удостоверение. Обычно пользователей называют по-разному на разных этапах в системе цифровой идентификации, в зависимости от их роли, определяемой их действиями, по отношению к каждому из трех элементов системы цифровой идентификации, как описано ниже.
Соискатель	Лицо, которое нужно идентифицировать и зарегистрировать. Соискатель — лицо, проходящее процессы проверки и подтверждения идентичности, регистрации/привязки (выпуска учетных данных). Это название применяется к Пользователю с того момента, когда Пользователь подает заявку на цифровую идентификацию и предоставляет доказательства идентичности, и до тех пор, пока идентичность Пользователя не будет проверена и не будет создана учетная идентификационная запись с привязкой к аутентификатору(-ам). После этого Соискатель становится Подписчиком.
Подписчик (субъект)	Лицо, удостоверение которого было проверено и привязано к аутентификаторам, удостоверенным Провайдером учетных данных (CSP) и которое может использовать эти аутентификаторы для подтверждения личности. Подписчики получают аутентификатор(ы) и соответствующие учетные данные от CSP и могут использовать эти идентификатор(-ы) для подтверждения личности.
Заявитель	Подписчик, который заявляет Полагающейся стороне (ПС) права собственности на удостоверение и хочет его проверить, используя протоколы аутентификации. Заявитель — это лицо, которое хочет подтвердить свою личность и получить права, связанные с этой личностью (например, открыть финансовый счет или получить к нему доступ).

Полагающаяся сторона (ПС)	(Физическое или юридическое) лицо, которое полагается на учетные данные или аутентификаторы подписчика либо на подтверждение верификатором удостоверения заявителя в целях идентификации Подписчика с использованием протокола аутентификации. ПС доверяет подтверждению удостоверения на основе источника, времени создания, времени действительности подтверждения с момента создания и соответствующей структуры доверия, которая регулирует политики и процессы CSP и ПС. ПС отвечает за аутентификацию источника подтверждения (например, верификатора) и за проверку достоверности подтверждения. ПС полагается на результаты протокола аутентификации, доверяя удостоверению или атрибутам подписчика при установлении деловых отношений (открытии счета) или при авторизации доступа к счету и/или проведении операции. ПС могут использовать подтвержденное удостоверение подписчика, уровень надежности определения идентичности (IAL), уровень надежности аутентификации (AAL) и уровень надежности федеративной интеграции (FAL), метаданные, предоставляющие информацию о надежности каждого из элементов и процессов цифровой идентификации, а также другие факторы для принятия окончательного решения об идентификации/проверке или авторизации. Типичные ПС включают в себя финансовые учреждения, правительственные департаменты и ведомства.
Провайдер структуры доверия/ доверенный орган	Доверенное учреждение, которое сертифицирует и/или проверяет соблюдение IDSP технических стандартов (процессов и мер контроля) в отношении уровней надежности определения идентичности, аутентификации и федеративной интеграции (IAL, AAL и FAL). Провайдеры структуры доверия также могут отвечать за определение технических стандартов для этих уровней доверия. Кроме того, Провайдеры структуры доверия могут быть государственные организации (например, EC/eIDAS) или доверенные отраслевые организации, такие как Open Identity Exchange (OIX), альянс «Fast Identity Online Alliance» (FIDO) (спецификации и сертификаты для аппаратных, мобильных и биометрических аутентификаторов, которые уменьшают зависимость от паролей и защищают от фишинговых атак, атак через посредника и атак повторного воспроизведения с использованием украденных паролей), Инициатива Kantara или Ассоциация «GSMA» (для устройств мобильной связи).

ПРИЛОЖЕНИЕ B: ПРИМЕРЫ

Вставка 4. Единый уникальный идентификатор (UID) Индии

Особенности системы цифровой идентификации: Единый уникальный идентификатор (UID) в Индии, или Aadhaar — программа идентификации, в которой используется несколько типов биометрических и биографических данных, а также официальные удостоверения личности, где это возможно, для предоставления цифрового идентификатора всем жителям Индии, независимо от возраста или национальности.

Агентство Индии по уникальной идентификации (UIDAI) выпустило мобильное приложение m-Aadhaar, которое генерирует номер «виртуального идентификатора», связанный с номером Aadhaar, но отличный от него, для повышения конфиденциальности и безопасности. И номер Aadhaar, и виртуальный идентификатор могут быть аутентифицированы онлайн, в базе данных Aadhaar или в автономном режиме с использованием QR-кода.

Меры по расширению доступности финансовых услуг: Процесс регистрации в системе Aadhaar UIDAI предусматривает гибкие требования к доказательствам идентичности, что обеспечивает полный охват населения в юрисдикции, где у многих людей нет основных документов, удостоверяющих личность, и основан на биометрии, которая используется для установления уникальности. Регистрация осуществляется при личном присутствии уполномоченными регистраторами по всей стране (главным образом это правительства штатов, центральные министерства, банки и государственные организации), с использованием программного обеспечения для сбора биометрических данных и другого оборудования, указанного UIDAI. Регистраторы обязаны принимать специальные меры для регистрации женщин, детей, пожилых людей, лиц с ограниченными возможностями, неквалифицированных рабочих и рабочих, не являющихся членами профсоюзов, представителей кочевых племен и всех других маргинализированных/уязвимых групп населения, не имеющих постоянного жилья.

UIDAI принимает различные типы документов, удостоверяющих личность, для проверки основных атрибутов при регистрации — 32 типа документов, удостоверяющих личность и содержащих имя и фотографию; 14 типов документов, подтверждающих нахождение в родственных отношениях; 10 типов документов с указанием даты рождения; 45 типов документов с указанием адреса. (См. https://uidai.gov.in/images/commdoc/valid_documents_list.pdf).

Если у человека нет ни одного из «объявленных» документов, удостоверяющих личность, он может зарегистрироваться в системе Aadhaar, если его/ее имя включено в правоустанавливающий семейный документ, а глава этой семьи регистрируется в системе Aadhaar на основании требуемого удостоверения личности — документа, удостоверяющего личность или подтверждающего адрес, — и представляет члена семьи во время его/ее регистрации. Если нет ни документов, подтверждающих нахождение в родственных отношениях, ни других необходимых документов, житель может привлечь Представителей или удостоверителей, чьи личности зарегистрированы Регистратором или региональным офисом UIDAI, и которые могут присутствовать в центре регистрации.

Использование в целях НПК: Важно, что в соответствии с Законом о внесении изменений в Закон о схеме Aadhaar, принятым в июле 2019 года в соответствии с решением Верховного суда от 26 сентября 2018 года, и отменяющем некоторые положения первоначального Закона о схеме Aadhaar по соображениям конфиденциальности, наличие номера Aadhaar по-прежнему обязательно для целей налогообложения и получения государственных пособий, субсидий и услуг, финансируемых за счет Государственного фонда Индии, но более не обязательно для открытия банковского счета (или получения номера мобильного телефона). Зато использование номера Aadhaar в целях НПК является строго добровольным и должно основываться на информированном согласии клиента. Регулируемые субъекты могут проверять идентичность своих клиентов на основании:

(i) аутентификации или верификации номера Aadhaar в автономном режиме, (ii) паспорта или (iii) любых других документов, указанных центральным правительством.

Источник: Всемирный банк

Вставка 5. Перу

Национальная система цифровой идентификации Перу - Национальный регистр идентификации и актов гражданского состояния (Registro Nacional de Identificación y Estado Civil (RENIEC)) - предоставляет услуги цифровой идентификации широкому кругу государственных и частных субъектов из различных секторов, что позволяет им упорядочить верификацию и аутентификацию идентичности, повысить качество предоставления услуг. В финансовом секторе система RENIEC является основной системой для идентификации и проверки клиентов в соответствии с требованиями НПК для платформы электронных денег и мобильных счетов Перу - Billetera Movil (BiM), которая была запущена в феврале 2016 года и обеспечивает такие услуги, как внесение/снятие наличных у агентов, возможность проверить баланс, проводить платежи с карты на карту и зачислять деньги на счет миллионам клиентов.

Источник: Всемирный банк (2018 г.), «Прием на обслуживание на основании цифрового удостоверения»

Вставка 6. Банковские верификационные номера (BVN) Нигерии

Каждый нигериец, имеющий банковский счет, зарегистрирован в системе банковских верификационных номеров (BVN), которая состоит из базы данных биометрических идентификаторов и электронной инфраструктуры «Знай своего клиента» под управлением Нигерийской системы межбанковских расчетов (NIBSS). В базу данных BVN внесены номера более 36 миллионов взрослых граждан, которые могут использовать номер BVN для открытия нового счета в другом банке, открытия онлайн-кошелька или подачи заявки на получение кредита. Это позволило снизить расходы, связанные с принятием на обслуживание, и способствует более здоровой конкуренции на рынке финансовых услуг. Идентификация и проверка клиента с помощью BVN происходит мгновенно и также позволяет проводить удаленную (без личного присутствия) верификацию с помощью мобильных устройств. NIBSS предоставила интерфейсы прикладного программирования (ИПП), позволяющие интегрировать номер BVN с банками и небанковскими поставщиками цифровых финансовых услуг, включая ФинТех-компании по всей стране.

Источник: Всемирный банк

Вставка 7. Мексика: высокие затраты на использование системы идентификации для целей НПК

В Мексике базовой системой идентификации для физических лиц является Clave icanica de Registro Nacional de Población (CURP). Несмотря на то, что она ориентирована на все население и обладает потенциалом для использования биометрических данных, она не является уникальной и не соответствует необходимым уровням надежности для нормативных требований в отношении НПК в Мексике.

Зато карточка избирателей, выпускаемая Национальным избирательным институтом (Instituto Nacional Electoral) каждые десять лет, с 2016 года включает две формы биометрических данных (распознанное изображение лица и отпечатки пальцев), которые представляют меньший риск с точки зрения дублирования, чем система CURP. В соответствии с временным правовым положением, включенным в Ley General de Población, для взрослого населения была разработана карточка «общего назначения» на базе INE, которая должна использоваться в качестве основного источника идентификационных данных для мексиканцев, пока в системе CURP не будут обеспечены уровни надежности, аналогичные уровням надежности карточки INE.

INE разработал сервис, позволяющий третьим сторонам верифицировать учетные данные по базе данных, но стоимость этого сервиса, хотя он и необходим, велика для мелких и средних финансовых учреждений, а также для ФинТех-компаний, желающих работать в стране.

В 2018 году был издан Закон о ФинТех, и, осознавая, что в стране участились случаи кражи идентификационных данных, власти приняли меры для снижения таких рисков, с соблюдением Рекомендаций ФАТФ в отношении НПК. Принятые меры включали использование INE регулируемыми субъектами в качестве основного источника для верификации учетных данных и детализированные правила, касающиеся использования биометрических данных, побуждающие регулируемые субъекты искать адекватные коммерческие решения по цифровой идентификации, отвечающие нормативным требованиям в отношении НПК.

Однако INE была разработана как карточка избирателя, а не как карточка общего назначения для идентификации, и поэтому власти начали согласованно проводить комплексную реформу в отношении цифрового удостоверения личности, чтобы создать официальное цифровое удостоверение, которое может также использоваться в целях НПК.

Источник: Всемирный банк

Вставка 8. УВКБ ООН: цифровые удостоверения личности для беженцев

Согласно оценкам Управления верховного комиссара ООН по делам беженцев (УВКБ ООН), на конец 2018 года в мире насчитывалось 25,9 миллионов беженцев и 3,5 миллиона лиц, ищущих убежище. Страны в развитых регионах приняли 16% беженцев, в то время как треть общемирового количества беженцев (6,7 млн. человек) проживает в наименее развитых странах мира.

Принимающие страны несут основную ответственность за выдачу официальных удостоверений личности беженцам, хотя этим процессом могут руководить уполномоченные и признанные международным сообществом органы.

Проблемы подтверждения идентичности, с которыми сталкиваются беженцы, во многом уникальны. Многие беженцы, прибывая в принимающую страну, не имеют идентификационных документов, так как они были оставлены, потеряны или уничтожены во время бегства. Некоторым беженцам, возможно, официальные удостоверения личности или другие идентификационные документы не выдавались никогда, часто из-за того, что они прибыли из уязвимых регионов или зон конфликта, либо столкнулись с дискриминацией, которая помешала их регистрации. В то же время существует общий принцип, который не позволяет связываться с властями страны происхождения для установления личности беженца без его согласия, а также, если существует риск причинения ему вреда. Таким образом, согласно международным стандартам, при установлении личности беженцев требуется больше опираться на доказательства, полученные при личной подаче заявления, и в ходе собеседования, а также на сведения о стране происхождения заявителя, местную культуру и другую местную информацию. Надежности определения идентичности усиливаются благодаря регулярным контактам и периодическим проверкам, позволяющим контролировать непротиворечивость, управлять рисками и определять идентичность беженца в новом контексте.

Система цифровой идентификации УВКБ ООН используется многими принимающими странами и УВКБ ООН для управления регистрацией и определением идентичности лиц, ищущих убежище, и беженцев. К марту 2020 года более 9 миллионов беженцев в 72 странах были зарегистрированы в системе по биометрическим данным.

Характеристики системы цифровой идентификации

- УВКБ ООН находится в процессе укрепления своей системы цифровой идентификации для лиц, ищущих убежище, и беженцев. Процесс проверки и подтверждения личности, регистрации этих лиц, применяемый УВКБ ООН, описан в Руководстве УВКБ ООН по организации регистрации и установле-

нию личности[55], глава 5.3 «Установление личности человека: проверка документов и сбор данных» и 5.6 «Биометрическая регистрация и фотографии».

- Способы аутентификации, предусмотренные системой цифровой идентификации УВКБ ООН, различаются в зависимости от ситуации в стране и вариантов использования. Учетные идентификационные данные, выданные системой, в основном используются при личных контактах. Учетные идентификационные данные лиц, ищущих убежище, и беженцев различаются в зависимости от требований правительства принимающей страны, но содержат изображение лица и биографическую информацию, которая включает минимальный набор данных и дополнительные элементы, которые однозначно идентифицируют человека. Идентификационные удостоверяющие документы содержат также печатный штрих-код или QR-код и уникальный идентификационный номер для владельца.

- Система цифровой идентификации УВКБ ООН может поддерживать аутентификацию с использованием биометрических данных, которые первоначально использовались для распределения гуманитарной помощи, включая денежные переводы (которые называются мероприятиями по оказанию помощи денежными средствами). Например, в ряде стран Ближнего Востока, включая Иорданию, мероприятия по оказанию помощи денежными средствами осуществляются через банкоматы с использованием оборудования для сканирования радужной оболочки глаза, которое подтверждает личность пользователя.

- В Малайзии и Индонезии власти используют Android-приложение для проверки достоверности удостоверения личности, выданного беженцу УВКБ ООН, а для облегчения верификации идентичности владельца производится сравнивание с фотографией, отображаемой в приложении.

- В Уганде Канцелярия премьер-министра (которая отвечает за регистрацию и идентификацию беженцев и использует систему цифровой идентификации УВКБ ООН) при сотрудничестве с Комиссией по связи Уганды и УВКБ ООН создает систему, которая позволит проводить биометрическую аутентификацию в пунктах продаж сим-карт. На момент написания данного Руководства эта система находилась на стадии тестирования. В Сомали была введена биометрическая аутентификация возвращающихся беженцев при их принятии на обслуживание с целью предоставления финансовых услуг (более подробная информация приводится ниже).

Участники системы цифровой идентификации: Роли участников цифровой системы идентификации УВКБ ООН различаются в зависимости от ситуации в стране.

- В тех случаях, когда УВКБ ООН осуществляет управление регистрацией и определением идентичности беженцев от имени правительства принимающей страны или при возвращении и переселении, УВКБ ООН является единственным контролером данных.

- В других ситуациях применяется гибридное решение: чаще принимающее государство использует систему УВКБ ООН для управления регистрацией и определением идентичности беженцев. В этих обстоятельствах УВКБ ООН предоставляет систему, а правительство принимающей страны и УВКБ ООН совместно являются контролерами данных, и их деятельность регулируется соглашениями о передаче данных.

- В случае использования биометрической системы, как в Египте, Ираке, Иордании, Ливане и Сирии, УВКБ ООН сотрудничает с поставщиком услуг из частного сектора в контексте протокола защиты данных.

Использование в целях НПК и для иных обязательных требований: Система цифровой идентификации УВКБ ООН и выданные ей учетные данные разрешается использовать для идентификации / проверки клиентов при принятии их на обслуживание в различных странах, включая Бурунди, Малави, Иорданию, Нигерию и Замбию[56].

[55] УВКБ ООН «Руководство по управлению регистрацией и определением идентичности» https://www.unhcr.org/registration-guidancehapter5/registration/

[56] УВКБ ООН, «Перемещенные и отключенные» (2019 г.) https://www.unhcr.org/innovation/displaced-and-disconnected/

Центральный банк Сомали согласился применять этот подход к НПК по отношению к возвращающимся беженцам, которые были зарегистрированы в системе УВКБ ООН по биометрическим данным в Кении и других соседних странах. Форму добровольного возвращения, выдаваемую УВКБ ООН возвращающемуся лицу до отъезда в страну убежища, вместе с биометрической идентификационной информацией с использованием системы УВКБ ООН, будет разрешено использовать для идентификации/проверки клиента при открытии банковского счета. Это решение было опробовано в декабре 2018 года при открытии счетов для двух человек, и ожидается, что оно будет использоваться в более широком масштабе поставщиками финансовых услуг в 2020 году.

Уровень надежности системы: Уровень надежности системы УВКБ ООН по цифровой идентификации не проверялся на предмет соответствия структуре доверия и техническим стандартам, которые обсуждались в настоящем Руководстве, однако на момент написания настоящего документа УВКБ ООН заказало проведение внешних оценок экспертами-консультантами и оценивает выводы.

Расширение доступности финансовых услуг: Расширение доступности финансовых услуг для беженцев является важным элементом защиты, обеспечения самостоятельности и адаптации беженцев. В 2016 – 2019 гг. УВКБ ООН распределило 2,4 млрд. долларов США в рамках гуманитарной материальной помощи. В целях расширения доступности финансовых услуг УВКБ ООН стремится осуществлять мероприятия по переводу денежных средств через банковские или мобильные счета получателей (с соблюдением местного законодательства) и отдавать приоритет «открытым» системам, которые привлекают местные рынки и экосистемы, а не инвестировать в «замкнутые» системы, которые делают небольшой вклад в расширение доступности финансовых услуг. Используя цифровые технологии и, в частности, мобильные платформы, УВКБ ООН стремится содействовать расширению доступности финансовых услуг, которое положительно и ощутимо влияет на жизнь беженцев.

Источник: УВКБ ООН

Вставка 9. Китай: система цифровой идентификации создана частным сектором

Особенности и участники системы цифровой идентификации: Компания Ant Financial создала систему цифровой идентификации на основе информации НПК, проверенной Министерством общественной безопасности (МОБ) Китая, а также на других собранных данных, включая распознавание лиц. Имя и идентификационный номер клиента проверяется по официальной базе данных, которую ведет МОБ Китая, для обеспечения точности идентификационной информации. Распознавание лиц (сопоставление с изображениями в действительных документах), многоканальная перекрестная валидация и проверка по «черным» спискам сочетаются с сценариями проведения бизнесом надлежащей проверки клиентов. Каждая проверка основана на непосредственной авторизации пользователя и подтверждается использованием услуг по верификации.

Использование в сфере финансовых услуг: Ant Financial и финансовые учреждения сотрудничают при оказании клиентам финансовых услуг, таких как страхование, субсидирование и микрофинансирование, а также в полной мере используют цифровую идентификацию для предоставления финансовым учреждениям таких услуг, как идентификация клиентов и оценка рисков клиентов. Система цифровой идентификации Ant Financial повсеместно используется в различных сценариях предоставления финансовых услуг, обеспечивая более 3 миллиардов проверок по лицам сотен миллионов пользователей Alipay. Она также используется в связи с запросами пенсий, пенсионными взносами, налоговыми декларациями и другими государственными услугами. Кроме того, Ant Financial предоставляет цифровые идентификаторы для туристов, приезжающих в Китай на короткий срок, которые не имеют счета в китайском банке, но хотят совершать мобильные платежи. Ant Financial принимает специальные меры по верификации идентичности в Иммиграционном бюро для подтверждения подлинности информации, указанной в паспорте.

Уровень надежности системы: В Китае нет прозрачных правовых механизмов надежности и технических стандартов цифровой идентификации, но было предложено, чтобы при оценке в соответствии со Стандартами Национального института стандартов и технологий США система цифровой идентификации Ant Financial имела уровень надежности определения идентичности 2 (IAL2), уровень надежности аутентификации 1 (AAL1) и уровень надежности федеративной интеграции 2 (FAL2).

Меры по расширению доступности финансовых услуг:

(1) Для жителей сельских или отдаленных слаборазвитых районов, не имеющих доступа к банковским счетам или в тех случаях, когда технологии распознавания лиц недостаточно развиты, Ant Fianncial может верифицировать информацию о клиентах с помощью Платформы верификации идентичности граждан. На счет накладываются ограничения (платежи не могут превышать 1 000 юаней), международные платежи не разрешены.

(2) Что касается студентов колледжей, не имеющих доступа к банковским счетам, Ant Financial может проверять личности студентов через Информационную сеть студентов высших учебных заведений Китая, включая учебный статус студентов.

Источник: Китай

Вставка 10. Сингапур: Национальная цифровая идентификационная система

В рамках Национальной цифровой идентификационной системы (NDI) правительство Сингапура разрабатывает пакет услуг цифровой идентификации, позволяющий жителям и организациям Сингапура осуществлять цифровые операции с правительством и частным сектором удобным и безопасным способом. Система NDI основана на технологиях криптографической защиты инфраструктуры открытых ключей (PKI). Услуги постепенно внедряются с 2017 года, и ожидается, что к 2020 году они станут полностью работоспособными.

Особенности системы цифровой идентификации: В пакете услуг NDI различают 4 отдельных уровня.

Достоверные данные: MyInfo — служба достоверных идентификационных данных NDI, которая была запущена в начале 2017 года. MyInfo включает проверенные правительством данные, полученные из различных государственных учреждений, и содержит более 100 разделов с персональными данными. Она обеспечивает гражданам и резидентам доступ к своим данным и управление доступом к своим данным. Люди могут дать согласие на автоматическое внесение своих проверенных правительством личных данных при обращении за электронными услугами в организации государственного и частного сектора посредством надежного и независимого канала.

- Достоверная идентичность: правительством будет учрежден Национальный орган сертификации (NCA), который выдаст каждому жителю цифровое удостоверение с криптографической защитой, созданное в защищенном режиме, хранящееся в мобильном телефоне. Этому цифровому удостоверению могут доверять как государственные, так и частные компании. Это внесет вклад в многоуровневую модель надежности определения идентичности, что позволит пользователям осуществлять более конфиденциальные операции, т.к. повысится уровень надежности определения их идентичности.

- Достоверный доступ: NDI будет поддерживать открытую и интегрированную экосистему провайдеров услуг аутентификации (ASP). Правительство будет обеспечивать услуги одного из ASP, а другие ASP могут эксплуатироваться частным сектором, причем все они будут ссылаться на один

и тот же цифровой идентификатор, выданный правительством. В конце 2018 года была запущена система SingPass Mobile, обеспечивающая безопасную аутентификацию без необходимости использовать аппаратные токены или одноразовые пароли по СМС, что гарантирует расширение доступности цифровых услуг и простоту доступа как для государственного, так и для частного сектора.

- Достоверные услуги: это цифровые услуги на основе уровней системы NDI. Примером является цифровая подпись. Финансовые учреждения могут полагаться на NDI для предоставления более надежных услуг с более высоким уровнем надежности, а также для оптимизации поездок клиентов независимо от границ систем или организаций.

Участники системы цифровой идентификации: Уровни достоверных данных и достоверной идентичности предоставляются правительством. Уровень доверенного доступа будет поддерживать открытую и интегрированную экосистему провайдеров услуг аутентификации и провайдеров электронной цифровой подписи (ASP и DSAP). Правительство будет обеспечивать услуги одного из ASP.

Использование в целях НПК: В настоящее время более 60 финансовых учреждений Сингапура используют MyInfo при оказании более чем 220 цифровых услуг, чтобы принимать клиентов на обслуживание и проводить НПК.

Актуальные нормативные положения в сфере ПОД/ФТ, относящиеся к цифровым идентификаторам: Управление денежного обращения Сингапура выпустило Руководство по использованию MyInfo и применению мер НПК при заочных деловых отношениях (AMLD 01/2018)[57]. В случае использования MyInfo от финансовых учреждений не требуется получать физические документы для верификации идентичности клиента, а также не обязаны отдельно получать фотографию клиента. Управление денежного обращения Сингапура уточнило, что считает MyInfo надежным и независимым источником для проверки имени клиента, уникального идентификационного номера, даты рождения, национальности и адреса проживания. Финансовые учреждения обязаны вести надлежащий учет данных, включая данные, полученные из MyInfo, в соответствии с нормативными требованиями Сингапура.

Уровень надежности системы: При разработке NDI в качестве примеров использовались Стандарты Национального института стандартов и технологий США и Регламент ЕС об электронной идентификации. В NDI уровень надежности будет оцениваться по сравнению с уровнями надежности в системах других стран, поскольку Сингапур открыт для возможностей двустороннего сотрудничества. Для надежности обеспечения аутентификации используются Общие критерии Уровня надежности оценки (EAL) с использованием класса AVA «оценка уязвимости» (AVA_VAN, от 1 до 5).

Расширение доступности финансовых услуг: Система NDI предоставляется бесплатно всем гражданам и резидентам Сингапура и является частью программы расширения доступности финансовых услуг соответствующих государственных учреждений.

Источник: Сингапур

[57] https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Anti_Money-Laundering_Countering-the-Financing-of-Terrorism/Circular-on-MyInfo-and-CDD-on-NFTF-business-relations.pdf

Вставка 11. Южно-Африканская Республика

В связи с возрастающей необходимостью борьбы с мошенничеством и кражей идентификационных данных, а также для выполнения требований в отношении НПК, в 2002 году был создан Южноафриканский информационный центр по банковским рискам (SABRIC). Первоначально состоящий из четырех крупнейших банков, в настоящее время SABRIC включает и другие банки, трех провайдеров инкассаторских услуг и одного провайдера по обслуживанию банкоматов. В 2007 году SABRIC и Министерство внутренних дел (МВД) ЮАР начали сотрудничество по борьбе с преступлениями, связанными с идентификационными данными. Изначально банки устанавливали личность клиента, визуально проверяя зеленое удостоверение личности в виде книжки со штрих-кодом и визуально сравнивая фотографию в нем с внешностью явившегося к ним (потенциального) клиента. Однако у «ручного» метода верификации идентичности были недостатки. Для их устранения члены SABRIC и МВД ЮАР объединили усилия, чтобы обеспечить возможность верификации идентичности клиентов путем сопоставления их отпечатков пальцев непосредственно с данными биометрической базы данных HANIS МВД, которая отправляет ответ «верифицировано» или «не верифицировано». Защищенное соединение для доступа к базе данных МВД ЮАР было установлено в участвующих банковских отделениях через Государственное агентство по информационным технологиям ЮАР (SITA). Банки платят МВД ЮАР за верификацию. В процессе верификации генерируется контрольный след, и система выдает надежную управленческую информацию. К концу 2018 года в проекте приняли участие семь банков и 4 000 филиалов. В настоящее время количество верификаций составляет около 3 миллионов в месяц. Запросы к базе данных МВД ЮАР обычно занимают от 4 до 16 секунд. От 2 до 3,8 процента электронных верификаций оказываются неуспешными, потому что у человека, идентичность которого верифицировалась, не было биометрических данных в HANIS.

Источник: Всемирный банк

Вставка 12. Функциональная совместимость и взаимное признание в рамках Регламента ЕС об электронной идентификации (eIDAS)

Согласно Регламенту ЕС об электронной идентификации (eIDAS), государства-члены могут использовать цифровой идентификатор для доступа к онлайн-услугам. Кроме того, они могут принять решение о привлечении частного сектора к предоставлению решений (средств) цифровой идентификации. В соответствии с принципом взаимного признания, государства-члены обязаны принимать объявленные средства цифровой идентификации других государств-членов, если они разрешают использовать цифровой идентификатор для онлайн-доступа к государственным услугам своей страны, а уровень надежности объявленных средств не ниже того, который необходим для доступа к услуге. Регламент eIDAS определяет три различных уровня надежности (низкий, существенный и высокий) в зависимости от степени доверия к заявленной или объявленной идентичности физического лица.

Источник: Европейская комиссия

Вставка 13. Бельгия: электронные карты и система itsme®

Бельгийская система цифровой идентификации включает элементы как государственного, так и частного секторов. Как более подробно объясняется ниже, правительство предоставляет цифровые учетные идентификационные данные общего назначения, Электронную карту гражданина

Бельгии и Электронную карту иностранца (совместно именуемые «Бельгийскими электронными картами»). Оно также предоставляет платформу для аутентификации цифровой идентичности для системы услуг электронного правительства. Почти все граждане и резиденты Бельгии имеют электронную карту (eCard), которая в настоящее время открывает доступ к широкому спектру более 800 приложений системы услуг электронного правительства, включая приложения Tax-on-Web, социального обеспечения и eHealth, Police-on-web, приложения региональных правительств и онлайн-порталы для муниципалитетов. Кроме того, служба аутентификации цифровой идентичности для частного сектора, itsme®, обеспечивает аутентификацию идентификационных данных на основе мобильного телефона, привязанных к электронной карте и конкретному мобильному телефону и SIM-карте, для участвующих банков и операторов мобильной связи. Существующие клиенты могут использовать itsme® для аутентификации идентичности для входа в свои учетные записи и проведения операций.

Особенности и основные участники системы цифровой идентификации:

Электронные карты

- Регистрация в системе бельгийских электронных карт происходит при личном присутствии. Муниципалитеты/консульства и посольства отвечают за проверку и подтверждение личности, запись (регистрацию), выдачу и доставку электронной карты.
- Правительство Бельгии передает Федеральной службе аутентификации (FAS) удостоверение идентичности в целях получения доступа к услугам электронного правительства. Платформа FAS поддерживает доступ как через Интернет-браузер, так и с мобильного телефона и опирается на стандарт IETF TLS, который обеспечивает сквозное шифрование для криптографической защиты коммуникаций в рамках сети. Аутентификация FAS включает следующие шаги:
  - Гражданин или иностранец пытается войти в систему услуг электронного правительства, введя PIN-код электронной карты физического лица.
  - Интернет-браузер отправляет в FAS сертификат аутентификации, который может быть необходим для верификации сертификата, чтобы обеспечить целостность, действительность и подлинность представленного сертификата проверки подлинности клиента TLS.
  - FAS подтверждает сертификат, позволяя человеку завершить вход в систему и получить доступ к запрошенному приложению системы услуг электронного правительства.

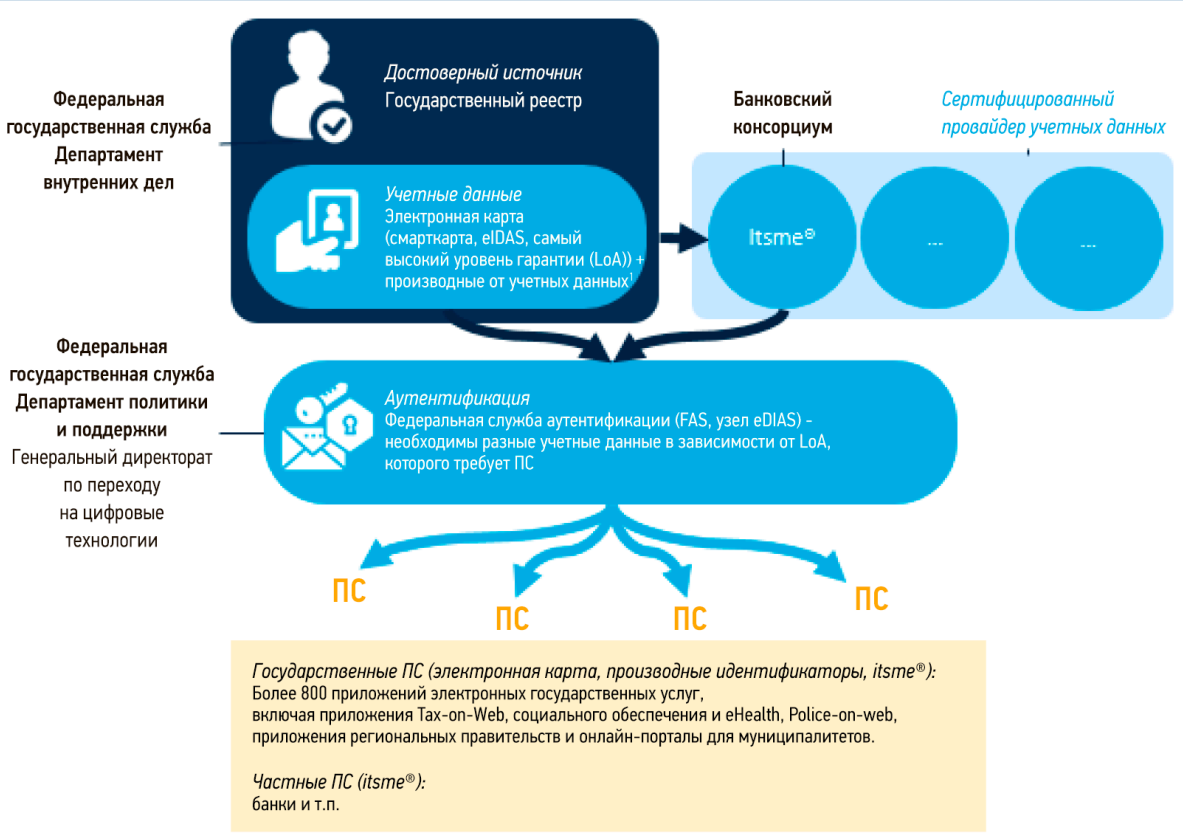
Itsme®

- Itsme® — инициатива Belgian Mobile iD, консорциума, включающего четыре ведущих бельгийских банка (Belfius, BNP Paribas Fortis, ING, KBC) и операторов мобильной связи (Orange, Proximus, Telenet). Активация itsme® на мобильном устройстве привязана к Бельгийской электронной карте, что гарантирует установление личности. В процессе аутентификации передача данных между пользователем itsme® и FAS с использованием приложения itsme® осуществляется в соответствии со стандартом OpenID Connect (Doc Ref. 1.2.4).

Использование в сфере финансовых услуг: Бельгийская платформа FAS предназначена только для доступа к государственным услугам, получение финансовых услуг в настоящее время недоступно. Решение itsme® используется для подтверждения операций.

Уровень надежности системы.

- Бельгийские электронные карты обеспечивают высокий уровень надежности в соответствии со спецификациями Регламента ЕС об электронной идентификации (eIDAS), что подтверждено государствами-членами сети сотрудничества eIDAS после тщательной коллегиальной проверки.
- Система itsme® прошла тщательную проверку в сфере безопасности и управления, и бельгийское правительство признало ее надежным средством аутентификации с высоким уровнем надежности.



[1]После первоначального входа в FAS с помощью электронной карты / считывающего устройства физические лица могут запрашивать другие производные аутентификаторы (одноразовые пароли через мобильное приложение или текст, токены, имя пользователя (пароль), принимаемые некоторыми приложениями, предусматривающими более низкий уровень надежности).

Источник: Бельгия

Вставка 14. Швеция: Платформа электронной идентификации eID и идентификатор BankID

Шведское правительство, которое ведет центральную базу данных удостоверений личности всех граждан и резидентов Швеции, содействует цифровой идентификации посредством государственно-частного партнерства. Правительство предоставляет объединенную архитектуру цифровой идентификации (платформа eID - Техническая платформа Connect Швеции), а частные субъекты, включая банки, выступают в качестве провайдеров цифровых идентификационных услуг, выдавая цифровые удостоверения и предоставляя услуги аутентификации.

Особенности и основные участники системы цифровой идентификации: В состав интеграции входят как провайдеры цифровых идентификационных услуг, так и полагающиеся стороны, которые предоставляют коммерческие товары, услуги или государственные услуги в режиме онлайн. В настоящее время существует четыре провайдера цифровых идентификационных услуг: (1) AB Svenska Pass, (2) BankID, (3) Freja eID и (4) Telia E-identification — несмотря на то, что Telia прекратила запись (регистрацию) физических лиц в целях электронной идентификации осенью 2017 года, выданные учетные цифровые идентификационные данные действительны до истечения срока их действия.

Система BankID, впервые запущенная в 2003 году и управляемая консорциумом из 10 шведских банков, предоставляет клиентам бесплатный цифровой идентификатор, который можно использовать для подтверждения идентичности при проведении операций с участием частного и государственного сектора. Компании, желающие интегрировать BankID со своими услугами, заключают договоры с банками сети BankID и оплачивают услуги BankID, и благодаря этому участвующие банки получают доход. Учетные идентификационные данные доступны в «твердой» форме, т.е. в закодированном виде на интеллектуальном чипе, или в «мягкой» форме, т.е. в виде программы на персональном компьютере, планшете, мобильном телефоне или другом цифровом устройстве пользователя.

Использование в сфере финансовых услуг: Идентификатор BankID может использоваться при принятии клиентов на обслуживание. Чтобы получить BankID впервые, физическое лицо должно пройти документарную НПК, проводимую банком, выпустившим цифровой идентификатор. Полученный идентификатор BankID можно использовать для открытия счета в других финансовых учреждениях. По состоянию на 2016 год BankID фигурировал в 2 миллиардах операций ежегодно, и его использовали более 80 процентов граждан Швеции.

Актуальные нормативные положения в сфере ПОД/ФТ, относящиеся к цифровым идентификаторам: Использование цифрового идентификатора для идентификации/верификации клиента прямо предусмотрено в Законе о ПОД/ФТ (гл. 3, п. 7):

«Подотчетное учреждение обязано идентифицировать клиента и подтвердить его личность с помощью документов, удостоверяющих личность, или выписок из реестров или другой информации и документов из независимого и надежного источника.

При применении первого подпункта могут использоваться инструменты электронной идентификации и удостоверяющих услуг в соответствии с Регламентом ЕС об электронной идентификации (eIDAS). Также могут использоваться другие защищенные процессы удаленной или электронной идентификации, которые регулируют, признают, утверждают или принимают соответствующие органы».

Уровень надежности системы. Шведский Совет по электронной идентификации проводит проверки эмитентов электронных удостоверений в соответствии со шведскими законами об электронных удостоверениях личности (Svensk e-legitimation). Четыре уровня надежности (от 1 до 4) определены в Шведских правовых механизмах надежности электронной идентификации[58].

Источник: Швеция

Справочные материалы: https://elegitimation.se/inenglish/howeidentificationworks.4.769a0b711614b669f2953f.html

[58] https://docs.swedenconnect.se/technical-framework/mirror/digg/Tillitsramverk-for-Svensk-e-legitimation-2018-158.pdf (на шведском языке)

Вставка 15. Италия: государственная система цифровой идентификации

Особенности и участники системы цифровой идентификации: Разработанная в соответствии с Регламентом ЕС об электронной идентификации (eIDAS) и запущенная в 2016 году, итальянская Государственная система цифровой идентификации (SPID) является государственной открытой системой цифровой идентификации, которая позволяет государственным и частным субъектам (поставщикам идентификационной информации), аккредитованным Агентством цифрового развития Италии (AgID), предоставлять услуги регистрации цифровых удостоверений физическим лицам (гражданам или лицам с видом на жительство) в возрасте 18 лет и старше, а также проводить аутентификацию цифровых удостоверений SPID, позволяющих идентифицированному лицу получать доступ к государственным и частным услугам. К марту 2018 года в системе SPID было около 2,5 миллионов цифровых удостоверений. Регистрация в системе SPID может осуществляться лично, через Интернет или с помощью мобильного устройства с веб-камерой, в зависимости от процедур регистрации, предлагаемых данным поставщиком идентификационной информации. Чтобы получить идентификационные учетные данные в системе SPID физическое лицо может предоставить поставщику идентификационных данных действительный документ, удостоверяющий личность (удостоверение личности или паспорт), медицинскую карту, адрес электронной почты и номер мобильного телефона, либо использовать свою цифровую подпись, электронное удостоверение личности (CIE) или национальную сервисную карту (CNS).

Использование в сфере финансовых услуг: Использование SPID является обязательным для организаций государственного сектора и необязательным для организаций частного сектора (коммерческих и финансовых). Согласно анкетированию итальянских банков, проведенному ABI Lab (Итальянской банковской ассоциацией), 38% банков выборки планировали использовать систему SPID для принятия на обслуживание клиентов мобильного банкинга, а 18% планировали начать использовать ее для подключения к интернет-банкингу к концу 2019 года.

Актуальные нормативные положения в сфере ПОД/ФТ, относящиеся к цифровым идентификаторам: Итальянское законодательство разрешает подотчетным учреждениям использовать цифровые идентификаторы, соответствующие требованиям Регламента ЕС об электронной идентификации (eIDAS), такие как SPID, для идентификации и верификации клиентов, являющихся физическими лицами.

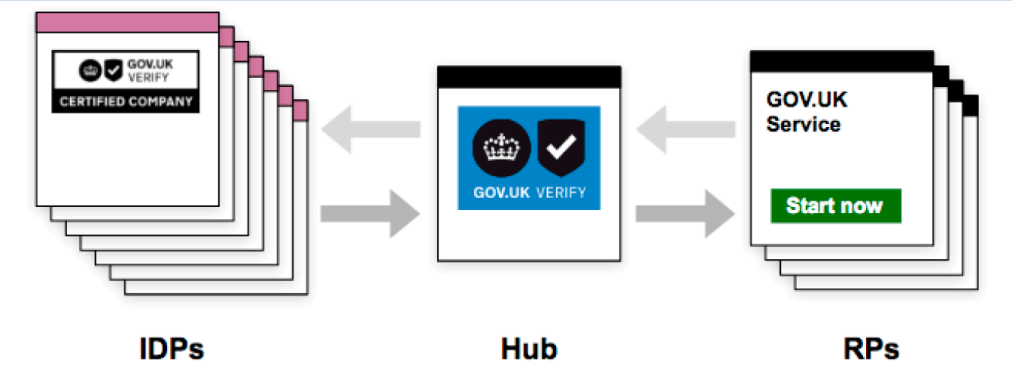
Уровень надежности системы: SPID предлагает три уровня надежности подтверждения идентичности в соответствии со стандартом ISO-IEC 29115. Уровень 1 обеспечивает доступ к онлайн-сервисам с использованием имени пользователя и пароля, выбранных пользователем. Уровень 2, предназначенный для сервисов, требующих более высокой степени безопасности, обеспечивает доступ через имя пользователя и пароль, выбранные пользователем, плюс предполагает генерацию временного кода доступа (одноразового пароля), который можно использовать на цифровом устройстве (например, смартфоне). Уровень 3 предусматривает дополнительные меры безопасности, включая использование физических устройств (например, смарт-карт), предоставляемых менеджером идентификации. Уровень надежности, необходимый для подтверждения идентичности в системе SPID, зависит от уровня безопасности, определенного провайдерами онлайн-услуг.

Источник: Всемирный банк, Банк Италии (Banca d'Italia) и Европейская банковская федерация

Вставка 16. Великобритания: система GOV.UK Verify

В 2012 году правительство Великобритании опубликовало Правительственную цифровую стратегию, в которой было введено понятие «цифровой по умолчанию», т.е. предоставление услуг в Интернете и предоставление широкого доступа тем, кто хочет получить доступ к этим услугам, без исключения тех, кто не может или не желает получать доступ к этим услугам в режиме онлайн. В рамках этой политики «Цифровой по умолчанию» было признано, что необходимо надежное решение для цифровой идентификации, которое позволило бы пользователям удостоверять личность в Интернете, и правительство должно поверить пользователям, что они те, кем себя объявили.

GOV.UK Verify — интегрированная система цифровой идентификации, которая позволяет гражданам и резидентам Великобритании удостоверять свою личность онлайн. В ней используются услуги поставщиков идентификационных данных (IDP) из частного сектора, которые проверяют подлинность идентичности и удостоверяют идентичность физического лица в соответствии с заданным набором требований и спецификаций. В рамках GOV.UK Verify IDP должны обеспечить соответствие государственным и отраслевым стандартам для предоставления услуг надежного определения идентичности.

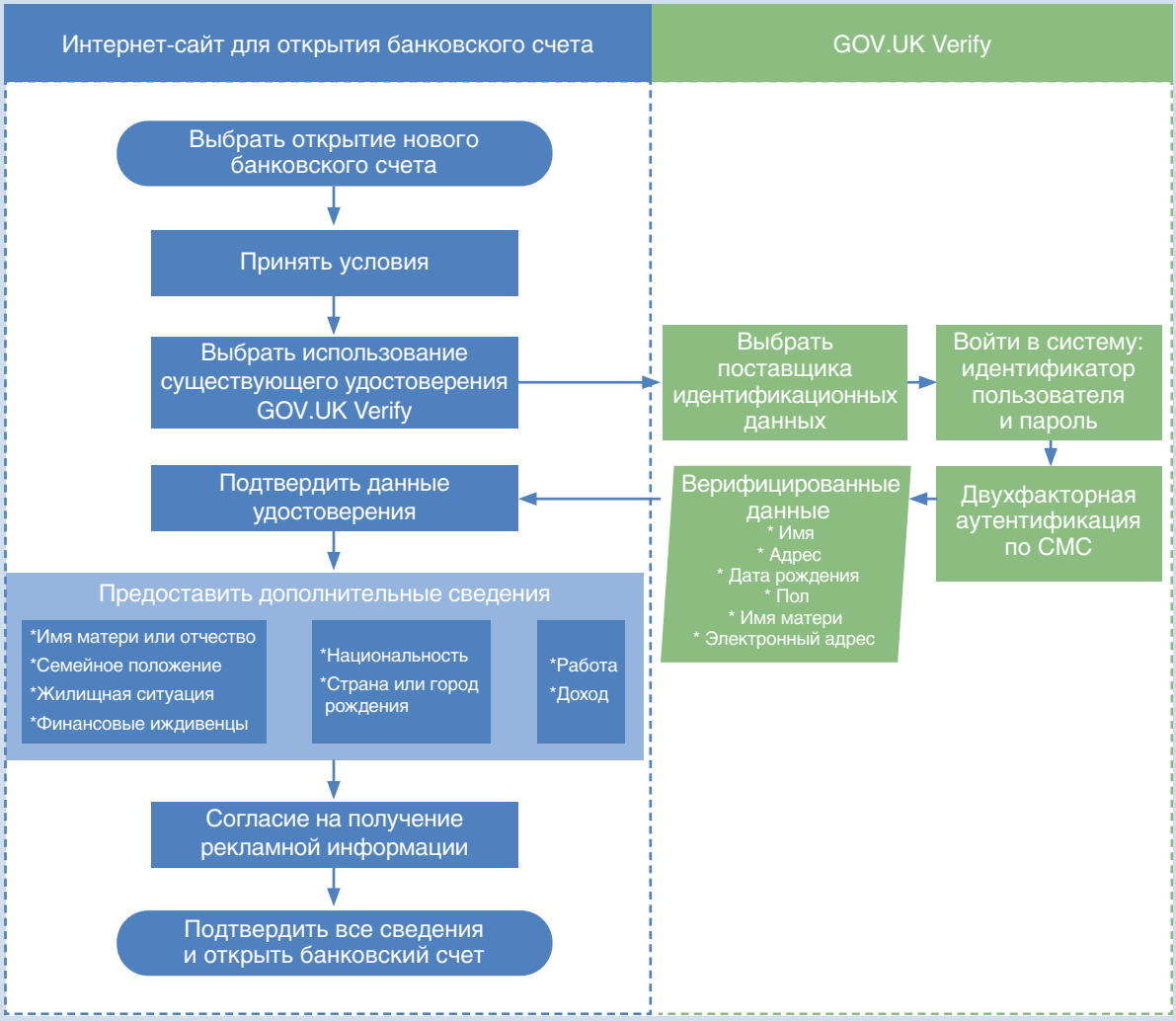


Хаб GOV.UK Verify — это централизованная инфраструктура, которая обеспечивает руководство взаимодействия между пользователями, государственными услугами, IDP и соответствующими службами с целью аутентификации пользователя государственными службами. А также она гарантирует, что к IDP предъявляются необходимые требования по уровню надежности определения идентичности.

Продукт, называемый Службой проверки документов (DCS), является конечной точкой API, которая позволяет IDP запускать проверки документов, выданных правительством Великобритании, по государственным базам данных для обеспечения проверки подлинности идентичности в GOV.UK Verify.

Все учетные записи в GOV.UK Verify требуют как минимум двухфакторной аутентификации.

На диаграмме ниже, разработанной организацией Open Identity Exchange, показан путь открытия банковского счета с использованием системы GOV.UK Verify.



Источник: OIX (2017 г.), https://openidentityexchange.org/wp-content/uploads/2017/01/The-value-of-digital-identity-to-the-financial-service-sector-Full.pdf стр.13

Источник: Великобритания

Вставка 17. Эстония

В Эстонии существует ряд систем цифровой идентификации, в том числе следующие:

- Идентификационная карта (ID-card) — основной удостоверяющий личность документ в Эстонии, обязательный для всех граждан и резидентов, и наиболее широко используемый вариант цифрового идентификатора. ID-карта имеет фотографию и чип, на котором безопасно хранятся личные данные и сертификаты электронно-цифровой подписи с использованием инфраструктуры открытых ключей (PKI).

- Мобильный идентификатор (Mobile-ID) — это услуга цифровой идентификации частного сектора, которую можно использовать с помощью мобильного телефона. Mobile-ID выдается оператором связи с привязкой к SIM-карте и идентификационной карте ID-card. Услугу необходимо активировать на Интернет-сайте Департамента полиции и пограничной охраны Эстонии.

- Смарт-идентификатор (Smart-ID) — это услуга цифровой идентификации частного сектора, которая использует Smart-ID API на мобильном телефоне и серверную службу управления ключами Smart-ID. Smart-ID может выдаваться лицам, у которых есть эстонский персональный идентификационный код. Работает аналогично карте ID-card и идентификатору Mobile-ID при идентификации и проверке клиента.

Участники системы цифровой идентификации:

- Центр разработки государственных информационных систем Эстонии координирует решения для аутентификации цифровой идентичности. Департамент полиции и пограничной охраны Эстонии выдает учетные идентификационные данные (идентификационные карты ID-card, вид на жительство, Digi-ID и Digi-ID электронного резидента) в соответствии с Законом об удостоверениях личности. Министерство иностранных дел отвечает за программу электронного резидентства.

- Две частные компании предоставляют технические решения — Tieto Estonia AS предлагает поддержку пользователей базового программного обеспечения ID-card и SK ID Solutions AS выпускает и проверяет сертификаты электронных идентификаторов eID.

Использование в целях НПК: Эстонские решения для цифровой идентификации используются для идентификации/верификации клиента при приеме его на обслуживание, а также для усиленной проверки клиента в соответствии с Директивой (ЕС) 2015/2366 (вторая Директива ЕС о платежных услугах) и ее регулирующими техническими стандартами для авторизации платежных операций.

Актуальные нормативные положения в сфере ПОД/ФТ, относящиеся к цифровым идентификаторам: В Эстонии клиент может быть принят на обслуживание при личном визите, с помощью информационных технологий (прием на обслуживание по видеосвязи) и с использованием двух различных источников верификации идентичности. В законодательстве не определено какими должны быть эти два средства верификации, но Управление финансового надзора Эстонии выпустило соответствующее руководство[59], в котором говорится, что решение цифровой идентификации (то есть информация, полученная посредством аутентификации с использованием цифрового идентификатора) может быть одним из таких источников (пункт 4.3.1.22), но должен быть один дополнительный источник информации (пункт 4.3.1.23) для верификации личности клиента.

Уровень надежности системы: Все указанные эстонские схемы eID имеют высокий уровень надежности согласно Регламенту ЕС об электронной идентификации (eIDAS).

Источник: Эстония

[59] www.fi.ee/sites/default/files/2019-01/FI%20rahapesu%20t%C3%B5kestamise%20juhend%202018%20%28EN%29_pdf.pdf

ПРИЛОЖЕНИЕ C: ПРИНЦИПЫ ИДЕНТИФИКАЦИИ В ЦЕЛЯХ УСТОЙЧИВОГО РАЗВИТИЯ

В настоящем Руководстве освещаются несколько конкретных способов, с помощью которых страны могут разрабатывать экосистемы цифровой идентификации и использовать преимущества этих систем, одновременно снижая риски, описанные в Разделе IV. Прежде всего страны должны следовать десяти «Принципам идентификации в целях устойчивого развития», которые в настоящее время одобрены более чем 25 международными организациями, агентствами по вопросам развития и другими партнерами[60]. Несмотря на то, что эти Принципы были разработаны в целях содействия созданию «хороших» признанных правительством систем идентификации, они применяются более широко и могут предоставляться и использоваться как государственными, так и частными системами и службами идентификации.

Таблица 3. Принципы идентификации в целях устойчивого развития

	ПРИНЦИПЫ
РАСШИРЕНИЕ ДОСТУПНОСТИ: УНИВЕРСАЛЬНЫЙ ОХВАТ И ДОСТУПНОСТЬ	1. Обеспечение универсального охвата физических лиц на протяжении всей жизни, без дискриминации. 2. Устранение барьеров для доступа и использования, а также различий в доступности информации и технологий.
РАЗРАБОТКА НАДЕЖНОЙ, БЕЗОПАСНОЙ, БЫСТРО РЕАГИРУЮЩЕЙ И УСТОЙЧИВОЙ СИСТЕМЫ	3. Создание надежной — уникальной, безопасной и точной — идентификации. 4. Создание платформы, отвечающей потребностям различных пользователей. 5. Использование открытых стандартов и обеспечение независимости от поставщиков и технологий. 6. Защита неприкосновенности частной жизни пользователя и контроль посредством проекта системы. 7. Планирование финансовой и операционной устойчивости без ущерба для доступа.
РУКОВОДСТВО: СОЗДАНИЕ АТМОСФЕРЫ ДОВЕРИЯ ПУТЕМ ЗАЩИТЫ НЕПРИКОСНОВЕННОСТИ ЧАСТНОЙ ЖИЗНИ И ПРАВ ПОЛЬЗОВАТЕЛЯ	8. Защита конфиденциальности и безопасности данных и прав пользователей посредством создания всесторонней нормативно-правовой базы. 9. Определение четких ведомственных полномочий и ответственности. 10. Обеспечение правовых рамок и основы доверия посредством независимого надзора и рассмотрения жалоб.

[60] Всемирный банк. 2017 г. «Принципы идентификации в целях устойчивого развития: к эпохе цифровых технологий». Вашингтон, округ Колумбия: Группа Всемирного банка http://id4d.worldbank.org/principles. Перечень подписавших организаций приводится на сайте.

Цель 1. Обеспечение расширения доступности

Первые два принципа обеспечивают охват всех без исключения системами идентификации, в соответствии с ЦУР 16.9. *Принцип 1* предписывает странам выполнять свои обязательства по предоставлению услуг правовой идентификации всем резидентам — не только гражданам — на протяжении всей жизни и без дискриминации, в соответствии с международным правом и конвенциями, а также их собственными законодательными базами. Сюда входит обязательство всеобщей регистрации всех родившихся на их территории или в юрисдикции, а также распространяется на систему цифровой идентификации, особенно когда они являются непременным условием для получения доступа к основным услугам государственного и частного сектора, таким как банковские операции, SIM-карты и денежные переводы.

Осознавая тот факт, что определенные группы населения будут сталкиваться с несоразмерными трудностями при доступе к услугам идентификации — и, в частности, к цифровым услугам — *Принцип 2* предписывает исполнителям выявлять и устранять правовые, процедурные и социальные барьеры для регистрации в системах цифровой идентификации и их использования, уделяя особое внимание неимущим и тем группам населения, которые могут подвергаться риску исключения по культурным, политическим или другим причинам (таким как женщины и представители сексуальных меньшинств, дети, сельское население, представители этнических меньшинств, лингвистические группы и группы по вероисповеданию, лица с ограниченными возможностями, мигранты, вынужденные переселенцы и лица без гражданства). Кроме того, системы цифровой идентификации и идентификационные данные не должны использоваться в качестве инструмента для дискриминации или ущемления индивидуальных или коллективных прав.

Цель 2. Разработка надежных, безопасных, быстро реагирующих и устойчивых систем идентификации

Помимо обеспечения всеобщего охвата, системы цифровой идентификации должны быть неуязвимы к мошенничеству и ошибкам, полезными для различных заинтересованных сторон и устойчивыми, а также защищать неприкосновенность частной жизни пользователей и использовать открытые стандарты, что способствует инновациям и позволяет избежать жесткой привязки к конкретным поставщикам и технологиям.

В частности, *Принцип 3* гласит, что точная и актуальная идентификационная информация имеет важное значение для обеспечения достоверности идентичности и атрибутов, используемых при операциях. Кроме того, идентичности должны быть уникальными для данного контекста и не дублироваться, и не должны использоваться идентификаторы, которые могут быть приписаны нескольким людям. Кроме того, системы цифровой идентификации должны быть защищены от подделки (внесения исправлений или других несанкционированных изменений в данные или регистрационную информацию), кражи идентификационных данных, неправомерного использования данных и других ошибок, возникающих в течение жизненного цикла идентификационных данных.

Принцип 4 подчеркивает необходимость гибкости, масштабируемости услуг идентификации, аутентификации и их соответствия потребностям и интересам людей (пользователей) и полагающихся сторон (например, государственных учреждений и частных компаний). Для обеспечения соответствия систем и услуг, связанных с идентификацией, конкретными потребностями пользователей, исполнители должны привлекать общественность и заинтересованные стороны на протяжении всего процесса планирования и внедрения. Ценность цифровых систем идентификации для полагающихся сторон в значительной степени зависит от их способности к переносу и оперативной совместимости с несколькими модулями — при условии соблюдения надлежащих мер обеспечения конфиденциальности и безопасности — как внутри страны, так и за ее пределами.

В частности, что касается признанных на государственном уровне систем цифровой идентификации, в *Принципе 5* дополнительно подчеркивается необходимость независимости от поставщиков для повышения гибкости и недопущения разработки систем, не соответствующих назначению или целям политики и развития. Для этого требуются четкие руководящие указания по закупкам, способствующие конкуренции и инновациям, предотвращающие возможную жесткую привязку к конкретным поставщикам и технологиям, что может увеличить затраты и уменьшить гибкость для учета изменений, происходящих с течением времени. Кроме того, открытые принципы разработки обеспечивают рыночную конкуренцию и инновации. Они необходимы для повышения эффективности и улучшения функциональных возможностей систем цифровой идентификации, а также для обеспечения долговременной эксплуатационной совместимости. Аналогичным образом открытые ИПП (API) также способствуют эффективному обмену данными и способности к переносимости, обеспечивая возможность замены элемента системы цифровой идентификации — например, определенного типа учетных данных — с минимальным прерыванием работы.

Помимо быстро реагирующей на изменения и гибкой архитектуры, *Принцип 6* подчеркивает, что системы цифровой идентификации должны защищать неприкосновенность частной жизни людей и контролировать их данные посредством проекта системы. Это имеет решающее значение для снижения многих рисков нарушения конфиденциальности и защиты данных, указанных в разделе IV настоящего Руководства. Разработка с учетом неприкосновенности частной жизни людей означает, что от физического лица не требуется никаких действий для защиты своих личных данных. Информация должна быть по умолчанию защищена от ненадлежащего и несанкционированного использования с помощью как технических стандартов, так и превентивных деловых практик.

Эти меры должны дополняться жесткой правовой базой (как подчеркивается ниже в Принципе 8).

Например, данные, собираемые и используемые для идентификации и аутентификации, должны соответствовать цели, быть соразмерными сценарию использования и контролироваться в соответствии с международными нормами защиты данных, такими как Принципы честного использования данных (FIP) ОЭСР, и со ссылкой на появляющиеся лучшие международные практики, такие как Общий регламент о защите персональных данных (GDPR) или Закон штата Калифорния о защите конфиденциальности покупателей. Протоколы аутентификации должны только подтверждать или не подтверждать заявленную идентичность или, если это предусмотрено законодательством о ПОД или ПФТ, раскрывать только минимальный объем данных, необходимых для совершения операции. Метод аутентификации должен отражать оценку уровня риска в операциях и может основываться на признанных международных стандартах и основах для определения уровней надежности. Кроме того, системы учетных данных и нумерации идентификаторов не должны без необходимости раскрывать уязвимую личную информацию (например, идентификационные номера должны быть случайными).

В *Принципе 7* признается важность разработки государственных систем, устойчивых в финансовом и операционном отношении и при этом по-прежнему доступных для людей и полагающихся сторон. Они могут включать различные бизнес-модели, в том числе предполагающие разумную и соответствующую плату за услуги по верификации идентичности, расширенные или ускоренные услуги для пользователей, тщательно спроектированные и управляемые партнерства с участием государства и частного сектора (ГЧП), возмещение затрат за счет повышения эффективности и производительности и сокращения утечек данных, а также другие источники финансирования, которые не ставят под угрозу доказательства подлинности идентичности, доступные для всех и отвечающие потребностям населения и полагающихся сторон.

Цель 3. Создание атмосферы доверия путем защиты неприкосновенности частной жизни и прав пользователя

Последняя группа принципов касается способов управления системами цифровой идентификации, позволяющих защитить неприкосновенность частной жизни и права пользователей, обеспечить безопасность системы, а также четкую ответственность и контроль.

В *Принципе 8* изложены требования к всесторонней правовой базе. Системы цифровой идентификации должны опираться на обязательные меры, законы и нормативные акты, которые повышают доверие к системе, обеспечивают конфиденциальность и безопасность данных, снижают количество злоупотреблений, таких как несанкционированное наблюдение в нарушение надлежащей процедуры, и обеспечивают ответственность провайдера. Это, как правило, предполагает законодательные и нормативные акты о самой системе цифровой идентификации, а также законы и нормативные акты, в частности, о защите данных, цифровом или электронном правительстве, электронных операциях и торговле, ПОД, регистрации актов гражданского состояния, системах идентификации ограниченного назначения и свободе информации.

Законы и нормативные акты о системах цифровой идентификации должны четко описывать назначение системы, ее элементы, роли и обязанности различных заинтересованных сторон, определять, как и какие данные следует собирать, ответственность и средства для владельцев цифровых идентификаторов (субъектов) и полагающихся сторон, обстоятельства, при которых данные можно передавать, определять порядок исправления неточных атрибутов данных, способ расширения доступности и обеспечения отсутствия дискриминации. Законы и нормативные акты о защите данных и неприкосновенности частной жизни должны также включать надзор со стороны независимого надзорного органа (например, национальной комиссии по обеспечению конфиденциальности), наделенного соответствующими полномочиями по защите субъектов от несанкционированного доступа и использования их данных третьими сторонами в целях коммерческого наблюдения или составления профиля без осознанного согласия или законной цели. Правовые рамки требуют хорошей сбалансированности регулятивных и саморегулируемых моделей, которые не подавляют конкуренцию, инновации или инвестиции.

Кроме того, в *Принципе 9* подчеркивается необходимость четких институциональных мандатов и отчетности для управления системами цифровой идентификации. Структуры доверия в масштабах всей экосистемы должны устанавливать и регулировать механизмы управления системами идентификации. Сюда входит определение условий и положений, регулирующих институциональные отношения между участвующими сторонами таким образом, чтобы права и обязанности каждой из них были понятны для всех. Должна быть четкая ответственность и прозрачность в отношении ролей и обязанностей провайдеров систем идентификации.

Наконец, в *Принципе 10* подчеркивается, что система идентификации должна включать четкие механизмы контроля соблюдения этих правовых и нормативных требований. Использование систем идентификации должно подвергаться независимому контролю (для обеспечения эффективности, прозрачности, недопущения злоупотреблений и т.п.), что гарантирует, что все заинтересованные стороны надлежащим образом используют системы идентификации по назначению, осуществляют мониторинг и реагируют на потенциальные утечки данных, а также получают претензии физических лиц или опасения по поводу обработки персональных данных. Кроме того, споры относительно идентификации и использования персональных данных, которые не могут быть в штатном режиме разрешены провайдерами — например, отказ зарегистрировать человека или исправить данные, либо отрицательное решение по юридическому статусу физического лица — должны быстро подвергаться малозатратной проверке независимыми административными и судебными органами, имеющими полномочия для внесения надлежащих корректировок.

ПРИЛОЖЕНИЕ D: ОРГАНИЗАЦИИ, УСТАНАВЛИВАЮЩИЕ ТЕХНИЧЕСКИЕ СТАНДАРТЫ И МЕХАНИЗМЫ НАДЕЖНОСТИ ЦИФРОВОЙ ИДЕНТИФИКАЦИИ

Этот список не включает национальные или региональные организации, такие как Регламент ЕС об электронной идентификации (eIDAS) и Национальный институт стандартов и технологий США (NIST), которые также разработали структуры и стандарты на национальном/региональном уровне — см. Приложение E.

Международная организация по стандартизации (ISO) — независимая международная организация, находится в Женеве, состоящая из 163 национальных органов по стандартизации (по одному на страну), которая разрабатывает добровольные, согласованные, востребованные на рынке международные стандарты, определяющие спецификации продукции, услуг и систем, гарантирующие качество, безопасность и эффективность, и поддерживающие инновации. Некоторые из соответсвующих стандартов включают: проверку и подтверждение личности, регистрации физических лиц (ИСО/МЭК 29003:2018); структуру проверки аутентификации субъекта (ИСО/МЭК 29115:2013 — в стадии пересмотра) и применение Руководства по управлению рисками (ИСО 3100:2018) для рисков, связанных с идентификацией. Через свою недавно созданную Рабочую группу 7 Технического комитета TC68[61] Международная организация по стандартизации в настоящее время работает над созданием глобальных стандартов по идентификации физических лиц, в том числе в цифровом контексте.

Международный союз электросвязи (МСЭ) — специализированное учреждение Организации Объединенных Наций по информационным и коммуникационным технологиям (ИКТ), созданное для упрощения установления международных соединений в сетях связи. МСЭ распределяет глобальный спектр радиочастот и спутниковые орбиты и разрабатывает технические стандарты, обеспечивающие беспрепятственное соединение сетей и технологий ИКТ в международном масштабе.

Консорциум Всемирной паутины (W3C) — международная организация, которая разрабатывает и продвигает широкий спектр добровольных согласованных открытых технических стандартов и протоколов для сети Интернет, обеспечивающих оперативную совместимость, масштабируемость, стабильность и отказоустойчивость. В области цифровых идентификаторов W3C разработала стандарт браузера/платформы Web-аутентификации для МФА, используя биометрические данные, мобильные устройства и ключи безопасности FIDO, а также разрабатывает стандарты для верифицированных идентификационных заявок в децентрализованных системах идентификации.

Альянс «Fast Identity Online Alliance» (FIDO) — отраслевая ассоциация, которая продвигает эффективные и простые в использовании решения для усиленной аутентификации путем разработки технических спецификаций, определяющих открытый масштабируемый совместимый набор механизмов для аутентификации пользователей; отраслевые операционные программы сертификации, обеспечивающие успешное принятие спецификаций во всем мире; и сформированные технические спецификации для признанных организаций по разработке стандартов (например, ИСО, МСЭ X.1277 и X.1278) для формальной стандартизации. FIDO также участвует в разработке стандартов верификации через свою Рабочую группу по верификации и виртуальным каналам (IDWG).

Фонд «OpenID Foundation (OIDF) — независимая от технологий некоммерческая торговая организация, которая занимается продвижением услуг цифровой идентификации на основе открытых стандартов.

[61] ISO/TC68 — Технический комитет в составе Международной организации по стандартизации (ISO), на который возложена задача разработки и соблюдения международных стандартов, охватывающих банковскую сферу, рынок ценных бумаг и другие финансовые услуги.

Ассоциация «GSMA» — международная отраслевая ассоциация операторов мобильной связи, которая занимается разработкой различных технических стандартов для платформ мобильной связи, включая стандарты идентификации и аутентификации пользователей.

Европейский институт телекоммуникационных стандартов (ETSI) — один из трех основных европейских органов стандартизации, наряду с Европейским комитетом по стандартизации (CEN) и Европейским комитетом электротехнической стандартизации (CENELEC). ETSI предоставляет своим членам открытую и инклюзивную среду для разработки, ратификации и тестирования международных стандартов для систем и услуг ИКТ во всех секторах промышленности и общества. ETSI работает над проверкой и подтверждением личности, в первую очередь направленной на трастовые услуги, определенные в Регламенте ЕС об электронной идентификации (eIDAS), которая потенциально применима в других областях, таких как выдача электронных идентификаторов и НПК. ETSI разработал набор стандартов для реализации требований Нормативно-технических стандартов в соответствии со второй Директивой ЕС о платежных услугах для использования проверенных сертификатов, определенных в Регламенте ЕС об электронной идентификации (eIDAS) для идентификации третьих сторон платежных операций.

ПРИЛОЖЕНИЕ E: ОБЗОР ТЕХНИЧЕСКИХ СТАНДАРТОВ И ПРАВОВЫХ МЕХАНИЗМОВ НАДЕЖНОСТИ ЦИФРОВОЙ ИДЕНТИФИКАЦИИ В США И ЕС

Национальный институт стандартов и технологий США (NIST) — Соединенные Штаты Америки

- Уровень надежности определения идентичности (IAL) относится к надежности процесса проверки и подтверждения личности, определяемому техническими требованиями к цифровой идентификации, которые предусмотрены. Уровни надежности проверки подлинности личности в порядке повышения надежности: IAL1, IAL2 и IAL3.
- Уровень надежности аутентификации (AAL) — надежность процесса аутентификации. Уровни надежности аутентификации (и управления жизненным циклом учетных данных) в порядке повышения надежности: AAL1, AAL2 и AAL3.
- Уровень надежности федеративной интеграции (FAL) (если применимо) — надежность объединенной сети, т.е. надежность (мощность) оператора контроля, используемого для передачи результатов аутентификации и атрибутов идентификатора в объединенной среде. Уровни надежности федеративной интеграции в порядке повышения надежности: FAL1, FAL2 и FAL3.

Доказательство идентичности

Вставка 18. Эффективное использование технических стандартов цифровой идентификации Национального института стандартов и технологий США (NIST) для оценки надежности доказательства идентичности

IAL1: требование о привязке соискателя к конкретной реальной идентичности отсутствует, т.е. нет никакой надежности, что соискатель является тем, кем он себя объявляет, потому что доказательства идентичности не требуется. Это означает, что:

- Атрибуты идентичности не требуются.
- Соискатель может, но не должен, самостоятельно заявлять атрибуты идентичности.
- Если какие-либо атрибуты предоставлены или собраны, они либо заявленные самостоятельно, либо рассматриваются как самостоятельно заявленные и не оценивается правильные ли они, не верифицируются.

IAL2: имеется высокая степень доверия к тому, что доказательства идентичности подлинные, содержащаяся в них информация об атрибутах точная и относится к соискателю.

- Доказательства атрибутов идентичности собираются на основе качества доказательств (слабых, достаточно убедительных, убедительных и очень убедительных) и количества документов или цифровой информации, на которые можно полагаться.
- Доказательства идентичности оцениваются как подлинные.
- Доказательства идентичности и атрибуты идентичности, которые они содержат, подтверждают существование заявленной идентичности в реальном мире.

- Доказательства идентичности верифицируются, подтверждая, что валидированная идентичность относится к физическому лицу (соискателю), включая подтверждение адреса.
- Проверка и подтверждение личности может быть или очная, или удаленная. Примечание. В Стандартах цифровой идентификации Национального института стандартов и технологий США (NIST) «очная» проверка подлинности личности включает **контролируемые удаленные взаимодействия** с соискателем, а также взаимодействия, когда соискатель и провайдер идентификационных услуг физически присутствуют в одном и том же месте (см. описание ниже).
- Биометрия не является обязательной.
- В тех случаях, когда физическое лицо не может выполнить обычные требования по доказательству идентичности, такие как требования к удостоверению личности, для проверки подлинности идентичности соискателя может привлекаться доверенный поручитель.
- Доказательства атрибутов идентичности должны соответствовать определенным требованиям к качеству доказательств, допускающим различные комбинации необходимого количества доказательств с заданными показателями строгости, определяемыми указанными характеристиками.

IAL3: имеется очень высокая степень доверия к тому, что доказательства идентичности подлинные и точные, атрибуты идентичности относятся к реальному человеку, и соискатель является физическим лицом, надлежащим образом связанным с идентичностью этого реального человека.

- Проверка подлинности идентичности должна быть очной. Примечание. «Очная» проверка подлинности идентичности включает контролируемые удаленные взаимодействия с соискателем, а также взаимодействия, когда соискатель и провайдер идентификационных услуг физически присутствуют в одном и том же месте. (См. описание заочного (без личного присутствия) принятия на обслуживание в разделе III.)
- Требования к качеству проверки подлинности идентичности более строгие.
    - Требуется больше дополнительных доказательств идентичности с большей строгостью.
    - Биометрия является обязательной. Атрибуты биометрической идентичности и биометрические процессы необходимы для обнаружения мошеннических или дублирующихся учетных записей и для привязки верифицированной идентичности к учетным данным.
- Атрибуты идентификации должны быть верифицированы уполномоченным и квалифицированным представителем провайдера учетных данных (CSP).

Источник: Стандарты Национального института стандартов и технологий США (NIST)

Таблица 4. Перечень требований к доказательству идентичности для уровней IAL1, IAL2 и IAL3

Требование	IAL1	IAL2	IAL3
Присутствие	Требования отсутствуют	Личное и неконтролируемое удаленное присутствие	Личное и контролируемое удаленное присутствие
Подтверждение	Требования отсутствуют	• Минимальные атрибуты, необходимые для подтверждения идентичности. • Для повышения степени уверенности может использоваться верификация на основе знаний	То же, что и для IAL2
Доказательство	Доказательства идентичности не собираются	• Одно ОЧЕНЬ УБЕДИТЕЛЬНОЕ или УБЕДИТЕЛЬНОЕ доказательство, в зависимости от строгости изначальной проверки, и валидация субъектом, выдавшим доказательство, ЛИБО • два ОЧЕНЬ УБЕДИТЕЛЬНЫХ доказательства, ЛИБО • одно УБЕДИТЕЛЬНОЕ доказательство плюс 2 (два) ДОСТАТОЧНО УБЕДИТЕЛЬНЫХ доказательства	• Два ОЧЕНЬ УБЕДИТЕЛЬНЫХ доказательства, ЛИБО • одно ОЧЕНЬ УБЕДИТЕЛЬНОЕ доказательство и одно УБЕДИТЕЛЬНОЕ доказательство, в зависимости от строгости изначальной проверки, и валидация субъектом, выдавшим доказательство, ЛИБО • два УБЕДИТЕЛЬНЫХ доказательства плюс одно ДОСТАТОЧНО УБЕДИТЕЛЬНОЕ доказательство
Валидация	Валидации нет	Каждое доказательство должно быть валидировано посредством процесса такой же убедительности, что и предъявленное доказательство	То же, что и для IAL2
Верификация	Верификации нет	Верификация посредством процесса, обеспечивающего УБЕДИТЕЛЬНОЕ доказательство	Верификация посредством процесса, обеспечивающего ОЧЕНЬ УБЕДИТЕЛЬНОЕ доказательство
Подтверждение адреса	Подтверждение адреса не требуется	Требуется. Коды регистрации направляются по любому адресу учетной записи. Уведомление направляется способом, отличным от способа отправки кода регистрации	Требуется. Уведомление о проверке отправляется по почтовому адресу
Сбор биометрических данных	Нет	Необязательный	Обязательный
Меры контроля безопасности	Неприменимо	• Умеренный базовый уровень (или эквивалентный федеральному или отраслевому стандарту)	• Высокий базовый уровень (или эквивалентный федеральному или отраслевому стандарту)

Вставка 19. Очное доказывание идентичности и регистрация

Как отмечалось выше, технические стандарты разрешают очное доказывание идентичности для уровня IAL2 и *требуют* ее для IAL3. Важно отметить, что, в том числе в целях расширения доступности финансовых услуг, очное доказывание идентичности и регистрация могут осуществляться одним из следующих способов:

- физическое взаимодействие с соискателем под контролем оператора; или
- *удаленное взаимодействие* с соискателем *под контролем оператора* в соответствии со специальными требованиями к удаленному очному доказыванию идентичности, которые гарантируют уровни достоверности и безопасности, сравнимые с уровнями достоверности и безопасности очной проверки подлинности идентичности (физического взаимодействия).

Для любого типа очной проверки подлинности идентичности технические стандарты требуют, чтобы (1) в ходе проверки оператор проверял биометрический источник (например, пальцы, лицо) на наличие ненатуральных материалов; (2) CSP собирал биометрические данные таким образом, чтобы гарантировать, что они собираются у соискателя, а не у другого субъекта, и что применяются все требования к биометрическим характеристикам, изложенные в применяемых стандартах.

Требования к сопоставимости для контролируемого удаленного очного доказывания идентичности и регистрации

Чтобы установить сопоставимость между контролируемой удаленной очной проверкой подлинности идентичности и регистрацией, при которой соискатель физически находится в том же месте, что и CSP, должны выполняться следующие требования (помимо требований к валидации и верификации IAL3, которые описывались выше).

CSP должен:

– Контролировать весь сеанс проверки подлинности идентичности (например, путем непрерывной передачи видеоизображения соискателя в высоком разрешении).

– Распорядиться, чтобы реальный оператор дистанционно участвовал в сеансе проверки подлинности идентичности вместе с соискателем. Операторы должны пройти обучение по выявлению потенциального мошенничества, чтобы правильно проводить виртуальные сеансы проверки подлинности идентичности.

– Провести цифровую верификацию доказательств (например, с помощью чипов или беспроводных технологий) с помощью встроенных сканеров и датчиков,

– Обеспечить осуществление всех взаимодействий по защищенному каналу с взаимной аутентификацией.

– Использовать физические функции обнаружения и защиты от несанкционированного доступа, подходящие для среды, в которой проходит сеанс проверки подлинности идентичности (например, для киоска, расположенного в зоне ограниченного доступа или контролируемого доверенным физическим лицом, требуется меньше средств обнаружения физического несанкционированного доступа, чем для киоска, находящегося в полупубличной зоне, такой как вестибюль торгового центра).

Соискатель должен постоянно присутствовать на сеансе (и не может выходить из сеанса) контролируемой проверки подлинности идентичности, и все действия, предпринятые соискателем в ходе этого сеанса, должны быть четко видны удаленному оператору.

Вставка 20. Аутентификация и управление жизненным циклом

УРОВНИ НАДЕЖНОСТИ АУТЕНТИКАЦИИ (AAL) устанавливают технические требования к (1) протоколам и процессам аутентификации (включая выдачу и привязку учетных данных и аутентификаторов) и (2) управлению жизненным циклом аутентификатора (включая аннулирование в случае потери или кражи, и истечение срока действия / повторную проверку и повторное связывание). Усиленная (более строгая) аутентификация (более высокий уровень AAL) означает, что злоумышленники должны иметь больше возможностей и тратить больше ресурсов для успешного нарушения процесса аутентификации. Аутентификация с более высоким уровнем AAL может эффективно снизить риск использования чужих идентификационных данных, повторных и других атак, которые могут привести к мошенническим притязаниям с использованием цифровых идентификационных данных субъекта. Уровни AAL включают технические требования к разным типам аутентификаторов; утвержденным криптографическим и защищенным каналам аутентификации (включая требования к обнаружению компрометации данных, имперсонации и устойчивости к атакам повторного воспроизведения), повторной аутентификация (расширенных) сессий подписчика, хранению записей, компьютерной безопасности и конфиденциальности. AAL также устанавливают требования к привязке аутентификаторов к проверенным идентификационным данным и к действиям, которые должны быть предприняты в ответ на события, которые могут произойти в течение жизненного цикла аутентификатора подписчика, и влияют на достоверность аутентификатора после привязки, включая потерю, кражу, несанкционированное дублирование, истечение срока действия и аннулирование. Многие из этих требований носят технический характер и включают в себя ссылки на другие технические стандарты информационной безопасности.

Далее кратко и очень обобщенно описываются только некоторые требования к аутентификации на разных уровнях AAL. Более подробное описание приводится в стандарте 800-63(b) Национального института стандартов и технологий США (NIST).

- AAL1: предусматривает *некоторые надежности* того, что заявитель (физическое лицо, заявляющее свою идентичность для авторизации учетной записи) контролирует аутентификаторы, привязанные к учетной записи подписчика. AAL1 допускает широкий спектр технологий аутентификации, типов аутентификаторов и средств контроля информационной безопасности на низком базовом уровне. МФА не является обязательной. В качестве однофакторного аутентификатора уровня AAL1 можно использовать одни лишь биометрические данные.

- AAL2: предусматривает *высокую степень доверия* к тому, что заявитель контролирует аутентификатор(-ы), привязанный(-ые) к учетной записи клиента/подписчика. Для этого уровня требуется МФА (многофакторный аутентификатор или два однофакторных аутентификатора), использующая безопасный(-ые) протокол(-ы) аутентификации, который(ые) включает(ют) определенные утвержденные криптографические технологии и средства контроля информационной безопасности на умеренном базовом уровне. AAL2 налагает более строгие требования к типам аутентификаторов, чем AAL1[62]. Биометрические данные могут использоваться в качестве одного *фактора* аутентификации (что-то, что является частью вас), а аутентификация устройства будет вторым фактором (что-то, что вы имеете), но они не могут быть единственным типом аутентификатора.

[62] Уровень надежности аутентификации 2 разрешает использование любого из следующих многофакторных аутентификаторов: многофакторное устройство генерации одноразовых паролей, многофакторная криптографическая программа или многофакторное криптографическое устройство. Когда используется комбинация двух однофакторных аутентификаторов, один аутентификатор должен храниться в памяти секретным аутентификатором, а другой должен основываться на владении (т.е. «что-то, что вы имеете») и использовать любой элемент из следующих: секретный код, устройство внеполосного канала, однофакторное устройство генерации одноразовых паролей, однофакторная криптографическая программа или однофакторное криптографическое устройство.

- AAL3: предусматривает *очень высокую степень доверия* к тому, что заявитель контролирует аутентификатор(-ы), привязанный(-ые) к учетной записи подписчика. Для AAL3 требуется МФА, при которой используется аппаратный аутентификатор и аутентификатор, который обеспечивает устойчивость верификатора к имперсонации (VIR) на основе доказательства владения ключом посредством утвержденного криптографического протокола[63]. Заявители должны доказать владение и контроль над двумя различными факторами аутентификации через защищенный(ые) протокол(ы) аутентификации с использованием утвержденных криптографических технологий. Аутентификаторы должны быть устойчивы к имперсонации верификатора, устойчивы к атакам повторного воспроизведения и противостоять соответствующим атакам по побочным каналам. При использовании биометрического фактора провайдер идентификационных услуг (верификатор) должен самостоятельно определить, соответствует ли биометрический датчик и последующая обработка указанным требованиям к характеристикам. CSP должен применять соответствующим образом настроенные меры безопасности на *высоком* базовом уровне.

Регламент ЕС об электронной идентификации (eIDAS) — Европейский союз

Структура eIDAS предусматривает три уровня надежности для средств электронной идентификации, предоставляемых в рамках объявленной схемы электронной идентификации: низкий, существенный и высокий. Исполнительное решение Европейской комиссии (EU) 2015/1502 от 8 сентября 2015 года устанавливает минимальные спецификации безопасности для каждого из этих уровней. При составлении спецификаций и процедур, изложенных в этом Исполнительном решении, в качестве основного международного стандарта в области уровней надежности для средств электронной идентификации был принят Международный стандарт ИСО/МЭК 29115. Содержание Регламента eIDAS отличается от этого международного стандарта, в частности, в части требований к проверке подлинности идентичности и верификации, а также способа учета различий между механизмами идентификации, используемыми государствами-членами, и существующими в ЕС инструментами, применяемыми для этой же цели. Если в стране ЕС/ЕЭЗ государственный орган требует для доступа к одной из своих онлайн-услуг электронной идентификации с существенным или высоким уровнем надежности, то при предоставлении доступа к этой онлайн-услуге он также должен принимать все средства электронной идентификация с таким же или более высоким уровнем надежности, относящиеся к схеме идентификации, объявленной Комиссией и опубликованной в Официальном вестнике Европейского Союза. Кроме того, государственные органы могут принять решение на добровольной основе о признании схем электронной идентификации с низким уровнем надежности.

Для целей регламента eIDAS элементами системы цифровой идентификации являются следующие.

- **Регистрация** обеспечивает идентификацию, уникально представляющую либо физическое или юридическое лицо, либо физическое лицо, представляющее юридическое лицо. Регистрация предполагает разные этапы.

[63] Заявитель использует закрытый ключ, хранящийся в аутентификаторе, для подтверждения того, что он владеет аутентификатором и контролирует его. IDSP (верификатор), узнав открытый ключ заявителя через некоторые учетные данные (обычно сертификат открытого ключа), использует утвержденный протокол криптографической аутентификации для проверки того, что заявитель владеет аутентификатором закрытого ключа и контролирует его, и подтверждает Полагающейся стороне проверенные идентификационные данные этого человека.

  - Заявка и регистрация: (1) убедиться, что соискателю известны условия использования средств электронной идентификации, (2) убедиться, что соискателю известны рекомендуемые меры предосторожности, связанные со средствами электронной идентификации, (3) собрать соответствующие идентификационные данные, необходимые для проверки подлинности идентичности и верификации.

  - Проверка подлинности идентичности и верификация, заключающиеся в проверке подлинности и действительности документа, удостоверяющего личность, и относящиеся к реальному человеку, и проверка того, что идентичность этого лица является заявленной идентичностью.

- **Электронная идентификация** означает управление и имеет дело с количеством и характером факторов аутентификации, независимо от того, может ли средство электронной идентификации считаться используемым только в том случае, если оно находится под контролем или во владении лица, которому оно принадлежит, и его аннулирование и возобновление.

- **Аутентификация** устанавливает требования к уровню надежности в отношении механизма аутентификации, посредством которого физическое или юридическое лицо использует средства электронной идентификации для подтверждения полагающейся стороне своей идентичности.

- **Руководство и организация:** все участники, предоставляющие услуги, связанные с электронной идентификацией в международном контексте, должны иметь в своем распоряжении документированные методики управления информационной безопасностью, политики, подходы к управлению рисками и другие признанные меры контроля, позволяющие убедить компетентные руководящие органы, отвечающие за электронные схемы идентификации в соответствующих государствах-членах, в наличии эффективных методик.

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

- **низкий** — обеспечивает низкую степень доверия к заявленной идентичности физического лица и характеризуется со ссылкой на соответствующие технические спецификации, стандарты и процедуры, включая технические средства контроля, цель которых состоит в снижении риска злонамеренного использования или изменения идентичности;

- **существенный** — обеспечивает существенную степень доверия к заявленной идентичности физического лица и характеризуется со ссылкой на соответствующие технические спецификации, стандарты и процедуры, включая технические средства контроля, цель которых состоит в существенном снижении риска злонамеренного использования или изменения идентичности;

- **высокий** — обеспечивает более высокую степень доверия к заявленной идентичности физического лица, чем средства электронной идентификации с существенным уровнем доверия, и характеризуется со ссылкой на соответствующие технические спецификации, стандарты и процедуры, включая технические средства контроля, цель которых состоит в предотвращении злонамеренного использования или изменения идентичности.

Предполагается, что если средство электронной идентификации, выданное в рамках объявленной схемы электронной идентификации, соответствует требованию, указанному в описании более высокого уровня доверия, то выполняется и эквивалентное требование более низкого уровня доверия.

Таблица 5. Требования к аутентификации для разных уровней надежности eIDAS

УРОВЕНЬ НАДЕЖНОСТИ	НЕОБХОДИМЫЕ ЭЛЕМЕНТЫ
НИЗКИЙ	• Выдаче идентификационных данных человеку предшествует надежная проверка средств электронной идентификации и их действительность. • В тех случаях, когда идентификационные данные человека хранятся как часть механизма аутентификации, эта информация защищена от потери и компрометации, в том числе с использованием анализа в автономном режиме. • В механизме аутентификации реализованы меры безопасности для проверки средств электронной идентификации, поэтому крайне маловероятно, что такие действия, как угадывание, прослушивание, повторное воспроизведение или манипулирование связью со стороны злоумышленника, обладающего расширенными базовыми возможностями для атаки, могут нарушить механизмы аутентификации.
СУЩЕСТВЕННЫЙ	Низкий уровень плюс: • Выдаче идентификационных данных человеку предшествует надежная проверка средств электронной идентификации и их действительность посредством динамической аутентификации. • В механизме аутентификации реализованы меры безопасности для проверки средств электронной идентификации, поэтому крайне маловероятно, что такие действия, как угадывание, прослушивание, повторное воспроизведение или манипулирование связью со стороны злоумышленника, обладающего **умеренными возможностями для атаки,** могут нарушить механизмы аутентификации.
ВЫСОКИЙ	Существенный уровень плюс: • В механизме аутентификации реализованы меры безопасности для проверки средств электронной идентификации, поэтому крайне маловероятно, что такие действия, как угадывание, прослушивание, повторное воспроизведение или манипулирование связью со стороны злоумышленника, обладающего **большими возможностями для атаки,** могут нарушить механизмы аутентификации.

ГЛОССАРИЙ

Приложение — компьютерная программа, помогающая пользователю в выполнении определенных задач.

Интерфейс прикладного программирования (API) — набор определений и протоколов для разработки и интеграции прикладного программного обеспечения. API позволяют цифровым продуктам или услугам легко взаимодействовать с другими продуктами и услугами.

Уровни надежности — уровни достоверности или уверенности в надежности каждого из трех этапов процесса цифровой идентификации. См. обзор технических стандартов в разделе II данного отчета и в теме «Использование технических стандартов цифровой идентификации для внедрения РОП» в разделе V отчета.

Подтверждение атрибута может быть либо физическим (документарным), либо чисто цифровым, либо являться цифровым представлением физического подтверждения атрибута (например, цифровым представлением бумажных или пластиковых водительских прав).

Аутентификация устанавливает, что заявитель, который декларирует свою идентичность, является тем же лицом, идентичность которого была получена, верифицирована и зарегистрирована при принятии его на обслуживание.

Аутентификатор — это то, что находится во владении и под контролем заявителя и используется для аутентификации (подтверждения) того, что заявитель является физическим лицом, которому были выданы учетные данные, и, следовательно (в зависимости от строгости аутентификации системы цифровой идентификации), является (с разной степенью вероятности, определяемой уровнем надежности аутентификации) фактическим подписчиком и владельцем учетной записи.

Биометрия

- Биофизическая биометрия — атрибуты, такие как отпечатки пальцев, радужная оболочка глаз, спектрограммы голоса и распознавание лиц; все они не меняются.

- Биомеханическая биометрия — атрибуты, такие как механика нажатия клавиш, которые являются результатом уникальных взаимодействий мышц, скелетной и нервной систем человека.

- Поведенческие биометрические схемы — атрибуты, основанные на новой вычислительной общественной науке — социальной физике, которые состоят из различных схем движения человека и использования им геопространственных временных данных и включают, например, схемы электронных писем или текстовых сообщений человека, журнал регистрации доступа к файлам, использование мобильного телефона и геолокационные схемы.

Сбор и отождествление являются частью процесса проверки подлинности идентичности и предполагают получение атрибутов (идентификаторов), сбор подтверждений атрибутов и отождествление доказательства и атрибутов идентичности с единственной уникальной личностью в рамках данной группы населения или контекста.

Непрерывная аутентификация — это динамическая форма аутентификации. В ней может использоваться биомеханические биометрические данные, поведенческие биометрические схемы и/или динамический анализ риска операций, что обеспечивает соответствие определенных данных, собранных в ходе интерактивного взаимодействия с физическим лицом (например, данных геолокации, MAC-адресов и IP-адресов, скорости набора текста и угла наклона мобильного устройства) «тому, что следует ожидать» в течение всего сеанса.

Заявитель — это лицо, которое хочет установить свою личность и получить права, связанные с этой личностью (например, открыть финансовый счет или получить к нему доступ). Заявителя также можно описать как Подписчика, который заявляет Полагающейся стороне (ПС) права собственности на удостоверение и хочет его проверить, используя протоколы аутентификации.

Учетные данные — это физический объект или цифровая структура, которая достоверно привязывает установленную личность подписчика, посредством идентификатора(ов), по крайней мере к одному аутентификатору, который находится во владении и под контролем подписчика.

Провайдер учетных данных (CSP) — учреждение, которое выдает подписчикам и/или регистрирует аутентификаторы и соответствующие электронные учетные данные (привязывая аутентификаторы к проверенным удостоверениям) подписчиков. CSP отвечает за хранение идентификационных учетных данных подписчика и всех связанных учетных данных в течение всего жизненного цикла учетных данных, а также за предоставление верификаторам информации о статусе учетных данных.

Атака с подстановкой учетных данных (credential stuffing) (также называемая повторным воспроизведением утечки (breach replay) или очисткой списка (list cleaning)) — тип кибератаки, при которой украденные учетные данные (часто из-за утечки данных) проверяются на совпадения в других системах. Этот тип атаки на учетную запись может быть успешным, если жертва использовала этот же пароль (который был украден при утечке данных) для другой учетной записи.

Исключение дубликатов (de-duplication) — процесс отождествления доказательств и атрибутов идентичности с единственной уникальной личностью в рамках данной группы населения или контекста.

Для целей настоящего Руководства **системы цифровой идентификации** — системы, которые включают процесс проверки подлинности идентичности/регистрации и аутентификации. Проверка подлинности идентичности и регистрация могут быть или цифровыми, или физическими (документарными), или их комбинацией, но привязка, выпуск учетных данных, аутентификация и переносимость / федеративная интеграция должны быть цифровыми.

Механизмы и технические стандарты надежности цифровой идентификации представляют собой набор открытых согласованных механизмов обеспечения качества и технических стандартов систем цифровой идентификации, разработанных в нескольких юрисдикциях, а также международными и отраслевыми организациями. См. **Приложение D «Организации, устанавливающие технические стандарты и механизмы надежности цифровой идентификации».** Например, см. Стандарты Национального института стандартов и технологий США и Регламент ЕС об электронной идентификации в Приложении E «Обзор механизмов и технических стандартов надежности цифровой идентификации США и ЕС».

Регламент ЕС об электронной идентификации (eDISA) — Регламент (ЕС) NN№910/2014 об электронной идентификации и удостоверительных сервисах для электронных транзакций на внутреннем рынке.

Регистрация — это процесс, посредством которого IDSP регистрирует (записывает) соискателя, подлинность идентичности которого была проверена, в качестве «подписчика» и создает его учетную идентификационную запись. В рамках этого процесса уникальные идентификационные данные подписчика (то есть атрибуты/идентификаторы подписчика) достоверно **привязываются** к одному или нескольким аутентификаторам, которые находятся во владении и под контролем подписчика, с использованием соответствующего протокола связываний. Процесс привязки идентичности подписчика к аутентификатору(-ам) также называется **«выпуском учетных данных».**

Интеграция означает использование обобщенной цифровой архитектуры и протоколов подтверждения для передачи удостоверения и аутентификационной информации по сетевым системам.

Системы идентификации общего назначения (или базовые системы идентификации) обычно содержат документарные и/или цифровые удостоверения, которые повсеместно признаются и принимаются государственными учреждениями и провайдерами услуг частного сектора в качестве проверки подлинности официальной идентичности для различных целей (например, национальные системы идентификации и органы регистрации актов гражданского состояния).

Доказательство идентичности — см. «подтверждение атрибута».

Управление жизненным циклом идентификационных данных относится к действиям, которые следует предпринять в ответ на события, которые могут произойти в течение жизненного цикла идентификационных данных и повлиять на использование, безопасность и надежность аутентификаторов, например, потеря, кража, несанкционированное дублирование, истечение срока действия и аннулирование аутентификаторов и/или учетных данных.

Проверка подлинности идентичности дает ответ на вопрос: «Кто вы?» и относится к процессу, посредством которого провайдер идентификационных услуг (IDSP) собирает, валидирует и проверяет информацию о человеке и отождествляет ее с уникальным физическим лицом в рамках данной группы населения или контекста. Он включает три действия: (1) сбор/отождествление, (2) валидацию и (3) верификацию.

Провайдер идентификационных услуг (IDSP) — обобщающий собирательный термин, который относится ко всем типам учреждений, участвующих в обеспечении процессе эксплуатации и элементов систем или решений цифровой идентификации. IDSP предоставляют решения цифровой идентификации пользователям и полагающимся сторонам. Одно учреждение может выполнять функциональные роли одного или нескольких IDSP — см. **Приложение А «Описание основной системы цифровой идентификации и ее участников»**, чтобы получить сводную информацию обо всех соответствующих учреждениях, включая поставщика идентификационных данных (IDP), провайдера учетных данных (CSP), орган регистрации (или менеджера идентификации), верификатора, пользователя/физическое лицо, соискателя, подписчика, заявителя, полагающуюся сторону и Провайдера структуры доверия/Доверенный орган.

Имперсонация обозначает ситуацию, когда какое-либо лицо выдает себя за обладателя идентификационных данных другого человека, либо с использованием украденного документа кого-то с похожей внешностью, либо в сочетании с использованием фальшивого или поддельного удостоверения личности (например, замена фотографии в паспорте на изображение самозванца).

Системы идентификации ограниченного назначения (или функциональные системы идентификации) обеспечивают идентификацию, аутентификацию и авторизацию для конкретных услуг или секторов, таких как налоговая администрация, доступ к определенным государственным пособиям и услугам, голосование, права на управление транспортным средством, а также (в некоторых юрисдикциях) доступ к финансовым услугам и т.д. Примеры функциональных систем идентификации включают (без ограничения): идентификационные номера налогоплательщиков, водительские права, паспорта, регистрационные карточки избирателей, номера социального страхования и документы, удостоверяющие личность беженцев.

Атака через посредника имеет ту же цель, что и фишинг и может быть инструментом фишинга, но данные похищаются путем перехвата сообщений между жертвой и провайдером услуг.

Многофакторная аутентификация (MFA) сочетает использование двух или нескольких факторов аутентификации для повышения безопасности.

Стандарты/Руководство Национального института стандартов и технологий США — Руководство №800-63 по цифровым идентификационным данным Национального института стандартов и технологий США.

Для целей настоящего Руководства **официальной идентичностью** является описание уникального физического лица, которое (1) основано на характеристиках (идентификаторах или атрибутах) этого лица, определяющих уникальные черты человека в рамках группы населения или определенной(ых) контекста(ов), и (2) признается государством в регулятивных и других официальных целях.

Информация, позволяющая установить личность, включает любую информацию, которая сама по себе или в сочетании с другой информацией позволяет идентифицировать конкретного человека.

Фишинг (также называемый перехватом через посредника или перехватом учетных данных) — это мошенническая попытка сбора учетных данных не подозревающих об этом жертв с использованием обманных электронных писем и Интернет-сайтов. Например, преступник пытается обмануть свою жертву, указав имена, пароли, правительственные идентификационные номера или учетные данные для, казалось бы, заслуживающего доверия источника.

Перехват и воспроизведение PIN-кода включает перехват PIN-кода, введенного на клавиатуре ПК, с помощью перехватчика данных ввода и незаметно для пользователя, а также использование перехваченного PIN-кода, когда смарт-карта вставляется в считывающее устройство для доступа к услугам.

Переносимость/совместимость: переносимость удостоверения означает, что цифровые идентификационные учетные данные физического лица могут использоваться для проверки подлинности официальной идентичности при установлении новых клиентских отношений в несвязанных учреждениях частного сектора или государственных учреждениях без необходимости каждый раз получать и проверять информацию, позволяющую установить личность и осуществлять идентификацию/проверку клиента. Переносимость требует разработки совместимых продуктов, систем и процессов цифровой идентификации. Переносимость/совместимость может обеспечиваться различными архитектурами и протоколами цифровой идентификации.

Прогрессивное удостоверение — официальное удостоверение, которое может меняться со временем по мере того, как идентифицируемое физическое лицо приобретает все более надежный цифровой след, с возрастающим количеством атрибутов и/или аутентификаторов, которые можно проверять по возрастающему количеству и расширяющемуся спектру источников.

Проверка подлинности официальной идентичности, как правило, зависит от формы обеспечиваемой или предоставляемой правительством регистрации, документации или сертификации (например, свидетельство о рождении, удостоверение личности или учетные данные цифрового удостоверения личности), которые подтверждают основные идентификаторы или атрибуты (например, имя, пол, дату и место рождения) для установления и проверки официальной идентичности. Критерии проверки подлинности «официальной идентичности» могут различаться в разных юрисдикциях.

Шифрование с открытым ключом (используется в сертификатах инфраструктуры открытых ключей (PKI)) — шифрование, при котором для объекта (человека, системы или устройства) генерируется пара ключей, и этот объект надежно хранит секретный ключ, при этом свободно предоставляя открытый ключ другим лицам. Любой человек, имеющий открытый ключ, может затем использовать его для шифрования и отправки сообщения владельцу секретного ключа, зная, что только он сможет открыть это сообщение.

Для целей настоящего Руководства под **регулируемыми субъектами** понимаются финансовые учреждения, провайдеры сервисов виртуальных активов и установленные нефинансовые предприятия и профессии (УНФПП), в той мере, в которой УНФПП обязаны предпринимать меры по надлежащей проверке клиентов (НПК) в обстоятельствах, указанных в Рекомендации 22. В июне 2019 года ФАТФ пересмотрела Рекомендацию 15 (Новые технологии) и Пояснительную записку к Рекомендации (ПЗР) 15, чтобы, помимо прочего, наложить на провайдеров сервисов виртуальных активов обязательства по НПК, предусмотренные Рекомендацией 10.

Полагающаяся сторона (ПС) — (физическое или юридическое) лицо, которое полагается на учетные данные или аутентификаторы подписчика либо подтверждение верификатором удостоверения заявителя в целях идентификации Подписчика с использованием протокола аутентификации. Типичные ПС включают финансовые учреждения, правительственные департаменты и организации.

Подписчик — лицо, удостоверение которого было проверено и привязано к аутентификаторам, удостоверенным провайдером учетных данных (CSP) и которое может использовать эти аутентификаторы для идентификации. Подписчики получают аутентификатор(ы) и соответствующие учетные данные от CSP и могут использовать эти идентификатор(ы) для идентификации.

Синтетические идентификационные данные создаются преступниками путем объединения реальной (обычно украденной) и поддельной информации для создания новой (синтетической) идентификационной информации, которую можно использовать для открытия мошеннических счетов и совершения мошеннических покупок. В отличие от имперсонации, преступник притворяется тем, кого не существует в реальном мире, а не маскируется под обладателя существующих идентификационных данных.

Многоуровневая НПК (иногда называемая многоуровневой учетной записью или прогрессивной НПК) — доступ к ряду различных функций учетной записи в зависимости от степени идентификации/проверки, проводимой регулируемым субъектом. Доступ к базовому набору услуг 1-го уровня предоставляется при минимальной идентификации. Доступ к последующим уровням учетной записи и дополнительным услугам (например, более высоким лимитам операций или остаткам на счетах, диверсифицированным каналам доступа и доставки) разрешается только в том случае, если/когда клиент предоставляет необходимую дополнительную информацию для идентификации/проверки. В то же время для счетов предусмотрены ограничения услуг (например, верхние пределы сумм ежедневных/ежемесячных изъятий средств, лимиты на депозиты в зависимости от уровня проведенной НПК и профиля риска клиента). См. ФАТФ (2013-2017 гг.), «Меры противодействия отмыванию денег и финансированию терроризма и расширение доступности финансовых услуг» с дополнением о надлежащей проверке клиентов.

Доверенные поручители (также называемые «представителями») — назначенные физические лица или организации (например, нотариусы, законные опекуны, медицинские работники, опекуны, обладатели доверенностей или другие обученные и одобренные или сертифицированные лица), которые могут поручиться за заявителя для доказательства его идентичности в соответствии с применимыми законами, нормативными положениями или агентскими политиками данной юрисдикции. Этот термин используется в Стандартах Национального института стандартов и технологий США, см. NIST №800-63A 4.4.2. «Требования к проверке доверенных поручителей, уровень надежности определения идентичности 2».

Валидация является частью процесса проверки подлинности идентичности и предполагает определение того, что доказательства являются подлинными (не поддельными или незаконно присвоенными), и что информация, содержащаяся в доказательствах, является точной. Для этого информация об идентичности / доказательства идентичности проверяются по приемлемым (достоверным/надежным) источникам, что позволяет установить, что информация соответствует данным/записям из надежных независимых источников.

Верификация является частью процесса доказательства идентичности и предполагает подтверждение того, что валидированная идентичность относится к физическому лицу (соискателю), подлинность идентичности которого была проверена.

Верификатор — учреждение, которое проверяет идентичность Заявителя для Полагающейся стороны (ПС), подтверждая, с использованием протокола аутентификации, что один или несколько аутентификаторов находятся во владении и под контролем Заявителя.