FATF

ПАРТНЕРСТВО В БОРЬБЕ С ФИНАНСОВЫМИ ПРЕСТУПЛЕНИЯМИ

ЗАЩИТА ДАННЫХ, ТЕХНОЛОГИИ И ОБМЕН ИНФОРМАЦИЕЙ МЕЖДУ СУБЪЕКТАМИ ЧАСТНОГО БИЗНЕСА

Июль 2022 г.

ФАТФ является независимой международной организацией, которая разрабатывает и распространяет регламентирующие документы, касающиеся защиты мировой финансовой системы от отмывания денег, финансирования терроризма и финансирования распространения оружия массового уничтожения. Рекомендации ФАТФ являются всемирным стандартом в области ПОД/ФТ.

Дополнительную информацию о ФАТФ можно найти на **www.fatf-gafi.org**

Этот документ и (или) любая карта, являющаяся его частью, не ограничивают статус или суверенитет какой-либо территории, не влияют на действительность международных границ или разграничительных линий и на название какой-либо территории, города или области.

Неофициальный перевод выполнен МУМЦФМ

Ссылка для цитирования:

ФАТФ (2022 г.) Партнерство в борьбе с финансовыми преступлениями: Защита данных, технологии и обмен информацией между субъектами частного бизнеса, ФАТФ, Париж, Франция, https://www.fatf-gafi.org/publications/digitaltransformation/documents/partnering-in-the-fight-against-financial-crime.html

Содержание

[1] В Разделе 6 Аналитического отчёта по итогам 1 этапа проекта, касающегося критической оценки объединения данных, совместного анализа и защиты данных (Stocktake Report), содержится общий обзор трудностей и проблем, связанных с использованием новых технологий в целях совместного анализа данных.

Список сокращений

ДКУС	Денежно-кредитное управление Сингапура
ЗДЛЖ	Защита данных и неприкосновенности личной жизни
ЗСК	Знай своего клиента
МПГПП	Международный пакт ООН о гражданских и политических правах
НКО	Некоммерческая организация
НПК	Надлежащая проверка клиента
ОВПЧ	Оценка влияния на права человека
ОД	Отмывание денег
ООН	Организация объединенных наций
ОРЗД	Особый регламент ЕС по защите данных оружия массового уничтожения
ОЭСР	Организация экономического сотрудничества и развития
ПОД	Противодействие отмыванию денег
ПФР	Подразделение финансовой разведки
ПФРОМУ	Противодействие финансированию распространения
ПФТ	Противодействие финансированию терроризма
СЕ	Совет Европы
СНО	Сообщение о необычной операции
СПД	Сообщение о подозрительной деятельности
СПО	Сообщение о подозрительной операции
СУИ	Система уведомлений об инцидентах
ТУК	Технология, усиливающая конфиденциальность
УЗД	Управление по защите данных
УКИ	Управление уполномоченного по информации
ФАТФ	Группа разработки финансовых мер борьбы с отмыванием денег
ФинСЕН	Сеть по борьбе с финансовыми преступлениями (ПФР США)
ФРОМУ	Финансирование распространения оружия массового уничтожения
ФТ	Финансирование терроризма
ФУ	Финансовое учреждение

Основные положения

Противодействие отмыванию денег (ОД), финансированию терроризма (ФТ) и финансированию распространения оружия массового уничтожения (ФРОМУ), а также защита данных и неприкосновенности личной жизни (ЗДЛЖ) отвечают интересам общества. Целью указанных видов деятельности является решение важных задач, в т.ч. защита прав и основных свобод человека[1] (в т.ч. права на защиту неприкосновенности частной жизни) и защиту общества от преступной деятельности, в т.ч. терроризма. Эти цели не противоречат друг другу и не исключают друг друга. Эффективный режим ПОД/ФТ/ФРОМУ требует от общества и представителей частного сектора достигать как целей ПОД/ФТ/ФРОМУ,[2] так и целей ЗДЛЖ.

Задачей этого отчета является оказание помощи юрисдикциям, которые планируют повысить эффективность обмена информацией между представителями частного сектора, в ответственной разработке и применении таких программ в соответствии с правилами защиты данных и неприкосновенности частной жизни таким образом, чтобы риски, связанные с интенсификацией обмена личными данными, принимались во внимание надлежащим образом. Для достижения необходимого баланса при осуществлении этой работы ФАТФ провело консультации с представителями органов, обеспечивающих защиту данных, учеными, поставщиками технологий и представителями частного сектора.

Задачей систем по ПОД/ФТ/ФРОМУ является лишение членов ОПГ и террористических организаций, коррумпированных чиновников, тех, кто распространяет оружие массового уничтожения, осуществляет незаконный оборот наркотиков или торговлю людьми, доступа к финансовой системе. Несмотря на соответствующие усилия, деятельность преступных группировок становится все более изощренной, они используют недостатки данной системы. Одно финансовое учреждение обладает лишь частичным пониманием финансовой операции и видит одну небольшую часть того, что зачастую является большим и сложным явлением. Для структурирования незаконных финансовых средств злоумышленники используют недостаток информации, прибегая к услугам различных ФУ, находящихся в одной или нескольких странах. Без более точной и согласованной информации отдельным ФУ становится все труднее выявлять такую деятельность. Осуществляя совместный анализ, объединяя данные или реализуя другие программы по обмену информацией ответственным образом, ФУ могут получить более четкую картину существующего явления, которая позволит им глубже понимать, а также более эффективно оценивать и уменьшать риски ОД/ФТ.

Важно отметить, что сбор и использование личных данных для этих целей могут привести к возникновению проблем в области защиты данных и неприкосновенности личной жизни. Неправильное использование данных, неоправданный обмен ими или отсутствие защитных мер способны оказывать негативное влияние на тех людей, которые не имеют отношения к преступной деятельности. Управление и разработка соответствующих данных и систем должны осуществляться в соответствии с применимыми правилами в области ЗДЛЖ. При наличии соответствующих требований правовых систем такие действия должны быть необходимыми, разумно оправданными и соразмерными по отношению к целям обработки данных (т.е. ПОД/ФТ/ФРОМУ). Действия должны планироваться и осуществляться ответственно и эффективно, чтобы риски, связанные с интенсификацией обмена личными данными, были соответствующим образом учтены. В целом польза, которую получает общество от борьбы с финансовыми преступлениями, должна перевешивать такие риски.

В этом отчете члены ФАТФ и ее Глобальной сети обмениваются опытом увеличивающегося обмена информацией между представителями частного сектора, осуществляемого в правовых рамках систем по ЗДЛЖ своих стран. Каждая из этих инициа-

тив по обмену информацией должна рассматриваться индивидуально на основании ее особенных характеристик и соответствующих требований в области ЗДЛЖ.

Такой опыт свидетельствует о том, что меры по обмену информацией о ПОД/ФТ/ФРОМУ между субъектами частного сектора могут приниматься в соответствии с правилами и обязательствами по ЗДЛЖ при условии прохождения основных проверок и соблюдении основных требований. Хотя использование современных технологий может помочь соблюсти баланс между достижением целей политики и уменьшением рисков нарушения неприкосновенности частной жизни, ключом к успешной реализации этих инициатив является соответствующее управление и наличие правового регулирования. По мере реализации инициатив в области обмена информацией между субъектами частного сектора, его развития и совершенствования, будет поступать большее количество данных, которые позволят оценить, повышает ли такой обмен эффективность ПОД/ФТ/ФРОМУ, когда и как это происходит.

ФАТФ надеется, что эта работа поможет странам, которые анализируют возможность совершенствования механизмов обмена информации между субъектами частного сектора, понять, как другие страны выполняли обязательства в области ЗДЛЖ при разработке инициатив по обмену информацией.

Этот отчет не носит обязывающего характера. Содержащиеся в нем рекомендации, предназначенные для стран, которые задумываются над интенсификацией обмена информацией между субъектами частного сектора, отражают наблюдения и уроки, извлеченные юрисдикциями, входящими в Глобальную сеть ФАТФ.

- Государственным учреждениям следует рассмотреть возможность активного участия в инициативах по обмену информацией между субъектами частного сектора, например, путем внесения необходимых изменений в законы или документы, регулирующие надзор, использования регулятивных песочниц и реализации пилотных программ, определения областей, типологий или типов данных, которые выиграют от такого обмена, назначения учреждения или контактного лица, которые будут содействовать сотрудничеству и координации действий, составления руководства или списков контрольных вопросов, создания безопасных платформ для обмена информацией и контроля, разработки проектов по унификации и стандартизации данных.
- Государственные учреждения должны обеспечивать и способствовать регулярному диалогу между органами власти, отвечающими за ЗДЛЖ, и органами власти, отвечающими за ПОД/ФТ, в соответствии с Рекомендацией 2 как внутри своей страны, так и на международном уровне, например, путем проведения регулярных встреч, разработки совместной стратегии, подготовки совместного руководства или взаимодействия, охватывающего весь сектор, оказания содействия реализации инициатив, реализуемых в секторе, и реализации совместных инициатив, например, регулятивных песочниц или технологических спринтов.
- Частному сектору следует рассмотреть возможность применения технологий, повышающих конфиденциальность, в случае уместности их использования; принимать меры по подготовке данных; предусматривать меры по защите данных; осуществлять своевременное непрерывное взаимодействие с органами власти, отвечающими за ЗДЛЖ, разрабатывать индикаторы и количественные показатели для определения успеха деятельности и применять меры по исключению де-рискинга, касающегося обмена информацией.

[1] Право на неприкосновенность частной жизни предусмотрено в международных документах, касающихся прав человека, вместе с тем формулировки этого понятия в некоторых документах несколько разнятся, в т.ч. во Всемирной декларации прав человека от 1948 г., Конвенции Совета Европы о защите прав человека и основных свобод от 1950 г. и Международном пакте ООН о гражданских и политических правах от 1966 г. (права на свободу от необоснованного незаконного нарушения неприкосновенности частной жизни). Режимы ПОД/ФТ/ФРОМУ способствуют недопущению преступной деятельности, которая нарушает основные права человека (например, помогает выявлять и предотвращать торговлю людьми, коррупцию и терроризм). Кроме этого, ПОД/ФТ/ФРОМУ способствует достижению целей устойчивого развития (например, пункт 16.4. Целей устойчивого развития ООН).

[2] Организации, осуществляющие защиту данных: Европейский совет по защите данных (Подгруппа экспертов по финансовым вопросам (в т.ч. с помощью членов подгруппы)), Совет Европы (в т.ч. Комитет 108 и Подразделение по защите данных), Глобальная ассамблея по обеспечению конфиденциальности (Рабочая группа по обмену информацией), Рабочая группа ОЭСР по управлению данными и обеспечению неприкосновенности частной жизни и ее Секретариат. Органы власти отдельных стран, отвечающие за защиту данных: Департамент инноваций, науки и экономического развития Канады, Управление уполномоченного по информации, находящееся на Джерси, Комиссия по защите данных Люксембурга, Национальный институт по обеспечению прозрачности, доступа к информации и защите личных данных Мексики, Управление по защите данных Норвегии, Управление уполномоченного по информации Великобритании. Финансовые учреждения и ассоциации: Коммерцбанк, Ллойдс, Сантандер, Европейская банковская федерация, Институт международного финансирования, Вольфсбергская группа и финансовые учреждения, входящие в состав специальных рабочих групп Великобритании, Сингапура и Эстонии. Поставщики технологий и решений: Ant Group; Deloitte; FutureFlow; Duality; Elucidate; HAWK AI; Salv и Transactie Monitoring Nederland. Ученые, сотрудники аналитических центров или другие эксперты: программа «Будущее обмена данными финансовой разведки», Бенджамин Фогель – Институт Макса Планка, Елени Коста – Университет Тилбурга, Бен Хейс – консультант Совета Европы и Вивьен Артц – Проджект Роуз. Были получены различные виды комментариев и замечаний, в т.ч. письменные замечания, касающиеся проектов этого документа, приглашение ФАТФ выступить перед членами соответствующих рабочих групп, участие в обсуждениях, проводившихся в рамках работы специальной рабочей группы, осуществлявшей этот проект.

РАЗДЕЛ I.
Введение

1. В июле 2021 г. ФАТФ опубликовала «Аналитический отчёт по итогам 1 этапа проекта, касающегося критической оценки объединения данных, совместного анализа и защиты данных» (в дальнейшем именуемого «Отчет»). В Отчете говорится, что технологии, в том числе повышающие конфиденциальность, могут способствовать обмену информацией, одновременно с этим защищая частную жизнь и личные данные. Хотя в настоящее время мы не наблюдаем масштабного использования таких технологий и хотя их применение должно анализироваться в каждом конкретном случае, их применение, о котором говорится в Отчете, указывает на их возможности по обеспечению перспективных методов сотрудничества представителей частного сектора одновременно с отсутствием нарушения требований международных и национальных систем законодательств в области ЗДЛЖ. На основании результатов проведенного критического анализа в Отчете подчеркивалась необходимость большей ясности нормативных документов, стандартизации данных и управления ими, создания благоприятной среды, предотвращения сбоев при использовании искусственного интеллекта, в целях повышения эффективности обмена информации по ПОД/ФТ/ФРОМУ при соблюдении требований ЗДЛЖ как на международном, так и национальном уровнях. Данный отчет основывается на этих результатах, в нем рассказывается о том, каким образом некоторым странам, входящим в Глобальную сеть, удалось решить эти проблемы путем разработки и реализации инициатив по обмену информацией.

2. Компетентным органам (таким, как надзорные, регулирующие и правоохранительные органы) и финансовым учреждениям необходим доступ к определенной информации о клиентах и осуществляемых ими финансовых операциях для защиты людей от мошенничеств и незаконной финансовой деятельности, защиты общественности и мировых финансовых рынков и для достижения целей ПОД/ФТ/ФРОМУ, в т.ч. с помощью выявления, расследования, судебного преследования или наложения иных санкций на физических и юридических лиц за ОД/ФТ. Информация, полученная ФАТФ от субъектов частного сектора во время взаимных оценок, позволяет предположить, что пользователи финансовых услуг обычно знают о том, что коммерческие учреждения имеют доступ к личным данным, пользуются ими согласно соответствующим обязательствам внутренних и международных документов (например, обязательствам по установлению и проверке личностей клиентов) для снижения рисков совершения финансовых преступлений[3]. Кроме этого, общество также убеждено в том, что государство использует такую информацию законным образом для отстаивания его интересов, в т.ч. защиты его от мошенничества, коррупции, незаконного оборота наркотиков, торговли людьми или терроризма, в ходе сбора информации о финансовых следах такой деятельности.

[3] Это касается широких тенденций, касающихся ожиданий общества, и не отменяет законного права граждан многих юрисдикций получать информацию о любом таком использовании их персональных данных. Например, так обстоит дело в ЕС.

3. Людям предоставляются права по защите данных и (или) обеспечению неприкосновенности частной жизни на основании целого ряда международных конвенций и договоров, международных соглашений, законов и подзаконных актов. Такие права лежат в основе демократии и верховенства закона. В самом деле, наличие прав, касающихся защиты данных и неприкосновенности частной жизни, чрезвычайно важны для эффективного осуществления других прав и основных свобод человека (например, свобода самовыражения, религии, создания профсоюзов и собраний).

4. Как показано в примерах, приведенных в этом отчете, ФУ некоторых стран изучают возможность обмена информацией для целей ПОД/ФТ/ФРОМУ. Одному учреждению, вероятно, бывает трудно выявить сложную схему осуществления подозрительных операций, но информация от других учреждений может помочь ему получить полную картину. И наоборот, дополнительная информация может помочь учреждению понять, что предположительно подозрительная операция на самом деле такой не является. Чрезвычайно важно, чтобы любой такой обмен персональными данными (такими, как данные о клиентах или операции, по которым можно установить личность) между субъектами частного сектора ограничивался информацией, которая является необходимой, разумно обоснованной и достаточной; он должен осуществляться на основании применимой правовой базы. При обмене личными данными должны учитываться факторы и цели ЗДЛЖ. Инициативы по обмену данными должны осуществляться с учетом особенностей каждой ситуации на основании регламентирующих документов, подзаконных актов, процедур или других договоренностей, целью которых является защита законных интересов общества, заключающихся в его защите от преступной деятельности, в т.ч. терроризма. Задачей такого подхода, зачастую с опорой на современную технологию, является обеспечение равновесия между необходимостью борьбы с преступной деятельностью с одной стороны и достижением целей соответствующих национальных и международных законов и правовых баз в области ЗДЛЖ с другой.

5. При обеспечении оптимального достижения целей ПОД/ФТ/ФРОМУ с одновременной защитой персональных данных и неприкосновенности частной жизни могут возникать серьезные проблемы. Требования по защите данных и неприкосновенности частной жизни, включающие исключения и изъятия, могут быть разными в разных юрисдикциях. В 2021 г. те или иные законы, обеспечивающие защиту данных и неприкосновенность частной жизни, имелись в 145 юрисдикциях[4]. В этом отчете путем анализа конкретных примеров, приведенных различными юрисдикциями с разным законодательством в области ПОД/ФТ/ФРОМУ и ЗДЛЖ, изучается, как можно достичь обеих целей. На основании результатов, содержащихся в Аналитическом отчёте по итогам 1 этапа, и предметных обсуждений по второму этапу, в этом отчете описываются некоторые распространенные меры реагирования и решения, используемые частным сектором, а иногда и государственными учреждениями, для эффективного обмена информацией, сопровождаемого стремлением достигать целей и обязательств как по ПОД/ФТ/ФРОМУ, так и по ЗДЛЖ. Этот отчет может использоваться в качестве справочного руководства; он содержит накопленный опыт, который может использоваться заинтересованными лицами как из государственных, так и коммерческих учреждений, которые хотят реализовать и развивать инициативы по объединению данных и обмену информации для повышения эффективности ПОД/ФТ/ФРОМУ[5].

[4] Дж. Гринлиф (2021 г.) Ситуация с «Законодательствами по защите данных различных стран в 2021 г.: Несмотря на задержки, связанные с COVID-19, 145 стран приняли Общий регламент по защите данных», с доступно на: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3836348

[5] В Стандартах ФАТФ предусмотрены конкретные требования к обмену информацией между представителями частного бизнеса в определенных ситуациях. Подробнее об этом говорится в Разделе 2.

6. В примерах обмена информацией, приводимых в этом отчете, речь идет о достижении конкретных целей и задач, и именно, выявлении подозрительной деятельности. В некоторых случаях определенные личные данные клиентов и связанные с ними операции анализировались соответствующими ФУ на наличие возможной преступной деятельности и, после выявления подозрительной деятельности, ФУ действовало в соответствии со своими регламентирующими документами и процедурами. К таким действиям относятся принятие последующих мер и изучение ситуации, дополнительные вопросы к клиенту и (или) направление СПО. Хотя реализация ряда этих проектов находится на ранней стадии, они осуществляются в соответствии с применимыми требованиями по ЗДЛЖ, одновременно с этим позволяя добиваться более эффективных результатов в области ПОД/ФТ/ФРОМУ. Информация, содержащаяся в этом отчете, собиралась в ходе заседаний специальных рабочих групп с участием различных заинтересованных лиц на уровне стран. При составлении окончательной редакции отчета была использована информация, полученная от сотрудников органов, отвечающих за защиту данных, ученых и других экспертов, поставщиков технологий и представителей финансового сектора.

7. Выявление лиц, осуществляющих ОД/ФТ, расследование их деятельности и их судебное преследование с одновременной защитой данных и неприкосновенности частной жизни людей является обязательным; очень важно, чтобы осуществлялось и то, и другое. Это позволит защитить безопасность общества, мировые рынки и государственную безопасность, а также демократию и обеспечить верховенство закона. Более того, имеет смысл исследовать, способна ли реализация инициатив по обмену информацией с использованием соответствующих мер защиты обеспечить ЗДЛЖ путем: повышения точности информации, содержащейся в СПО, уменьшения количества ложноположительных случаев и их расследований или уменьшения объема персональных данных, предоставляемых органам власти. Это было отмечено некоторыми органами власти, отвечающими за ЗДЛЖ; они применили инициативный подход, способствуя обмену информацией между субъектами частного сектора, поддерживая его и одновременно с этим обеспечивая применение соответствующим мер защиты в области ЗДЛЖ. Например, Управление уполномоченного по информации Великобритании (органа власти, отвечающего за ЗДЛЖ) признало, что «подход к борьбе с финансовыми преступлениями на основе сотрудничества позволяет увеличить количество случаев выявления преступной деятельности и уменьшить количество ложноположительных случаев, одновременно с этим снижая нагрузку на клиентов - физических и юридических лиц в виде их проверок»[6]. По мере увеличения количества реализуемых инициатив по обмену информацией будет поступать больше данных, позволяющих понять, может ли этот вид обмена повысить эффективность ПОД/ФТ/ФРОМУ, а также когда и как это произойдет.

8. Для того, чтобы страны и субъекты частного сектора могли эффективно разрабатывать и реализовать проекты по обмену данными в области ПОД/ФТ/ФРОМУ в соответствии с законами, подзаконными актами и принципами, касающимися ЗДЛЖ, важно, чтобы каждый проект осуществлялся с учетом конкретной ситуации. Кроме этого, необходимо, чтобы каждый проект соответ-

[6] Отчет органа власти Великобритании, отвечающего за ЗДЛЖ (Управление уполномоченного по информации) о регулятивных песочницах, введенных органом власти Великобритании, отвечающим за ЗДЛЖ, стр. 3, пункт 1.2: https://ico.org.uk/media/for-organisations/documents/2618552/futureflow-sandbox-report.pdf

ствовал применимым требованиям и основывался на особенностях конкретной инициативы, ориентируясь, по возможности, на приведенные в данном отчете примерах. Например, общие цели, стандарты и протоколы, при помощи которых осуществляется обмен информацией между субъектами частного сектора, предназначенный для выявления сетей профессиональных отмывателей, направления сообщений о них и, в конечном итоге, прекращения их деятельности.

РАЗДЕЛ II.
Общие требования к ПОД/ФТ/ФРОМУ и вклад обмена информацией между субъектами частного сектора в их эффективное соблюдение

9. В этом разделе содержится введение в международные требования к ПОД/ФТ/ФРОМУ для экспертов, не являющихся специалистами в этой области. В нем приводится общее описание обмена информацией между субъектами частного сектора и подчеркивается полезность такого обмена для предотвращения ОД/ФТ/ФРОМУ. В последующих разделах уделяется внимание обмену информацией для выявления подозрительных операций, расследования и сбора информации о них.

10. В Стандартах ФАТФ[7] содержатся требования к национальным системам ПОД/ФТ/ФРОМУ и предусмотрена система для реализации международных правовых обязательств, содержащихся в Конвенции ООН о борьбе против незаконного оборота наркотических средств и психотропных веществ от 1988 г., Конвенции ООН против транснациональной организованной преступности от 2000 г., Конвенции ООН по борьбе с коррупций от 2003 г. и Конвенции о борьбе с финансированием терроризма от 1999 г., а также реализации резолюций СБ ООН. Они являются международным стандартом по борьбе с ОД/ФТ/ФРОМУ и другими связанными с ними угрозами безопасности мировой финансовой системе. Свыше 200 стран выразили решимость соблюдать Стандарты ФАТФ и проходить детальные оценки по их соблюдению.

11. В Стандартах ФАТФ содержится ряд обязательных требований, которые юрисдикции должны предъявлять к субъектам частного сектора своей страны (с помощью национального законодательства, подзаконных актов и других мер). Такие требования совместно именуются «превентивные меры»; они являются основой деятельности, направленной на выявление незаконных средств и осуществляемой регулирующими и правоохранительными органами. К таким требованиям относится сбор и хранение личных данных (например, для проверки личностей). Что касается именно обмена информацией, в настоящее время Стандарты ФАТФ требуют осуществлять такой обмен между субъектами частного сектора применительно к корреспондентским банковским отношениям, обработке электронных переводов, доверию мерам третьих сторон и реализации программ по ПОД/ФТ, охватывающих финансовую группу. Обмен информацией может осуществляться как автоматически, так и в ручном режиме. Несмотря на то, что в отношении остальных ситуаций обязательные требования ФАТФ к обмену информацией отсутствуют, юрисдикции могут реализовывать другие инициативы по обмену информацией для более эффективного распределения ресурсов на основе риск-ориентированного подхода и разрабатывать инновационные методы по борьбе с ОД/ФТ/ФРОМУ.

[7] Группа разработки финансовых мер борьбы с отмыванием денег (ФАТФ) является межгосударственной организацией, созданной в 1989 г. министрами ее стран-членов, задачей которой является установление стандартов и обеспечение эффективного применения правовых, регуляторных и оперативных мер по борьбе с ОД, ФТ и ФРОМУ и другими связанными с ними угрозами безопасности международной финансовой системы.

12. Этот отчет посвящен обмену информацией, целью которого является обеспечение направления СПО[8] в ПФР. Описание других требований, которые могут относиться к обмену информацией, приведено в Приложении А.

Требования к СПО[9]

13. Рекомендация 20 предусматривает, что если финансовое учреждение подозревает или имеет достаточные основания подозревать, что какие-либо денежные средства являются доходами от преступной деятельности либо имеют отношение к ФТ, оно должно незамедлительно сообщить о своих подозрениях в ПФР своей страны. Требование о направлении сообщения должно быть непосредственным императивным обязательством; в соответствии с Р.20 наличие какого-либо косвенного или опосредованного обязательства, касающегося направления сообщения о подозрительной операции, неприемлемо.

14. Для снижения рисков ОД/ФТ/ФРОМУ, с которыми сталкиваются субъекты частного сектора, они должны применять риск-ориентированный подход. Например, для выявления возможной подозрительной деятельности учреждения могут выделять дополнительные ресурсы для тех областей (клиенты, услуги, продукты, места и т.д.), которые, по их мнению, обладают повышенным риском. Для соблюдения требований, предусмотренных в Р.20, субъекты частного сектора должны собирать и направлять выявленную информацию в ПФР. Кроме этого, они должны устанавливать и проверять личности клиентов и осуществлять непрерывный мониторинг их операций или материального положения для того, чтобы убедиться, что деятельность клиентов соответствует предоставленной информации, и для того, чтобы иметь основание, позволяющее понять, являются ли осуществляемые ими операции подозрительными. Субъекты частного сектора используют системы мониторинга операций, в т.ч. распространенные индикаторы риска (например, индикаторы, предоставляемые ФАТФ, государственными учреждениями или коммерческими провайдерами) для выявления возможной подозрительной деятельности, имеющей отношение к различным видам преступлений. Задачей этой системы является обеспечение того, чтобы финансовый сектор не использовался для финансирования преступлений, терроризма или для уклонения от финансовых санкций, касающихся терроризма и ФРОМУ.

15. Как было указано в Аналитическом отчёте по итогам 1 этапа, обмен информацией (как между субъектами частного сектора, так и между субъектами частного бизнеса и государственными учреждениями) очень важен для борьбы с ОД/ФТ/ФРОМУ. Лицам, осуществляющим преступные схемы в нескольких странах, не мешают границы государств; злоумышленники или террористы не используют только одно учреждение для отмывания своих незаконных доходов или перемещения либо использования денежных средств, имеющих отношение к терроризму[10]. В Аналитическом отчёте по итогам 1 этапа говорится о целях и необходимых условиях обмена информацией по ПОД/ФТ/ФРОМУ между субъектами частного сектора и ее анализа[11]. Существуют требования ФАТФ по обмену информацией

---

[8] В законодательствах некоторых стран они иногда именуются сообщения о подозрительной деятельности (СПД) или сообщения о необычной операции (СНО).

[9] В пунктах 77-79 Аналитического отчёта по итогам 1 этапа объясняется, как правила соблюдения конфиденциальности информации, содержащейся в СПО, могут создавать проблемы для обмена информацией между субъектами частного бизнеса.

[10] См. также пункт 23 части I Отчета.

[11] См. раздел 4 Аналитического отчёта по итогам 1 этапа.

между субъектами частного сектора[12], которые касаются корреспондентских банковских отношений (Рекомендация 13), осуществления электронных переводов (Рекомендация 16) и применения мер по ПОД/ФТ ко всей финансовой группе (Рекомендация 18). Кроме этого, обмен информацией осуществляется для соблюдения других требований, в т.ч. установления и проверки личностей клиентов или бенефициарных владельцев (Рекомендации 10, 24 и 25), и управления риском (Рекомендация 1) особенно в рамках государственно-частных партнерств.

Вставка 2.1. Возможные случаи обмена информацией, которые могут помочь бороться с ОД, ФТ и ФРОМУ

Как говорится в части I Отчета, во многих юрисдикциях обмен данными между субъектами частного сектора, входящими в разные финансовые группы, запрещен в связи с наличием требований, касающихся ЗДЛЖ и (или) основных прав, предусмотренных законодательством конкретной страны. В соответствии с применимым национальным законодательством и необходимостью снижения риска ОД/ФТ/ФРОМУ, ФУ могут выразить желание обмениваться данными как внутри финансовых групп, так и за их пределами, а также, возможно, с ФУ, находящимися в других юрисдикциях. Это позволит им обеспечить более эффективное применение мер по НПК и достижение других таких целей по управлению риском совершения финансовых преступлений, о которых говорится ниже. В приведенном ниже списке указывается, почему обмен информацией для ПОД/ФТ/ФРОМУ между субъектами частного сектора может приносить пользу в качестве важной цели государственной политики. Включение в данный список не является основанием полагать, что рассматриваемая информация соответствует применимым оценкам, проверкам или пороговым значениям, предусмотренным в правилах по ЗДЛЖ.

- **Установление или проверка личности клиента:** для проверки личности клиента; для проверки того, присутствовали ли ранее в деятельности физического или юридического лица риск-индикаторы или проблемы; для определения рейтинга риска клиентов с помощью проверки того, не вел ли себя клиент аналогичным образом в других областях деятельности.
- **Мониторинг операций:** для выявления структурирования[13] путем проверки модели осуществлении операций клиентом для оценки профиля его финансовой деятельности; принятия последующих мер в случае выявления необычной деятельности, осуществляемой в одной или нескольких организациях; более эффективного выявления подозрительной деятельности (или наоборот, более эффективного выявление деятельности, которая необычна, но не является подозрительной); применения пороговых значений при совершении операций.
- **Проверка по санкционным или другим спискам:** для проверки клиентов и сторон операции по санкционным спискам ООН и национальным санкционным спискам (в т.ч. в связи с ФТ и ФРОМУ). К таким проверкам также относятся проверки по спискам ПДЛ или другим спискам, направленным провайдерами коммерческих услуг.

[12] ФАТФ (2016-2017 гг.) Все Стандарты ФАТФ, касающиеся обмена информацией, ФАТФ, Париж, в ноябре 2017 г. в документ внесены изменения.

[13] Структурирование происходит после размещения незаконных доходов в финансовой системе. Денежные средства дополнительно легитимизируются и отдаляются от своего незаконного источника с помощью дополнительных операций или использования финансовых инструментов (элементов структуры).

- **Понимание риска и управление коммерческими отношениями:** для непрерывного обновления информации о клиенте; для выявления подверженности глобальному риску в результате приема одного и того же клиента на обслуживания в учреждениях различных юрисдикций; активного управления риском для учета новой информации или изменений поведения клиента.
- **Выявление бенефициарного владельца:** для повышения точности выявления бенефициарных владельцев; для выявления одного и того же бенефициарного владельца в нескольких учреждениях; для повышения эффективности выявления подставных компаний или для разработки более эффективного порядка хранения данных, касающихся бенефициарных владельцев.
- **Выявление типологий совершения преступлений:** для более быстрого и точного выявления появляющихся типологий совершения преступлений, выработки мер противодействия, а также обмена результатами исследований с другими организациями и госсектором.
- **Расследования в целях финразведки:** проведение инициативных расследований на основе анализа возможных подозрительных операций для выработки более обоснованных выводов, которые могли быть использованы в расследованиях, проводимых ПФР и правоохранительными органами.

16. В соответствии с применимой правовой базой, страны или субъекты могут принять решение, что обмен информацией между субъектами частного сектора необходим для эффективного снижения рисков ОД/ФТ/ФРОМУ, с которыми они сталкиваются, и, в частности, (для целей этого документа) выявления подозрительных операций. Различные обсуждения, проведенные ФАТФ как с представителями государственных, так и коммерческих учреждений[14], показали, что одному субъекту частного сектора становится все труднее выявлять подозрительные операции, являющиеся частью сложных схем, которые нацелены на то, чтобы избежать их выявления. ФАТФ и другие заинтересованные лица сообщали об изощренных схемах ОД/ФТ/ФРОМУ, в которых участвовали сложные юридические образования и использовались модели осуществления операций, которые затрудняют или делают невозможным их выявление без получения информации от банков-контрагентов или других банков, предоставляющих услуги тому же клиенту или его сообщникам. Более того, по мере увеличения количества операций, системам мониторинга операций становится все труднее выявлять подозрительную деятельность. Отсутствие доступа к дополнительной информации, предоставляемой другими субъектами частного бизнеса, и возможности ее обработки создают опасность того, что такие системы будут выявлять операции, которые не являются подозрительными, в результате чего будут направляться сообщения о ложноположительных случаях. Осуществляемый соответствующим образом обмен данными между ФУ или между ФУ и ПФР может привести к повышению эффективности выявления подозрительных операций и уменьшению количества ложноположительных случаев. В результате, клиенты, не нарушающие закон, и операции, не связанные с незаконной деятельностью, не будут отмечаться как подозрительные.

[14] Например, проводимые ФАТФ Совместные заседания экспертов и другие встречи с представителями частного сектора, например, Консультативный форум с представителями частного сектора и другие обсуждения в рамках деятельности специальных рабочих групп и конференция на высоком уровне, проведенные в рамках этого проекта.

17. Как показали углубленные обсуждения некоторых случаев обмена информацией (см. примеры, приведенные ниже), в тех случаях, когда субъекты собирают информацию о потенциально опасных клиентах самостоятельно, им приходится собирать и фиксировать больше данных, поскольку каждому субъекту приходиться осуществлять сбор данных своими силами, чтобы понять, является ли операция или отношения подозрительными. Обмен информацией между субъектами частного сектора позволяет помочь клиентам (и органам власти) уменьшить объем собираемых данных на различных этапах и выявлять подозрительные операции с большей точностью, что позволяет улучшить результаты ПОД/ФТ/ФРОМУ и обслуживание клиентов при условии наличия надлежащих мер по ЗДЛЖ. Более целенаправленный сбор данных может также позволить субъектам частного сектора уменьшить объем работы, связанной с обработкой и анализом больших массивов недостаточно качественных данных, которые не всегда приводят к успешному выявлению подозрительной операции.

РАЗДЕЛ III.
В чем заключается защита данных, и каковы цели и требования к защите неприкосновенности личной жизни

18. Этот раздел содержит введение в требования к ЗДЛЖ для тех, кто не является специалистом в области ЗДЛЖ. Право на обеспечение неприкосновенности личной жизни предусмотрено во Всеобщей декларации прав человека и Международном пакте о гражданских и политических правах[15]. Хотя истолкование этих документов в разных юрисдикциях может быть разным, право на неприкосновенность личной жизни обычно включает в себя свободу от вмешательства или вторжения и возможность контролировать тех, кто может иметь доступ к личной информации и использовать ее[16]. Эта та точка, в которой право на неприкосновенность личной жизни пересекается с защитой данных. Несмотря на призыв ООН разработать правовую базу для защиты неприкосновенности личной жизни, в настоящее время отсутствует единая межгосударственная организация, объединяющая все страны мира, которая выработала бы международные стандарты, касающиеся законодательства в области ЗДЛЖ. Требования к ЗДЛЖ претерпели различные изменения в различных юрисдикциях, отражая их исторический и культурный опыт[17] и различные применимые правовые нормы или базы. Во многих юрисдикциях законодательство в области ЗДЛЖ обычно требует прозрачности сбора, использования данных и обмена ими, ограничивает раскрытие данных ситуациями, в которых человек дает свободное и информированное согласие[18] или в которых существует другое законное основание для раскрытия данных, и предоставляет людям право доступа к их данным, право вносить изменения в неправильные данные или удалять их, а также право на восстановление нарушенных прав или применение средств судебной защиты в связи с нарушениями права на неприкосновенность личной жизни с некоторыми ограниченными исключениями (например, касающимися правоохранительных органов или органов государственной безопасности).

19. Международные организации разработали принципы ЗДЛЖ, которые легли в основу конституций, законодательств и подзаконных актов некоторых стран. В 1976 г. ООН разработала Международный пакт о гражданских и политических правах (МПГПП), который требует от государств защищать определенные права и свобо-

[15] Статья 12 Всеобщей декларации прав человека; статья 17 Международного пакта о гражданских и политических правах (защита от «необоснованного или незаконного вмешательства в … личную жизнь»).

[16] Там же; Резолюция ООН 73/179 (2018) Право на защиту неприкосновенности частной жизни в цифровую эпоху.

[17] Серьезные нарушения ЗДЛЖ повлияли на интерпретацию соответствующих правил. Такие нарушения совершались как государственными, так и коммерческими учреждениями (например, технологические компании отслеживали данные в коммерческих или рекламных целях).

[18] Свободное согласие обычно требует, чтобы человек имел свободу выбора и был в состоянии отказаться или отозвать свое согласие без попадания в невыгодное положение. Другие требования, касающиеся дачи согласия, приведены в соответствующих национальных и международных законодательствах, например, Конвенции о защите частных лиц в отношении автоматизированной обработки данных личного характера.

ды человека, в т.ч. право на неприкосновенность личной жизни[19]. Первое заседание Глобальной ассамблеи по защите конфиденциальности состоялось в 1979 году; эта Ассамблея является глобальным форумом, где представители органов власти, отвечающие за защиту данных и неприкосновенность личной жизни, обсуждают проблемы этой области. Ассамблея играет ведущую роль в мире в области защиты данных и неприкосновенности личной жизни, объединяя свыше 130 органов власти различных стран, отвечающих за защиту данных и неприкосновенности личной жизни[20]. В 1980 г. Организация экономического сотрудничества и развития (ОЭСР) приняла Правила защиты неприкосновенности личной жизни, в 2003 г. этот документ был пересмотрен. В настоящее время ОЭСР формирует группу экспертов по странам, в т.ч. из правоохранительных органов, органов государственной безопасности и государственных органов, для разработки принципов доступа государства к личным данным, хранящимся у субъектов частного сектора, для обеспечения законности и государственной безопасности[21]. В 1981 г. Совет Европы (СЕ) – организация, которая играет ведущую роль в решении вопросов защиты неприкосновенности личной жизни в международном масштабе, – приняла Конвенцию о защите частных лиц в отношении автоматизированной обработки данных личного характера (Конвенцию 108). К настоящему времени эту Конвенцию подписало 55 стран, расположенных на трех континентах; недавно она стала называться Конвенция 108+[22]. Кроме этого, СЕ в настоящее время разрабатывает проект правил, касающихся вопросов защиты данных, возникающих при обмене информацией в целях ПОД/ФТ/ФРОМУ.

20. В действующей в Европе Европейской конвенции о правах человека указывается, что государственные органы не должны вмешиваться в осуществление права на защиту частной и семейной жизни, за исключением случаев, когда это осуществляется в соответствии с законом и необходимо в демократическом обществе (статья 8). В 2000 г. Европейский союз (ЕС) принял Хартию по правам человека, которая защищает основное право на защиту частной жизни (статья 7) и личных данных (статья 8). В ней указывается, что любое ограничение таких прав должно осуществляться по закону и что ограничения такого рода могут вводиться, если они необходимы и действительно отвечают интересам общества (статья 52). В ней также предусмотрен принцип соразмерности. В 2016 г. ЕС принял обширный регламент о защите данных, который непосредственно применяется его странами-членами - Общий регламент по защите данных (ОРЗД)[23].

---

[19] Во многих статьях этого Пакта говорится, что люди должны иметь «право на свободу и неприкосновенность личности», «неотъемлемое право на жизнь… защищенное законом», «свободу перемещения и выбора своего местожительства», «право придерживаться своих мнений без препятствования этому», и «право на свободу высказывания»; «никто не должен подвергаться произвольному или незаконному вмешательству в свою личную жизнь, семью, дом или переписку, и не подвергаться незаконным нападкам на свою честь и репутацию». http://www.ohchr.org/EN/Issues/RuleOfLaw/CompilationDemocracy/Pages/ICCPR.aspx

[20] Сначала Ассамблея называлась Международной конференцией уполномоченных по защите данных и частной жизни, https://globalprivacyassembly.org/.

[21] См, например, ОЭСР (2021 г.), Отчет Генерального секретаря ОЭСР перед министрами, 2021 г., Издательство ОЭСР, Париж, https://doi.org/10.1787/8cd95b77-en, ОЭСР (2021 г.), Доступ государств к личным данным, хранящимся у субъектов частного сектора: Заявление Комитета ОЭСР относительно политики в области цифровой экономики.

[22] Конвенция 108+, Конвенция о защите частных лиц в отношении автоматизированной обработки данных личного характера, июнь 2018 г., http://www.coe.int/dataprotection.

[23] Регламент (ЕС) 2016/679 Европейского Парламента и Совета Европы от 27 апреля 2016 г. о защите частных лиц в отношении автоматизированной обработки данных личного характера и о свободном перемещении таких данных, и признании недействительным Директивы 95/46/ЕС (Общий регламент по защите данных). В то же время, ЕС принял Директиву о защите данных (ЕС) 2016/680 для полиции и органов уголовной юстиции. Она применяется в тех случаях, когда личные данные обрабатываются компетентными органами для обеспечения законности, поэтому она не имеет отношения к обмену информацией между субъектами частного сектора.

Контроль за выполнением ОРЗД и обеспечение его выполнения осуществляется органами, отвечающими за защиту данных (ООЗД), всех стран-членов ЕС и Европейской экономической зоны. Европейский совет по защите данных, в который входят представители каждого ООЗД и Европейская инспекция по защите данных (ЕИЗД), обеспечивает последовательное применение ОРЗД во всех странах ЕС. ЕИЗД обеспечивает, чтобы Регламент ЕС по защите данных (этот документ дополняет ОРЗД) применялся учреждениями, организациями и органами власти стран-членов ЕС.

21. На американском континенте целью Принципов защиты частной жизни и личных данных (Организация американских государств, 2021 г.) и Стандартов защиты личных данных (Иберо-американская сеть по защите данных, 2017 г.) является определение основных элементов эффективной защиты и выработка общих принципов защиты данных в этом регионе.

22. Помимо этих документов, действие которых распространяется на множество стран, в мире также существуют различные конституции, законы, подзаконные акты, правила и регламентирующие документы отдельных стран, касающиеся прав на защиту частной жизни[24]. Законодательства примерно 145 юрисдикций обеспечивают защиту данных и частной жизни. Как отмечалось выше, на государства-члены ЕС распространяется действие Общего регламента ЕС по защите данных (ОРЗД). ОРЗД Великобритании и ее Закон о защите данных от 2018 г. являются правовой основой защиты данных в этой стране; они эквивалентны ОРЗД ЕС. Конституция США содержит основание для защиты частной жизни путем запрета проведения необоснованных обысков и конфискаций, а также другие меры защиты[25]. В ответ на опасения, возникающие в связи с внедрением компьютеров и систем автоматической обработки данных, в США были разработаны «принципы добросовестного использования данных», которые стали частью Закона о неприкосновенности частной жизни от 1974 г.[26] Этот закон регулирует сбор, хранение, использование и предоставление информации о физических лицах, которая хранится в системах данных федеральных органов власти, и требует прозрачности использования и предоставления информации, а также применения средств судебной защиты в отношении нарушений[27]. Законы США в области защиты данных, принятые позднее на федеральном уровне и уровне штатов, касались конкретных секторов и связанных с ними рисков,

[24] Дж. Гринлиф (2021 г.) Ситуация с «Законодательствами по защите данных различных стран в 2021 г.: Несмотря на задержки, связанные с COVID-19, 145 стран приняли Общий регламент по защите данных», доступно на: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3836348

[25] «Право народа на гарантии неприкосновенности личности, жилища, бумаг и имущества от необоснованных обысков и арестов не должно нарушаться, и никакие ордера не должны выдаваться иначе как при достаточных к тому основаниях, подтвержденных присягой либо заявлением, и с подробным описанием места, подлежащего обыску, и лиц или предметов, подлежащих аресту». 4-ая поправка к Конституции США.

[26] См. «Документы, компьютеры и права граждан», Доклад Консультационного комитета министра об автоматических системах обработки личных данных, Министерство здравоохранения, образования и социального обеспечения США (июль 1973 г.).

[27] См. Закон о неприкосновенности частной жизни от 1974 г., 5-ая сводная кодификация федерального законодательства США, пункт 552a, Министерство юстиции США, Управление по защите неприкосновенности частной жизни и гражданских свобод, Обзор Закона о неприкосновенности частной жизни от 1974 г., с документом можно ознакомиться по ссылке: https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition. Для правоохранительных органов и органов государственной безопасности применяются определенные исключения. Закон о неприкосновенности частной жизни, 5-ая сводная кодификация федерального законодательства США, пункты 552a (j)-(k). Обратите вниманием, что после принятия Закона о восстановлении нарушенных прав с помощью судебных органов от 2015 г. гражданам некоторых стран были предоставлены определенные права на восстановление нарушенных прав, 5-ая сводная кодификация федерального законодательства США, примечание к пункту 552a.

например, Закон Грэмма-Лича-Блайли (с учетом внесенных в него изменений и дополнений) содержит правила, касающиеся деятельности субъектов финансового сектора, в т.ч. правила обеспечения неприкосновенности частной жизни, выполнение которых обеспечивается соответствующими регуляторами финансовой деятельности США[28].

23. Несмотря на то, что тип и объем требований в области ЗДЛЖ в разных юрисдикциях являются разными, осуществленный выше анализ законов и правовых документов, а также обсуждения с органами власти, отвечающими за ЗДЛЖ, показывают, что в основе таких документов зачастую лежат схожие общие принципы и что они предусматривают механизмы контроля и отчетности, обеспечивающие наличие эффективных мер защиты. К таким принципам может относиться следующее:

- **Тип данных:** меры защиты данных и неприкосновенности частной жизни обычно применяются к личным данным, имеющим отношение к физическим лицам; при определении термина личные данные зачастую используются такие понятия, как идентифицируемость (например, с помощью имени, числа или места либо с помощью сочетания идентифицирующих факторов). Могут также существовать различные категории личных данных (как предусмотренных, так и не предусмотренных в нормативных базах).
- **Законное право (или «законное основание»):** в некоторых юрисдикциях (например, в ЕС) для обработки личных данных необходимо законное основание. В соответствии с ОРЗД, существует ограниченный список законных оснований для использования или обработки личных данных, в т.ч. свободное согласие субъекта на обработку для одной или нескольких конкретных целей; обработка, необходимая для выполнения контракта; для выполнения юридического обязательства; для выполнения задачи, осуществляемой в интересах общества, или при осуществлении официальных полномочий, которыми наделены лица, работающие с личными данными, или для обеспечения законных интересов (если только, после соответствующего анализа, не обнаружится веской причины защищать данные) при условии соблюдения требований обеспечения необходимости и соразмерности. Для применения основания, связанного с «законным интересом», оператору личных данных (физическому или юридическому лицу, определяющему цели и средства обработки)[29] обычно нужно идентифицировать законный интерес, продемонстрировать необходимость обработки данных для его обеспечения и сопоставить его с интересами, правами и свободами соответствующего физического лица.
- **Цель и использование:** данные должны обрабатываться или использоваться в соответствии с конкретной законной целью, они не должны использоваться для каких-либо ненадлежащих целей. Обработка личных данных должна осуществляться для конкретной, четко сформули-

[28] Закон о модернизации финансовых услуг Грэмма-Лича-Блайли, 15-ая Сводная кодификация федерального законодательства США, пункты 6801, 6809 и 6827 (1999)

[29] В ОРЗД содержится следующее определение понятия «оператор личных данных»: «Оператор личных данных — это физическое или юридическое лицо, которое самостоятельно или совместно с другими лицами определяет цели и средства обработки личных данных (пункт 4(7). Статус оператора влечет за собой юридические обязательства и возможную ответственность в случае нарушений.

рованной цели; данные не должны дополнительно обрабатываться или использоваться для других целей, за исключением того случая, если это разрешено и (или) совместимо с изначальной целью.

- **Необходимость, обоснованность, соразмерность и минимизация:** даже в случае наличия законного основания для обработки данных в некоторых юрисдикциях в этой ситуации обработка данных должна быть необходимой, обоснованной и пропорциональной. Например, в зависимости от юрисдикции это может значить, что: данные могут храниться только пока они необходимы; сбор информации должен быть обоснованным: ее не следует собирать больше, чем необходимо для целей ее обработки; не должно использоваться других обоснованных и менее «настойчивых» способов для достижения этой цели. Учреждения должны подумать над тем, до какой степени они могут достигнуть своих целей *без* обмена личными данными (например, за счет использования существующих технологий обезличивания).

- **Качество и достоверность:** личные данные должны храниться таким образом, чтобы они были точными, надежными, полными, непротиворечивыми и взаимосвязанными. Это может включать обязанность поддерживать данные в настолько актуальном состоянии, насколько это необходимо для их обработки, с учетом тех целей, для которых она осуществляется.

- **Справедливость, в т.ч. при принятии решений на основании автоматической обработки:** обработка должна быть корректной и осуществляться на законных основаниях. Решения, которые способны оказывать существенное негативное влияние на интересы человека, не должны приниматься исключительно на основании автоматической обработки личных данных, за исключением случаев, когда это разрешается осуществлять по национальному законодательству и при условии соблюдения соответствующих мер защиты. В зависимости от юрисдикции такой порядок может применяться только к тем случаям, когда негативное влияние касается цели, для достижения которой обрабатываются данные, или к большему количеству случаев. В некоторых юрисдикциях решения на основании автоматической обработки данных могут приниматься только при соблюдении определенных условий.

- **Прозрачность:** субъекты данных должны информироваться, помимо прочего, о том, как будут обрабатываться личные данные, кто будет их обрабатывать, для какой цели и в какой объеме они обрабатываются или будут обрабатываться; физические лица и соответствующие органы власти должны информироваться о несанкционированном доступе к данным.

- **Передача или раскрытие данных:** существуют юрисдикции, в которых передача данных или их раскрытие другой организации может происходить только после достижения предварительного добровольного согласия, которое может быть отозвано в любой момент. Существуют также юрисдикции, в которых разрешается осуществлять передачу или раскрытие (независимо от наличия согласия) при наличии соответствующего юридического основания при соблюдении определенных ограничений, предусмотренных в законодательстве, позволяющих обеспечить постоянную защиту данных, необходимость и соразмерность.

- **Защита данных от несанкционированного использования:** личные данные должны обрабатываться с помощью соответствующих физических, технических и организационных мер, обеспечивающих защиту данных, в частности, от несанкционированной или незаконной обработки, случайной утраты, уничтожения или повреждения. Должна вестись документация, в которой будет отражаться следующая информация: кто имеет доступ к личным данным, как они используются и раскрываются, например, компьютерные контрольные журналы.

- **Получение доступа, внесение изменений и другие права субъектов данных:** должны существовать процедуры, позволяющие физическим лицам получать информацию о личных данных, запрашивать и получать доступ к ним, а также направлять запрос о внесении изменений в данные, которые, по их мнению, являются неточными, либо их удаление в некоторых юрисдикциях, при условии соблюдения разумно обоснованных ограничений, предусмотренных в местном законодательстве, например, касающихся обеспечения правопорядка и государственной безопасности. В зависимости от применяемой правовой системы, к другим правам субъектов данных относится право на сокрытие или удаление данных, право на ограничение их обработки и право на компактность данных (т.е. право субъекта на получение личных данных от оператора личных данных в структурированном, общепринятом и машиночитаемом виде).

- **Подотчетность и контроль:** использование и обработка данных должны анализироваться одним или несколькими органами, которые осуществляют функционально независимый эффективный контроль либо самостоятельно, либо совместно с другими органами.

- **Восстановление нарушенных прав:** должны быть предусмотрены соответствующие эффективные механизмы, позволяющие человеку направлять претензии и восстанавливать нарушенные права. При условии соблюдения разумно обоснованных ограничений, предусмотренных во внутреннем законодательстве, такие механизмы должны предусматривать получение и изучение претензий, направляемых физическим лицом, к которому относятся личные данные и которое обращается за защитой своих прав в связи с доступом к данным, их изменением или предполагаемой недолжной их обработкой. В некоторых юрисдикциях физические лица могут добиваться восстановления своих прав, обращаясь в суды и действуя в соответствии с правовыми нормами.

- **Оценки влияния:** законы, подзаконные акты и регламентирующие документы многих юрисдикций требуют от учреждений оценивать риски, касающиеся защиты данных и неприкосновенности частной жизни, возникающие у физических лиц в связи с предполагаемым сбором, использованием, предоставлением или другими видами обработки личных данных, и находить способы сведения к минимуму таких рисков[30]. Например, в соответствии с ОРЗД такая оценка и уменьшение рисков должна документироваться и называться «Оценка влияния на защиту данных» («ОВЗД»); в США федеральные органы власти должны оформлять «Оценку влияния на личную жизнь»[31].

[30] Дополнительные оценки влияния могут также оказаться полезными для выявления и снижения других типов рисков. См. пункт 59 в Разделе 6 этого документа (Об оценках влияния на права человека и Оценках законных интересов).

[31] См. статью 35 ОРЗД; закон об электронном правительстве от 2002 г., государственный закон 107-347 (2002), раздел 208.

24. Законы и документы, касающиеся ЗДЛЖ, также содержат исключения, изъятия, ограничения, накладываемые на права на неприкосновенность частной жизни в определенных ситуациях, в т.ч. для предотвращения, расследования, выявления уголовных преступлений или судебного преследования за них. Все вышеперечисленное может применяться только к определенным преступлениям, таким, как мошенничество или терроризм. Даже в этих случаях соответствующим лицам, как правило, следует рекомендовать в той степени, в какой это применимо, учитывать изложенные выше принципы ЗДЛЖ при разработке инициатив по обмену информацией между субъектами частного сектора. Действуя таким образом, они, возможно, уменьшат риски, связанные с ЗДЛЖ, особенно возникающие у тех субъектов, которые действуют в нескольких юрисдикциях, и обеспечат большее доверие общества к таким инициативам[32].

[32] Например, в США Министерство юстиции разработало и применяет меры и процедуры в контексте обеспечения законности и государственной безопасности для защиты личных данных и уменьшения рисков, например, Правила Государственного прокурора по проведению ФБР расследований в области государственной безопасности и сбора им данных, получаемых за рубежом, Пособие по отправлению правосудия, Руководство ФБР по оперативно-следственной деятельности, в которое часто вносится информация о новых законах и процессуальных нормах, указы Президента США, внутренние регламентирующие документы, передовые методы работы и новые информационные технологии. См. раздел 2.3 Указа Президента США 12333; Пособие по отправлению правосудия (2018),; ФБР, Руководство по оперативно-следственной деятельности, (2016).

РАЗДЕЛ IV.
Примеры обмена информацией

25. Ниже приводятся примеры, в которых показано, как субъекты частного бизнеса и органы власти прилагали (или прилагают) усилия, чтобы соотнести цели ПОД/ФТ/ФРОМУ с целями ЗДЛЖ, действуя в рамках соответствующих правовых систем, в целях обеспечения обмена информацией между субъектами частного сектора в целях ПОД/ФТ/ФРОМУ. Большая часть этих проектов разрабатывалась, осуществлялась и координировалась совместно с органами власти, отвечающими за ПОД/ФТ/ФРОМУ, и органами власти, отвечающими за ЗДЛЖ. В этих примерах говорится не только о цифровой трансформации, но и о других мерах. Хотя большинство примеров касается обмена информацией в целях ПОД/ФТ/ФРОМУ, также приведен один пример обмена информацией, связанной с мошенничеством, поскольку в нем описывается режим сертификации/выдачи разрешения органом власти, отвечающим за ЗДЛЖ; он иллюстрирует реализацию похожих инициатив.

26. В этих примерах описываются различные ситуации, в каждой из которых осуществлялся свой анализ правил ЗДЛЖ: (a) обмен данными и анализ больших объемов обезличенной/псевдонимизированной/зашифрованной информации, целью которых является выявление подозрительных операций (этот процесс называется **«обмен информацией до возникновения подозрений»**), и (b) целенаправленный обмен информацией, имеющей узкую направленность, для проведения конкретных расследований с помощью персонифицированной информации, имеющей отношение к подозрительным операциям (этот процесс называется **«обмен информацией после возникновения подозрений»**). Как показано в приведенных ниже примерах, в зависимости от соответствующего режима эти два типа обмена информацией сопряжены с различными аспектами ЗДЛЖ, которые необходимо учитывать. При этом на обмен информацией перед возникновением подозрений налагаются более строгие ограничения, предусмотренные правами на защиту неприкосновенности частной жизни физического лица.

27. Большинство примеров посвящено обмену информацией между субъектами частного сектора (т.е. между финансовыми учреждениями); в некоторых из них речь идет об обмене информацией с государственными органами.

28. В основе приводимых ниже примеров лежит информация, предоставленная органами власти или соответствующими учреждениями, либо общедоступная информация. Правовая позиция и факты, представленные в этих примерах, отражают взгляды соответствующих юрисдикций и заинтересованных лиц, а не ФАТФ.

Вставка 4.1. Пилотный проект «Три Банка» (обмен информацией между субъектами частного сектора до возникновения подозрений в рамках регулятивной песочницы с участием компании «FutureFlow» и Управления уполномоченного по информации Великобритании)

Описание: В рамках пилотного проекта «Три Банка» осуществлялся обмен перед возникновением подозрений большими массивами данных об операциях, которые подверглись псевдонимизации, т.е. данными об операциях с псевдонимизированными идентификаторами счетов для создания кластеров или типологий.

Участники:

- Пилотный проект «Три банка» реализовывался под руководством консалтинговой компании; в нем участвовало три банка (операторы персональных данных) и один поставщик технологий (FutureFlow, лицо, обрабатывающее личные данные (физическое или юридическое лицо, которое обрабатывает личные данные))[1].
- До начала реализации этого проекта представители органа власти Великобритании, отвечающего за ЗДНЖ (Управления уполномоченного по информации (УКИ), встретились с представителями компании Future Flow и обсудили основные проблемы, связанные с защитой данных, которые возникают в ходе осуществления такой деятельности в ситуации «регулятивной песочницы»[2].

Конкретная задача или цель: задачей проекта «Три банка» являлось увеличение количества случаев выявления связанных между собой операций, которые казались необычными, и могли иметь отношение к ОД/ФТ. В тех случаях, когда операция помечалась как необычная, соответствующий банк повторно ее идентифицировал и, руководствуясь своими обычными регламентирующими документами и процедурами, проводил изучение дополнительной информации, и, если это было обоснованно, направлял СПО.

Виды данных, которые собирались и которыми обменивались: в рамках пилотного проекта «Три банка» изучались псевдонимизированные операции, которые совершались малыми и средними предприятиями ранее в течение года. Использование псевдонимизированных данных позволило свести к минимуму риски, связанные с защитой данных и неприкосновенностью частной жизни, но, в связи с тем, что такие данные могли быть повторно идентифицированы, в соответствии с применимым законодательством эти данные рассматривались в качестве личных данных. Эта технология позволила выявить модели осуществления операций, которые, возможно, были подвержены высокому риску или являлись необычными; после этого банки смогли повторно идентифицировать свои данные для получения дополнительной информации и установить наличие оснований для подозрений. После псевдонимизирования использовались следующие категории личных данных: идентификатор счета (например, номер счета, номер отделения банка, международный номер банковского счета и т.д.), сумма операции (суммы операций), код операции и отметки о времени совершения операции.

Правовое основание обработки личных данных: во время осуществления этого проекта каждому банку (операторам персональных данных) нужно было определить (в соответствии с национальным законодательством), какое правовое основание должно применяться к данным, которыми банки предлагали обмениваться. Во время этого проекта банки обменивались только псевдонимизированными данными об операциях до возникновения подозрений. После того как банк-участник проекта выявлял необыч-

ную операцию или операцию с повышенным риском, другие банки направляли только узконаправленную информацию, имеющую целевой характер, для расследования конкретной деятельности.

- Регулятивная песочница, созданная FutureFlow и УКИ до начала реализации проекта «Три Баннка», позволяла предположить, что наиболее подходящим правовым основанием является «законный интерес» (пункт 6.1(f) ОРЗД[3]). В этой связи в отчете о регулятивной песочнице, подготовленном УКИ, (а также в имеющих к нему отношение сообщениях) было помещено соответствующее заявление.
- Кроме этого, участники проекта изучали «соблюдение юридического обязательства» (пункт 6.1(c) ОРЗД[4]) в качестве возможного правового основания обмена, сравнения псевдонимизированых данных об операциях и осуществления их анализа. При этом в такой ситуации было маловероятно, что обмен данными, содержащими большое количество счетов до получения точной информации о том, что такие счета использовались для осуществления подозрительной деятельности (т.е. на стадии до возникновения подозрений) можно было бы рассматривать в качестве разумно обоснованного и пропорционального способа обеспечения соблюдения конкретного юридического обязательства. Скорее, участники проекта полагали, что это правовое основание может быть использовано для последующего обмена информацией между банками (т.е. в рамках проведения расследований с помощью платформы FutureFlow) для проведения совместных расследований, поскольку такой последующий обмен информацией касался бы тех счетов, в отношении которых возникли подозрения.

Оценка соразмерности: данные, которыми банки обменивались в рамках проекта «Три Банка», касались только малых и средних предприятий (юридических лиц) и были псевдонимизированы, что позволили свести к минимуму риски ЗДЛЖ. После формирования соответствующих кластеров содержащаяся в них информация могла быть повторно идентифицирована теми банками, которые направляли информацию (операторами персональных данных). Банки надлежащим образом изучали любые сообщения, в которых имелась информация о возможном совершении финансового преступления, на основании применимого законодательства в финансовой сфере и своих внутренних регламентирующих документов и процедур. Такое изучение происходило до изменения обслуживания подозреваемых лиц (т.е. подозреваемым лицам не отказывалось в предоставлении банковских услуг исключительно на основании наличия информации или сообщения на общей платформе).

Использовавшиеся технологии: данные об операциях псевдонимизировались на основании соглашения о хешировании и размещались на общей платформе. Такая платформа очищала собранные данные, устраняла их повторения и применяла алгоритмы анализа для выявления сложных нелинейных связей между счетами в различных банках для выявления возможных «предварительных подозрений», которые впоследствии анализировались соответствующими банками.

Участие органов власти (отвечающих за ПОД/ФТ/ФРОМУ и (или) ЗДЛЖ): хотя Управление уполномоченного по информации и не участвовало в этом проекте, оно сотрудничало с FutureFlow (поставщиком технологии и оператором персональных данных) в рамках регулятивной песочницы для оценки рисков защиты данных и определения способов их уменьшения с помощью оценки влияния на защиту данных (ОВЗД)[5]. В рамках этой работы УКИ выпустило заявление об обработке данных.

Результаты:

- Пилотный проект «Три банка» показал, что, не имея информации об определенных счетах, можно на основании обширной базы счетов автоматически создавать большие сложные кластеры и направлять их для последующего анализа учреждениями-участниками проекта. Вместе с тем, после изучения информации банками-участниками проекта некоторые такие кластеры были объяснимы. Это позволяет предположить, что анализ псевдонимизированных данных об операциях сам по себе вряд ли позволит получить необходимую информацию для выявления ОД и что потребуется провести дополнительную работу для более эффективного применения известных типологий ОД или другой оперативной информации, а также технологий или решений для выделения кластеров, в которых содержится подозрительная информация.
- Поставщик технологии создал модель, основанную на двухуровневой системе ЗДЛЖ. Деятельность на первом уровне основывалась на законном интересе, она включала в себя анализ больших массивов псевдонимизированных данных (таким образом осуществлялась защита подавляющего большинства клиентов, которые не имели отношения к полученным типологиям). Вместе с тем, после создания типологии, формирования кластеров, выявления необычной деятельности или появления предварительного подозрения дальнейший обмен информацией о счетах физических лиц мог бы основываться на соблюдении закона (сбор соответствующей информации и направление СПО либо использование правовых механизмов, предусмотренных в законодательстве о ПОД/ФТ/ФРОМУ или другом соответствующем законодательстве).

Источник: Обсуждения с участниками проекта «Три банка» и информация, полученная от них, Окончательный отчет о регулятивной песочнице: FutureFlow (октябрь 2020 г.), документ доступен по ссылке: https://ico.org.uk/media/for-organisations/documents/2618552/futureflow-sandbox-report.pdf

Примечания:

1. ОРЗД определяет лицо, обрабатывающие личные данные, как физическое или юридическое лицо, которое обрабатывает личные данные от имени оператора персональных данных (пункт 4(8)). Статус оператора персональных данных или лица, обрабатывающего данные, налагает юридические обязательства и в случае нарушений соответствующих обязанностей влечет ответственность.
2. Регулятивная песочница представляет собой механизм, позволяющий компаниям (например, поставщикам технологий) тестировать инновационные разработки и проводить эксперименты, как правило, с ограниченным количеством участников, в течение определенного периода времени, в контролируемых условиях под надзором регулирующего органа. Пилотный проект «три банка» осуществлялся не в рамках регулятивной песочницы, а после ее начального тестирования.
3. Действие регулятивной песочницы закончилось в ноябре 2020 г., в тот момент в соответствии с законодательством ЕС на Великобританию еще распространялось действие ОРЗД. В соответствии с законодательством Великобритании применимым положением является пункт 6.1(f) ОРЗД Великобритании.
4. И пункт 6.1(c) ОРЗД Великобритании.
5. Проведение ОВЗД требуется в тех случаях, когда в ходе реализации какой-либо программы может возникнуть «высокий риск для прав и свобод людей» (статья 35 ОРЗД; статья 35 ОРЗД Великобритании).

Вставка 4.2. КОСМИК (Сингапур): Программа по обмену информацией между государственным и частным сектором до и после направления СПО

Описание: КОСМИК представляет собой защищенную цифровую платформу, которая принадлежит органу финансового надзора Сингапура - Денежно-кредитному управлению Сингапура (ДКУС) – и управляется им. С помощью этой платформы осуществляется обмен информацией для выявления рисков и осуществления сотрудничества в области анализа данных. Эта платформа позволит ФУ, которые пользуются ей, обмениваться информацией о клиентах для оценки подозрений и предупреждения друг друга о наличии подозрительной деятельности в тех случаях, когда при проверке характеристик или поведения клиентов из областей повышенного риска выявляются настораживающие признаки[1]. ФУ будут обмениваться информацией об анализе рисков и данными о клиентах или операциях. На начальном этапе обмен информацией между субъектами частного бизнеса в рамках этой программы будет носить добровольный характер (до тех пор, пока работа платформы не будет отлажена), после чего ДКУС планирует сделать такой обмен обязательным.

Запланированные или достигнутые результаты: в настоящее время ФУ не разрешается предупреждать друг друга о подозрительной деятельности, осуществляемой их клиентами, поскольку им запрещается осуществлять неизбирательный обмен информацией о клиентах между собой в связи с опасениями, касающимися безопасности информации и защиты неприкосновенности частной жизни клиентов. Злоумышленники имеют возможность использовать этот изъян и осуществлять операции с помощью нескольких юридических лиц, открывая счета в нескольких ФУ. В такой ситуации одно ФУ не располагает достаточным количеством информации, позволяющей своевременно выявлять и пресекать незаконные операции. Появление у ФУ возможности обмениваться информацией о клиентах, в отношении которых было установлено, что их деятельность превышает порог серьезного риска, позволяет получить необходимую информацию, повысить эффективность выявления преступных сетей и злоумышленников, интенсифицировать борьбу с преступной деятельностью в областях основного риска и усилить борьбу с трансграничной преступной деятельностью и ее сдерживание. Для определения успешности проекта КОСМИК, его участники обсуждают основные индикаторы его реализации.

Участники: ДКУС разрабатывает КОСМИК совместно с Управлением по коммерческим вопросам полиции Сингапура и шестью крупнейшими банками, которые буду первыми участвовать в нем. ДКУС также тесно сотрудничает с Комиссией по защите личных данных для обеспечения соответствия обмена информацией в рамках этого проекта правилам Комиссии, касающимся использования личных данных.

Будучи органом по надзору в сфере ПОД, ДКУС объединит данные, имеющиеся на этой платформе, с данными, получаемыми им в ходе надзорной деятельности, и обеспечит надлежащее использование платформы КОСМИК ФУ. Бюро по работе с подозрительными операциями (ПФР Сингапура) получит непосредственный доступ к КОСМИК и сможет использовать информацию, получаемую с его помощью, для проведения анализа.

Порядок обмена информацией:

- В тех случаях, когда клиент демонстрирует поведение, характеризующееся наличием настораживающих признаков, и ФУ требуется дополнительная информация для того, чтобы понять, существуют ли причины подозревать клиента в осуществлении подозрительной деятельности, оно может **запросить** информацию о риске клиента у других ФУ, которые имеют отношение к этой деятельности.
- В тех случаях, когда необычная деятельность клиента превышает порог повышенного риска, свидетельствуя об увеличении риска осуществления им незаконной деятельности, ФУ должно в упреждающем порядке **направлять** информацию о риске клиента другим ФУ с описанием деятельности клиента.
- В тех случаях, когда деятельность клиента достигает высшего порога риска и ФУ направляет СПО информацию о его его деятельности, а также принимает решение прекратить с ним отношения, оно должно внести его в «Контрольный список» КОСМИК и поставить рядом с его именем отметку **«Внимание»**.
- На начальном этапе обмен информацией на платформе КОСМИК с помощью функций **«Запрос информации», «Предоставление информации»** и **«Внимание»** будет добровольным. ДКУС ожидает, что впоследствии обмен информацией с помощью функций **«Предоставление информации»** и **«Внимание»** станет обязательным. После окончания начального этапа ФУ-участники проекта обязаны будут отвечать на сообщения, направляемые с помощью функции **«Запрос информации»**.

Правовое основание для обработки личных данных: закон о защите личных данных (ЗЗЛД) предусматривает случаи, когда другие законы имеют преимущественную силу по отношению к нему. В этой связи, ДКУС вносит законодательные поправки в Закон о финансовых услугах и рынках, которые позволят создать нормативную основу для функционирования КОСМИК. После внесения таких поправок ФУ смогут обмениваться информацией о рисках для целей ПОД/ФТ/ФРОМУ. В частности, обмениваться информацией о рисках будет разрешено только тем ФУ, которые являются участниками КОСМИК, и только в пределах предусмотренных режимов обмена информации с помощью функций «Запрос информации», «Предоставление информации» и «Внимание».

Документ ДКУС, касающийся создающейся платформы по обмену информацией и нормативной базы, можно найти на: https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Consultation-Papers/1-Oct-2021-FI-FI-Information-Sharing-Platform-for-AMLCFT/Consultation-Paper-on-FI-FI-Information-Sharing-for-AMLCFT.pdf

Виды данных, которые собираются и которыми обмениваются: данные об анализе риска, информация об операциях и клиентах. Например, информация о клиентах может включать в себя данные о директорах, лицах, имеющих право подписи, или бенефициарных владельцах (такие, как их имена, дата регистрации или рождения, адрес проживания или юридический адрес, национальность или место регистрации и уникальный идентификационный номер). Может также происходить обмен информацией об операциях или наличии настораживающих признаков.

ФУ-участники проекта должны обмениваться информацией с помощью заранее разработанных шаблонов для обмена данными. Такой шаблон включает в себя следующую информацию:

- Идентификаторы дела и ФУ
- Выявленные настораживающие признаки и описание риска
- Данные о клиенте: имя или название, номер регистрации, дата регистрации, описание коммерческой деятельности, место регистрации и т.д.
- Характеристики счета: тип, статус и дата открытия/закрытия счета
- Данные об операции: названия или имена отправителя и получателя, номер счета, финансовые учреждения, дата, сумма и валюта
- Данные клиента, помещенного в список проблемных клиентов, и причины его включения туда.

Оценка соразмерности: на начальном этапе будет осуществляться обмен информацией, касающейся трех приоритетных областей риска, выявленных в ходе НОР и являющихся частью стратегии ПОД/ФТ/ФРОМУ. К ним относится использование юридических лиц в преступных целях, ОД с использованием торговли и ФРОМУ. Они представляют собой сложные формы финансовых преступлений, расследование которых требует обмена информацией. Для того, чтобы с помощью КОСМИК произошел обмен информацией, в поведении клиента или его данных должны быть обнаружены многочисленные настораживающие признаки или индикаторы достаточной серьезности, которые свидетельствуют о наличии опасений, касающихся совершения финансовых преступлений.

Другие соображения, касающиеся ЗДЛЖ: поскольку целью ФУ, участвующих в проекте КОСМИК, является оценка подозрений, касающихся клиентов, и предупреждение друг друга о лицах, которые, вероятно, являются подозрительными, информирование клиента об осуществлении ФУ обмена информацией может привести к тому, что злоумышленники поймут, что их незаконная деятельность попала под подозрение. С другой стороны, для защиты интересов клиентов, не нарушающих закон, в КОСМИК предусмотрено несколько уровней защитных мер, обеспечивающих соответствующий обмен, использование и защиту информации о клиентах.

Во-первых, перед началом обмена информацией о риске с помощью КОСМИК ФУ должно понять, показала ли предусмотренная проверка серьезность риска присутствия в деятельности клиента настораживающих признаков, доказывающих наличие риска. Такой порядок обеспечит обмен соответствующей информацией исключительно для целей ОД/ФТ/ФРОМУ в необходимом объеме. Это позволит ФУ определить наличие разумно обоснованных оснований для того, чтобы подозревать клиента в осуществлении незаконной деятельности или предупредить другие ФУ, что клиент, вероятно, осуществляет незаконную деятельность. ФУ, отвечающее на запрос о предоставлении информации о риске другого ФУ, перед направлением такой информации также должно будет осуществить оценку и быть уверенным в том, что запрашиваемая информация может помочь оценить и выявить проблемы, касающиеся риска ОД/ФТ/ФРОМУ.

Помимо этого, документ, регулирующий функционирование КОСМИК, будет предусматривать защитные меры, касающиеся использования и обеспечения конфиденциальности информации, получаемой с помощью этой платформы; он будет требовать от ФУ предпринимать меры в отношении ненадлежащего обмена информацией с помощью платформы. Кроме этого, в нем будут предусмотрены требования, касающиеся обеспечения того, чтобы информация, предоставляемая с помощью платформы, была точной и полной, и своевременного извещения ДКУС и других ФУ-участников проекта о неточностях предоставляемой информации и скорейшем исправлении таких неточностей.

Наконец, от ФУ также будет требоваться использовать процедуру, позволяющую анализировать отношения с клиентом, в т.ч. предоставлять клиенту возможность разъяснить вопросы, возникающие у ФУ, до прекращения существующих отношений. Перед принятием решения о прекращении отношений с клиентом ФУ не следует полагаться исключительно на информацию, получаемую с помощью КОСМИК, а анализировать всю картину отношений с ним, используя информацию из других источников, в т.ч. объяснения клиента. У клиентов уже имеются предусмотренные законом способы исправления информации о себе, которую ФУ получают от них, например, личной информации; клиент может использовать такие способы при взаимодействии с банком для внесения измененной информации в КОСМИК.

Передача и раскрытие данных: ФУ и их сотрудникам будет запрещено раскрывать информацию, получаемую с помощью КОСМИК, каким-либо иным лицам, за исключением случаев, предусмотренных в законодательстве. Любое дальнейшее раскрытие информации платформы КОСМИК должно осуществляться в строгом соответствии с принципом, предусматривающим, что предоставляемая информация будет соответствующей, достаточной и необходимой для целей оценки риска ОД/ФТ/ФРОМУ. Например, ФУ может понадобиться раскрыть информацию, получаемую с помощью платформы, в рамках осуществления своей деятельности для выполнения обязанностей по управлению риском ОД/ФТ/ФРОМУ или привлечения сторонних организаций для управления таким риском. Кроме этого, ФУ может потребоваться раскрыть такую информацию местным и заграничным дочерним компаниям для управления риском ОД/ФТ/ФРОМУ на уровне финансовой группы, для повышения эффективности и снижения такого риска в масштабе всей финансовой группы и для предотвращения перемещения недобросовестных клиентов из одного подразделения финансовой группы в другое ее подразделение. ФУ, раскрывающее информацию, полученную с помощью такой платформы, установленному кругу лиц для таких целей, должны будут применять дополнительные защитные меры для уменьшения рисков ее утечки и несанкционированного раскрытия, а также неумышленного правового риска, возникающего у финансовых учреждений, которые обменялись такой информацией.

Конфиденциальность и защита данных от несанкционированного использования: для предотвращения утечки данных ФУ-участники проекта должны надлежащим образом классифицировать данные, получаемые с помощью платформы КОСМИК, и применять меры по их защите от несанкционированного использования. Они, как минимум, должны обеспечить соблюдение требования ДКУС, касающиеся хранения и защиты данных, которые содержатся в следующих документах:

- Правила управления технологическими рисками, в которых описываются передовые практики, используемые в этом секторе, которые ФУ, по мнению ДКУС, должны применять

- Информационные сообщения об управлении технологическими рисками и кибербезопасности, в которых содержатся требования, предъявляемые к ФУ относительно применения необходимых мер контроля в области ИТ и мер по обеспечению кибербезопасности.

Данные, имеющие отношение к КОСМИК, должны храниться в безопасном месте и быть зашифрованы. Они не должны храниться в компьютерах сотрудников, кроме как в исключительных случаях. Просмотр, редактирование или скачивание конфиденциальной информации должно фиксироваться в контрольных журналах.

Используемые технологии: информация должна предоставляться в структурированном виде с помощью онлайн-платформы, которая снабжена такими элементами защиты данных от несанкционированного использования, как система аутентификация пользователей и шифрование данных, а также разрешение сущности и анализ сетей. Кроме этого, ДКУС будет использовать информацию, имеющую отношение к КОСМИК, в рамках своей более широкой системы анализа ПОД/ФТ/ФРОМУ для выявления незаконных сетей и возникающих тенденций.

Дополнительные факторы, которые нужно принять во внимание, и проблемы: ДКУС осознает, что расширение сотрудничества между банками-участниками проекта может привести к увеличению риска того, что злоумышленники перенесут свою деятельность в те ФУ, которые не являются участникам проекта КОСМИК. Для уменьшения этого риска ДКУС расширяет контроль, направленный на обнаружение таких ситуаций «миграции риска» и расширяет взаимодействие в области надзора с теми ФУ, которые не являются участниками проекта КОСМИК. Все это позволит предупредить их о таких случаях и снабдить их методическими рекомендациями для усиления мер контроля в области ПОД/ФТ/ФРОМУ. ДКУС и ПФР Сингапура также продолжат сотрудничать с ФУ при проведении важных расследований, касающихся ОД/ФТ, в рамках Секторального партнерства в области ПОД/ФТ/ФРОМУ, и будут привлекать ФУ, не являющиеся участниками проекта КОСМИК, к участию в таких расследованиях в необходимых случаях.

Источник: Обсуждения с участниками проекта КОСМИК и полученная от них информация, «Использование ДКУС и финансовыми учреждениями новой цифровой платформы для борьбы с отмыванием денег» (октябрь 2021 г.), выложено на: https://www.mas.gov.sg/news/media-releases/2021/mas-and-financial-industry-to-use-new-digital-platform-to-fight-money-laundering

Примечание:

1. Первыми тремя приоритетными областями риска являются использование юридических лиц в преступных целях, ОД с помощью торговли и ФРОМУ.

Вставка 4.3. Мониторинг операций Нидерланды (МОН): Проект по обмену информацией между субъектами частного сектора до возникновения подозрений

Описание: Мониторинг операций Нидерланды (МОН) является проектом, осуществляемым пятью нидерландскими банками, задачей которого является обеспечение более быстрого, более качественного и более эффективного мониторинга операций и усиление роли банков в качестве лиц, контролирующих доступ к финансовой системе. Долгосрочной целью этого проекта является создание средства мониторинга операций, которым могли бы пользоваться все ФУ и который обеспечивает выявление финансовыми учреждениями большего количества случаев ОД и ФТ и направление правоохранительным органам более ценной информации.

После своего запуска в июле 2020 г., МОН в настоящее время функционирует в качестве продукта «Минимальной функциональности». Его задачей на этом этапе является увеличение количества случаев выявления ОД путем выявления необычных операций, которые один банк не в состоянии выявить в одиночку (так называемые «предупреждения нескольких банков»). На этой стадии:

- Вся деятельность в рамках МОН осуществляется в дополнение к обычным мерам по ПОД/ФТ, принимаемыми банками-участниками этого проекта;
- особое внимание уделяется осуществляемому несколькими банками мониторингу и выявлению финансовых преступлений, совершаемых с помощью счетов, которые открыты в нескольких банках;
- МОН на стадии продукта «Минимальной функциональности» является только средством выявления; анализ настораживающих признаков и меры, принимаемые в отношении клиентов (в т.ч. направление сообщений о необычных операциях в ПФР) осуществляются банками;
- его действие распространяется только на юридических лиц;
- конфиденциальные данные, касающиеся личной жизни, псевдонимизируются.

Основной рабочий процесс МОН заключается в том, что банки передают туда псевдонимизированные данные об операциях. С помощью современных моделей анализа, предусмотренных в МОН специально для осуществления мониторинга операций несколькими банками, генерируются предупреждения о моделях осуществления операций, которые, возможно, являются необычными. МОН направляет банкам для анализа предупреждения об отдельных субъектах, которые являются частью такой необычной схемы (или «дела»), которая, возможно, является необычной. Поскольку информация о клиентах, позволяющая проанализировать предупреждение, имеется только у банков, в настоящее время анализ предупреждений осуществляется ими.

Планируемые или достигнутые результаты: в настоящее время задача этой системы заключается в выявлении денежных потоков и моделей, которые, возможно, являются незаконными; такие потоки и модели имеют отношение к нескольким банкам и не могут быть выявлены (с помощью имеющихся средств) соответствующим банком в одиночку, поскольку он видит только один элемент всего явления. Создание такой системы основано на предположении о том, что организации, занимающиеся ОД, все чаще намеренно создают сложные схемы, позволяющие им скры-

вать происхождение денежных средств и места, куда они направляются, с помощью нескольких банков и банковских счетов. Тестирование на этапе «Апробация концепции» и первые результаты, полученные с помощью первых предупреждений, созданных несколькими современными моделями анализа, существующими в МОН, позволили выявить множество таких дел, определенная часть которых привела к направлению СПО в ПФР.

Участники: МОН является программой, осуществляемой пятью нидерландскими банками: ABN Amro, ING Bank, Radobank, Tridos Bank и De Volksbank. Все они являются акционерами юридического лица МОН, который формально является полностью частной инициативой. На практике, эти нидерландские банки тесно сотрудничают с государственными органами для достижения консенсусных договоренностей, касающихся некоторых стратегических вопросов и вопросов регулирования. Кроме этого, было достигнуто соглашение с правоохранительными органами относительно оперативной информации и типологий, касающихся ОД, которые могут использоваться в моделях анализа, задачей которых является выявление «мультибанковских» необычных операций.

Способ обмена информацией: банки готовят данные об операциях для обмена самостоятельно; в рамках такой подготовки осуществляется псевдонимизация всех данных, которые могут быть прямо или косвенно связаны с отдельными субъектами (см. также ниже). МОН группирует и передает данные, направляемые банками-участниками, в модели анализа, расположенные на надежно защищенной IT-платформе. В предупреждениях, направляемых обратно в банки, содержатся идентификаторы, которые могут быть соотнесены с данными о своих клиентах только банком, получившим такое предупреждение. Этот процесс должен быть осуществлен банком до того, как его сотрудники приступят к изучению предупреждения, полученного от МОН.

Виды данных, которые собираются и которыми обмениваются: в настоящее время в МОН направляются только данные о юридических лицах; они ограничены тем, что требуется для достижения целей МОН и возможно в рамках действующего законодательства. Такие данные включают в себя информацию об операции (номер счета, тип и сумма операции) и ограниченную информацию о счете и клиенте (идентификационные номера, тип счета и клиента, сектор, в котором клиент осуществляет деятельность). В связи с применяемой в настоящее время псевдонимизацией (см. ниже) МОН не может идентифицировать личности отдельных клиентов в данных, направляемых банками. В этой связи, МОН может только предупреждать банки о моделях операций, осуществляемых с помощью нескольких банков, которые он выявляет.

Использование технологий, усиливающих конфиденциальность, или других технологий: хотя в настоящее время действие этой системы распространяется только на юридические лица, для сохранения конфиденциальности обрабатываемых данных применяются соответствующие меры. Деятельность банков и функционирование МОН основывается на предположении о том, что некоторые данные могут являться личными данными, и поэтому МОН воспринимает все данные как личные данные. Основным методом является псевдонимизация, с помощью которой все элементы данных, которые могут иметь отношение к отдельным клиентам (информация, позволяющая идентифицировать клиента, номера счетов, названия),

преобразуются в хешированные значения. Для процесса хеширования используется набор закрытых ключей, которые во время подготовки данных хранятся третьим лицом в защищенных модулях. Поскольку эти секретные ключи являются общими для всех банков, МОН способна устанавливать связи между данными об операциях на основании элементов псевдонимизированных данных, которые также являются общими для всех банков (например, номер, присвоенный клиенту торговой палатой или номер счета клиента). Поэтому, хотя МОН не располагает данными о личности клиента и информацией о нем, она все равно может анализировать операции, совершаемые банками.

Правовое основание обработки личных данных: для того чтобы у МОН появилась возможность осуществлять в полном объеме мониторинг операций, совершаемых несколькими банками, Министерства финансов и юстиции разрабатывают поправку в Закон Нидерландов о ПОД/ФТ. Внесение этой поправки является частью Национального плана действий по борьбе с ОД правительства Нидерландов. Помимо прочего, внесение этой поправки позволит нидерландским банкам обмениваться большим количеством данных и информации об операциях, которые, вероятно, являются необычными, отменит запрет на привлечение сторонних лиц к мониторингу операций и разрешит использовать номер гражданской службы (уникальный индивидуальный идентификационный номер) для коллективного мониторинга операций. Пока эта поправка не принята, в МОН на основании «законного интереса» поступают данные об ограниченном количестве клиентов. В рамках разработки этой системы был осуществлен всесторонний юридический анализ для того, чтобы понять, какие виды обработки данных соответствуют существующей правовой системе и как такая обработка должна осуществляться.

Факторы, касающееся ЗДЛЖ, которые необходимо принять во внимание: в рамках осуществления подхода под названием «встроенное обеспечение конфиденциальности» банки (как операторы персональных данных) и МОН (лицо, обрабатывающее персональные данные) проводят Оценку влияния на защиту данных («ОВЗД»), позволяющую оценить соблюдение основных принципов ОРЗД. В пользовательском соглашении, заключенном между банками и МОН, также предусмотрены важные меры по обеспечению конфиденциальности данных и их защите от несанкционированного использования. Более того, отдельно приняты в соответствие с надлежащими документами и оформлены меры по обеспечению конфиденциальности данных, используемых в каждой модели анализа.

ОВЗД и связанные с нею меры по обеспечению конфиденциальности основываются на законном интересе банков – участников программы, выступающих в качестве операторов персональных данных; такой интерес позволяет усилить их роль в качестве лиц, контролирующих доступ к финансовой системе, и за счет того, что они выступают в такой роли, более эффективно соблюдать требования в области ПОД/ФТ. С опорой на требования в области ПОД были выявлены, сформулированы и согласованы необходимость обработки данных для достижения задачи по повышению эффективности межбанковского выявления необычных операций, вопросы, также предусмотренные в упомянутом выше Национальном плане по борьбе с ОД, подтверждения того, что МОН (после тестирования) способна повысить эффективность ПОД банков-участников, и соображения, касающиеся соразмерности обработки данных. Чрезвычайно важным для таких факторов также является соблюдение принципов ограничения целей использования данных и сведения к минимуму объема используемых данных.

Во время функционирования МОН для обеспечения точности обработки данных и их защиты от несанкционированного использования применяется широкий спектр соответствующих мер. Для оценки пригодности использования элементов данных в моделях анализа банки и МОН осуществляют анализ качества данных и исправляют их неточности. Сами данные не могут быть переданы с ИТ-платформы МОН какой-либо другой (внешней) стороне. На ИТ-платформу МОН распространяется действие самых строгих стандартов в области информационной безопасности, в т.ч. осуществляется оценка, непрерывный мониторинг и проверка мер безопасности. Функционирование моделей анализа регулируется системой моделей риска, которая обеспечивает их правильную, надежную, объективную и транспарентную работу.

Дополнительные соображения и проблемы: МОН является новаторской инициативой, в ходе ее реализации стало ясно, что существующая правовая система обеспечивает возможности обмена данных, но также содержит в себе серьезные ограничения и является источником проблем. В настоящее время в МОН используется модель, которая способна функционировать в рамках этих ограничений и при наличии таких проблем, но которая не позволяет обеспечить эффективность ПОД в полном объеме. Для того чтобы она заработала в полную силу, необходимо устранить ограничения и проблемы, связанные с противоречиями между ПОД и законодательством о неприкосновенности частной жизни. Для того, чтобы такие системы, как МОН, успешно функционировали и обеспечивали эффективность борьбы с финансовыми преступлениями, необходима большая правовая ясность и определенность в области обмена данными, а также устранение противоречий между законодательством в области ПОД и законодательством о неприкосновенности частной жизни. Принятие международных правовых документов, которые обеспечат большую ясность относительно целей использования и областей применения таких систем, помогло бы представителям государственных органов и коммерческих учреждений активнее внедрять инновации и осуществлять сотрудничество, а также перейти на новый уровень деятельности по повышению эффективности регулирования банками доступа к финансовой системе и их противодействия отмыванию денег. В практическом плане, если бы в стандартах по ПОД было бы четче оговорено, какой информацией можно или следует обмениваться как для выявления ОД, так и для осуществления анализа, это позволило бы осуществлять более тщательный анализ, достигая более эффективных результатов, а также уменьшить объем обрабатываемых данных и нагрузку на клиентов с низким уровнем риска.

Участие органов власти (как отвечающих за ПОД/ФТ/ФРОМУ, так и отвечающих за ЗДЛЖ): для того, чтобы МОН мог функционировать, указанные выше банки интенсивно взаимодействуют с рядом государственных органов. В настоящее время органы власти разрабатывают законодательные положения, которые обеспечат дальнейшее развитие этого проекта.

Источник: Обсуждения с участниками проекта МОН и предоставленная ими информация: «Что такое МОН?» (2022 г.), документ выложен на: https://tmnl.nl/summary-eng/

Вставка 4.4. Система предупреждения о происшествиях (СПП) финансовых учреждений (Нидерланды): Обмен информацией, касающейся мошенничеств, после возникновения подозрений

Описание: обмен идентифицирующей информацией о лицах, осуществляющих мошенничества, после возникновения подозрений с использованием системы первоначального совпадения или отсутствия совпадения для выявления возможных рисков клиента.

Запланированные или достигнутые результаты: СПП начала использоваться в 1997 г., она позволяет участвующим в ней ФУ помогать друг другу выявлять и предотвращать мошенничества. Эта система дает возможность ФУ предупреждать друг друга о клиентах, сотрудниках или других лицах, участвующих в мошенничествах, и помогает проводить расследования возможных мошенничеств. Начиная с 1990 г. отделы безопасности ФУ фиксируют случаи мошенничеств во внутреннем реестре происшествий. Начиная с 1997 г., с помощью СПП некоторые элементы реестров внутренних происшествий включаются во внешний реестр, доступ к которому имеют другие банки-участники СПП для выявления наличия или отсутствия совпадений.

Участники: доступ к СПП могут получить все ФУ, которые являются членами общепризнанных профессиональных ассоциаций (например, Банковской ассоциации Нидерландов, Ассоциации страховых компаний, Ассоциации финансовых компаний Нидерландов, Фонда по недопущению мошенничеств с ипотечными кредитами или Ассоциации компаний по страхованию здоровья Нидерландов). Банки, которые не являются членами Банковской ассоциации Нидерландов, или страховые компании, которые не являются членами Ассоциации страховых компаний, могут быть допущены к участию в системе в порядке исключения.

Каждое ФУ-участник системы остается оператором персональных данных. Управление данными, направляемые в СПП другими ФУ, осуществляет Бюро регистрации кредитов (БРК), а управление данными, направляемыми в СПП страховыми компаниями, осуществляется Фондом центральной информационной системы (ФЦИС). Эти организации управляют вешним реестром и выступают в качестве лиц, обрабатывающих персональные данные.

Руководящий комитет (в его состав входят представители нескольких учреждений-участников) контролирует функционирование реестра и обеспечивает единообразное применение и соблюдение правил.

Способ обмена информацией: обмен данными осуществляется с помощью внешнего реестра, в который ФУ заносят данные о клиентах, сотрудниках или лицах, замешанных в мошенничестве.

Информация вносится во внешний реестр только в тех случаях, когда:

- Лицо, замешанное в мошенничестве, нарушило или пыталось нарушить какой-либо закон, что создало угрозу интересам клиентов или сотрудников ФУ, самому ФУ или финансовому сектору в целом;
- Существуют разумно обоснованные причины полагать, что выявленное лицо совершило такое деяние, которое повлекло или повлечет за собой составление

уголовного иска или заявления (или повлекло бы за собой такое составление, если бы соответствующее деяние было бы соразмерно преступлению или имело бы нежелательные последствия для обеспечения законности);

- При соблюдении принципа соразмерности.

СПП позволяет ФУ-участникам системы искать информацию во внешнем реестре на наличие или отсутствие совпадений, это позволяет ФУ, ищущему информацию, получать данные о мошенничествах с участием разыскиваемого лица. СПП также предоставляет возможность обнаруживать совпадения в прошлом: в тех случаях, когда направление запроса приводит к обнаружению совпадения за последние два месяца, ФУ, ищущее информацию, направляется к новой записи. В случае обнаружения совпадения ФУ может направить запрос о предоставлении дополнительных данных, чтобы понять, по какой причине данные о клиенте были внесены в реестр. ФУ, получившее запрос, рассматривает его в индивидуальном порядке. Любой обмен данными должен быть соразмерным, сообразным и ограниченным данными, необходимыми для использования в целях обмена ими.

Виды данных, которые собирают и которыми обмениваются: во внешнем реестре содержатся идентификационные данные лиц, причастных к мошенничествам, например, имя, адрес, дата рождения, гражданство, международный номер банковского счета. При этом во время первоначального обращения к СПП осуществляется поиск совпадений; это значит, что во время первоначального обращения идентификационные данные не предоставляются. В связи с этим, в случае выявления совпадения отдел безопасности соответствующего ФУ должен понять, следует ли обращаться за получением дополнительной информации, принимая во внимания требования, касающиеся ЗДЛЖ.

Правовое основание обработки личных данных: обмен данными с помощью СПП разрешается осуществлять на основании ОРЗД в связи с наличием «законного интереса», связанного с выявлением и недопущением мошенничества (пункт 6(1)(f)). Общий закон Нидерландов о защите данных («Закон») требует, чтобы лицо, обрабатывающее личные данные, имело соответствующее свидетельство. СПП прошла сертификацию, что потребовало оценки соблюдения ею требований ЗДЛЖ органом, отвечающего за защиту данных.

Оценка соразмерности: обмен данных с помощью СПП ограничивается узкой группой ФУ. На начальном этапе обмен информацией касается только найденных совпадений. Дополнительная информация предоставляется только в случае необходимости; отдел безопасности ФУ, получившего соответствующий запрос, рассматривает возможность предоставления информации в каждом случае индивидуально, анализируя, является ли ее предоставление соразмерным. ФУ-участники системы обязаны удалять данные из реестра после того, как они теряют актуальность (например, в тех случаях, когда их наличие в реестре больше не требуется для предотвращения мошенничества) или по истечении 8 лет.

Другие факторы ЗДЛЖ, которые необходимо учитывать:

- **Качество, а также непротиворечивость и точность:** ФУ-участники системы должны в случае необходимости исправлять, удалять или дополнять данные, хранящиеся во внешнем реестре, для обеспечения их точности. Вся информация, вносимая в реестр, должна быть доступна для отслеживания и документироваться.

- **Прозрачность и информирование:** субъект данных должен информироваться о включении таких данных в реестр, если только такое информирование не наносит ущерба предотвращению, выявлению и судебному преследованию уголовного преступлению или защите субъекта данных.
- **Справедливость решений, принимаемых с помощью автоматической обработки:** Хотя запросы во внешний реестр могут направляться в автоматическом режиме, каждое совпадение должно проверяться обоими участниками (т.е. ФУ, ищущим информацию, и ФУ, внесшим ее) для обеспечения того, что оно не является ложным. Кроме этого, любой последующий запрос о предоставлении информации после выявления совпадения должен рассматриваться в ручном режиме сотрудниками отделов безопасности как ФУ, направившего запрос, так и ФУ, получившего его.
- **Права субъекта данных на получение доступа к данным и их исправление:** субъект данных имеет право проверять, исправлять, удалять данные, находящиеся в реестре, и возражать против их нахождения там. В большинстве случаев ответы на обращения субъектов данных направляются в течение месяца с указанием всех обоснований. В тех случаях, когда такие ответы или доступ не могут быть предоставлены, например, если это необходимо для предотвращения или выявления уголовного преступления либо судебного преследования за него, должно быть принято и зафиксировано внутреннее решение.
- **Права субъекта данных на восстановление своих прав:** в случае возникновения разногласия относительно правильности данных в реестре или законности их нахождения в нем субъект данных может обратиться в совет директоров или к руководству соответствующего ФУ, а если проблема не будет решена, может обратиться за помощью к сторонней организаций, например, в Институт рассмотрения жалоб на предоставление финансовых услуг, орган, отвечающий за ЗДЛЖ, или суд надлежащей юрисдикции.
- **Передача или раскрытие данных:** данные, находящиеся в реестре, могут обрабатываться только в конкретных целях для предотвращения и выявления мошенничеств в соответствии с протоколом функционирования СПП. ФУ-участники системы обязуются обеспечить, чтобы данные не могли дополнительно обрабатываться или использоваться каким-либо дополнительным способом или каким-либо образом, который несовместим с целью обработки.
- **Обеспечение конфиденциальности данных и их защита от несанкционированного использования:** направлять запросы в реестр СПП могут только специально уполномоченные сотрудники ФУ. Каждый такой сотрудник обязан соблюдать конфиденциальность данных. После направления запроса (выявление или невыявление совпадения) любой обмен идентифицирующей информацией осуществляется исключительно между сотрудниками отделов безопасности соответствующих ФУ. Каждое ФУ-участник системы обязуется обеспечивать защиту данных от несанкционированного использования и анализировать соответствующие меры безопасности каждые два года. Кроме этого, ФУ должны внедрить процедуру по борьбе с утечкой данных, которая соответствует ОРЗД.

Дополнительные факторы, которые необходимо учесть, и проблемы:

- **Предоставление доступа к финансовым услугам:** включение во внутренний реестр происшествий ФУ может привести к принятию решения не предоставлять финансовые услуги соответствующему лицу или прекратить существующие отношения с ним. Органы власти также болезненно реагируют на возможность того, что включение во внешний реестр может привести к принятию такого же решения. Для предотвращения ситуации, когда кто-либо оказывается не в состоянии получить финансовые услуги, ФУ приняли на себя обязательство продолжать оказывать финансовые услуги, касающиеся основных потребностей такого человека (например, открывать основные банковские счета или предоставлять основное страхование). Кроме этого, при принятии решения об оказании услуг какому-либо клиенту, ФУ могут принимать во внимание информацию из СПП только после получения рекомендаций от сотрудников своего отдела безопасности (который управляет обменом данными). ФУ не имеют права действовать исключительно на основании наличия совпадения без проверки причины включения соответствующей информации в реестр.

Участие органов власти (отвечающих за ПОД/ФТ/ФРОМУ или за ЗДЛЖ:): орган, отвечающий за ЗДЛЖ, проверил этот проект на соответствие требованиям в области ЗДЛЖ и одобрил его. В 2021 г. было обновлено свидетельство, разрешающее функционирование этой системы. ФУ-участники системы обязаны пересматривать протокол деятельности каждые два года, принимая во внимание соответствующие изменения, внесенные в документы, регулирующие ЗДЛЖ и законодательство. Если такой пересмотр требует внесения изменений и дополнений в протокол, необходимо обратиться в орган, отвечающий за защиту данных, за получением нового разрешения на осуществление деятельности.

Примечание: В этом примере используется исключительно имеющаяся общедоступная информация. Она не была получена в результате деятельности целевой группы с участием заинтересованных сторон.

Источник: Протокол системы предупреждений о происшествиях (2021 г.), с документом можно ознакомится на: https://www.verzekeraars.nl/media/9002/protocol-incidentenwaarschuwingssysteem-financiele-instellingen-pifi-2021-eng_.pdf

Вставка 4.5. Пункт 314(b) (США): Обмен информацией между субъектами частного сектора до и после возникновения подозрений для выявления деятельности, связанной с ОД/ФТ, и направления сообщений о ней

Описание: правовые рамки, обеспечивающие обмен информацией между ФУ в «зоне безопасности», которая предоставляет защиту от ответственности, для более эффективного выявления деятельности, которая может быть связана с ОД или ФТ, и направления сообщений о ней.

Запланированные или достигнуты результаты: пункт 314(b) Закона об объединении и укреплении США путем обеспечения соответствующих мер, направленных на пресечение и предупреждение терроризма (Закон о борьбе с терроризмом США «Патриот») позволяет ФУ обмениваться информацией для более эффективного выявления возможных ОД и ФТ и направления сообщений о них. В частности, обмен информацией, предусмотренный в пункте 314(b), позволяет ФУ:

- собирать дополнительную информацию о клиентах или операциях, которые, возможно, имеют отношение к ОД/ФТ, в т.ч. ранее неизвестных счетах, деятельности и (или) связанных с ними физических или юридических лицах;
- получать более четкое представление об общих финансовых следах, особенно если они являются сложными и, по всей видимости, оставлены в многочисленных ФУ, юридических лицах и юрисдикциях;
- получать более полную и точную картину о деятельности клиента, которая может быть связана с ОД/ФТ, что позволяет принимать более выверенные решения, касающиеся надлежащей проверки и мониторинга операций;
- предупреждать другие ФУ-участников этой программы о клиенте, о подозрительной деятельности которого они, возможно, ранее не знали;
- направлять более полные отчеты о подозрительной деятельности, что было бы невозможно без обмена информацией, предусмотренного в пункте 314(b);
- выявлять и способствовать выявлению методов и схем ОД/ФТ;
- принимать правильные решения, касающиеся направления СПО, например, в тех случаях, когда ФУ получает более полную картину деятельности в ходе процесса добровольного обмена информацией и принимает решение об отсутствии необходимости в направлении СПД по операциям, которые изначально, возможно, казались подозрительными.

Данные, полученные ФинСЕН с 2017 по 2019 гг., показывают, что в среднем в 15 900 сообщениях о подозрительной деятельности в год говорится об обмене информацией в соответствии с пунктом 314(b). Учреждения, направляющие сообщения, в которых упоминается пункт 314(b), либо направляли запрос в другое учреждение в соответствии с этим пунктом для оказания поддержки в сборе информации о подозрительной деятельности или получали запрос в соответствии с пунктом 314 (b), который побуждал его проводить свое собственное расследование и направлять сообщение о подозрительной деятельности. Анализируя данные за 2017-2019 гг., мы можем видеть тенденцию к увеличению количества учреждений, упоминающих в своих сообщениях об обмене информацией на основании пункта 314 (b).

Участники: участие в обмене информацией на основании пункта 314(b) является добровольным, в нем могут принимать участие все ФУ при условии соблюдения требования программы ПОД, которое предусмотрено в регламенте деятельности ФинСЕН, и любая ассоциация таких ФУ. Лица, желающие осуществлять обмен информацией в соответствии с пунктом 314(b), должны быть зарегистрированы ФинСЕН. По состоянию на конец 2019 г. в таком обмене участвовало свыше 7 000 организаций. Подавляющее большинство таких участников составляют банки и кредитные союзы, но в нем также участвует ряд представителей других секторов, в т.ч. казино, компании по работе с ценными бумагами, страховые компании и организации, предоставляющие услуги по работе с денежными средствами. Деятельность всех учреждений участников этой системы регулируется нормативными актами, которые обеспечивают «зону безопасности», позволяющую обмениваться информацией, и требуют наличия соответствующих мер контроля, которые время от времени проверяются надзорными органами.

Способ обмена информацией: пункт 314(b) позволяет осуществлять обмен информацией между субъектами частного сектора при условии наличия предусмотренных мер контроля, касающихся использования информации и ее защиты от несанкционированного использования. Обмен информацией может осуществляться по принципу «один одному» или «один многим» между учреждениями, зарегистрированными ФинСЕН, на основании пункта 314(b) в письменной или устной форме либо с использованием имеющихся технологий. Любое учреждение, обменивающееся информацией на основании пункта 314(b), должно располагать соответствующими процедурами по защите конфиденциальности и защите от несанкционированного использования всей информации, обмен которой происходит в соответствии с пунктом 314(b) и другими законами, подзаконными актами и правилами.

Виды данных, которые собираются и которыми обмениваются: ФУ-участники могут обмениваться информацией, касающейся физических лиц, юридических лиц, учреждений и стран для выявления и, если применимо, направления сообщений о деятельности, которая может быть связана с террористической деятельностью или ОД. Пункт 314(b) и подзаконные акы, обеспечивающие его выполнение не налагают каких-либо ограничений на обмен информацией, позволяющей установить личность, если такой обмен в иных отношениях соответствует требованиям пункта 314(b) и подзаконных актов, обеспечивающих его выполнение. Этот пункт также не ограничивает тип или носитель информации, которым можно надежно обмениваться, например, данными видеонаблюдения или данными, относящимися к Интернету, например IP-адресами, а также устной или письменной информацией. При этом пункт 314(b) не разрешает ФУ-участникам программы обмениваться самими сообщениями о подозрительной деятельности или раскрывать информацию, которая указала бы на направление такого сообщения (при этом учреждения, обменивающиеся информацией, могут направлять совместные сообщения).

Правовое основание обработки личных данных: пункт 314(b) содержит правовое основание обмена информацией. Обмен в соответствии с этим пунктом защищен «зоной безопасности», которая обеспечивает защиту от ответственности за обмен информацией в соответствии с пунктом 314(b) и подзаконными актами, обеспечивающими его выполнение. Обмен информацией в соответствии с пунктом 314(b) является обоснованным в тех случаях, когда ФУ или ассоциация ФУ имеет разумно обоснованное основание полагать, что информация, обмен которой происходит, имеет

отношение к деятельности, которая может касаться ОД или ФТ, и что обмен информацией происходит в соответствии с одной из целей, предусмотренных в пункте 314(b) и подзаконных актах, обеспечивающих его выполнение.

Оценка соразмерности: для обмена информацией в соответствии с пунктом 314(b) учреждение, обменивающееся информацией, должно иметь разумно обоснованное основание полагать, что определенная информация имеет отношение к деятельности (например, мошенническим операциям или действиям в Интернете), которая, в конечном счете, может иметь отношение к ОД/ФТ. Пункт 314(b) косвенным образом показывает, что обмен информацией в рамках пункта 314(b) является обоснованным для достижения целей обмена информацией, т.е. обмен информацией является соразмерным целям обмена – выявлению деятельности, которая может, в конечном счете, быть связана с ОД/ФТ, и защите общества от финансовых преступлений и терроризма.

Другие факторы ЗДЛЖ, которые необходимо учитывать:

- **Передача или раскрытие данных:** данные, которыми обмениваются в соответствии с пунктом 314(b), могут использоваться только для целей, предусмотренных в этом пункте и подзаконных актах, обеспечивающих его выполнение, т.е. для выявления деятельности, которая может быть связана с ОД/ФТ, и, при необходимости, направления сообщений о ней; принятия решений об открытии или ведении счета либо осуществлении операции, а также для содействия соблюдению требований в области ПОД.
- **Качество и полнота данных:** ФУ, действующие на основании пункта 314(b), могут повышать точность и полноту своей информации, в т.ч. информации, которая должна направляться в ФинСЕН в составе сообщений о подозрительной деятельности.
- **Справедливость решений, принимаемых с помощью автоматической обработки:** ФУ, действующие на основании пункта 314(b), участвуют в обмене информацией, который контролируется людьми, в частности, для улучшения качества и полноты имеющейся у них информации, в т.ч. информации, которая должна направляться в ФинСЕН, будучи частью сообщений о подозрительной деятельности, что помогает обеспечивать справедливость по отношению к лицам, имеющим отношение к такой деятельности.
- **Обеспечение конфиденциальности данных и их защита от несанкционированного использования:** ФУ должны внедрить и применять соответствующие процедуры для обеспечения конфиденциальности и защиты от несанкционированного использований всей информации, обмен которой осуществляется на основании пункта 314(b). К таким процедурам относится назначение контактного лица для получения и направления информации. До начала обмена информацией ФУ должны принять разумно обоснованные меры для обоснования того, что учреждение, получающее информацию, имеет право участвовать в обмене информацией в соответствии с пунктом 314(b). ФинСЕН предоставляет доступ к списку участников, который зарегистрированные ФУ и ассоциации могут использовать для этой цели.

Участие органов власти (отвечающих за ПОД/ФТ/ФРОМУ или ЗДЛЖ): ФУ, которые хотят использовать пункт 314(b) для обмена информацией, обязаны зарегистри-

роваться в ФинСЕН и ежегодно продлевать свою регистрацию. Государственные органы, в т.ч. ФинСЕН, не участвуют в обмене информацией на основании пункта 314(b) и не имеют к ней доступа за исключением случаев, когда она содержится в сообщениях о подозрительной деятельности.

Источник: Обсуждения с участниками обмена информацией в соответствии с пунктом 314(b) и полученная от них информация, Казначейство США, пункт 314(b) Информационного бюллетеня, с документом можно ознакомиться по ссылке: http://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf; Казначейство США, Информация об обмене информацией; Осуществление обмена информацией на основании пункта 314(b) и направление сообщений с использованием такой информации, с документом можно ознакомиться по ссылке: http://www.fincen.gov/sites/default/files/shared/314bparticipationinfo.pdf

Вставка 4.6. Система «Мост для ПОД» (Эстония): Инициатива по обмену информацией между субъектами частного бизнеса после возникновения подозрений

Описание: система «Мост для ПОД» представляет собой защищенную цифровую платформу, разработанную независимой сторонней организацией. Она позволяет использующим ее банкам обмениваться псевдонимизированными данными (главным образом, данными об операциях) с одним или несколькими банками с помощью сквозного шифрования. Обмен информацией осуществляется практически в режиме реального времени, что позволяет проводить совместные расследования.

Запланированные или достигнутые результаты:

- С июля 2021 по март 2022 г. с помощью системы «Мост для ПОД» удалось провести 1 200 расследований, осуществленных субъектами частного бизнеса совместно (примерно 150 дел в месяц).
- Половина этих дел (свыше 600) касалась расследований ОД; такие расследования позволили повысить качество направленных СПО, в т.ч. за счет направления совместных СПО. Расследования этих дел также помогли быстрее снять подозрения с клиентов, деятельность которых изначально казалась подозрительной (т.е. уменьшило количество ложноположительных случаев).
- Треть этих дел (свыше 400) имеет отношение к мошенничествам, которые обычно связаны с выманиванием денег у людей. С помощью этой системы у преступников было конфисковано и возвращено пострадавшим примерно 3 млн евро. При расследовании мошенничеств очень важна быстрота: система «Мост для ПОД» позволяет раскрывать большинство преступлений в течение 15 минут.
- Изначально количество совместных расследований уклонений от санкций было небольшим. Однако после начала Специальной военной операции Российской Федерации на Украине в марте 2022 г. такие дела составляют большинство; начиная с марта 2022 г., их количество каждую неделю увеличивается в четыре раза. В настоящее время эта система в основном используется для быстрого прояснения ситуаций с новыми ложноположительными случаями, связанными с полными совпадениями, которыми перегружены отделы,

отвечающие за контроль соблюдения санкций, и которые мешают жить законопослушным клиентам. Кроме этого, в настоящее время изучаются возможности использования этой системы для обмена и распространения информации о приближенных лицах физических и юридических лиц, внесенных в санкционные списки, и принадлежащих им компаниях.

Участники: платформа «Мост для ПОД» разработана независимой сторонней организацией (в соответствии с ОРЗД она является лицом, обрабатывающим персональные данные). Изначально она использовалась четырьмя крупнейшими эстонскими банками (на долю которых в общей сложности приходится 90% операций); в настоящее время ей пользуются все 10 эстонских банков и несколько небанковских учреждений. В этом проекте очень важную роль играет ряд лиц и отделов банков, в т. ч. **генеральные директора** (административная поддержка), **сотрудники, отвечающие за ПОД** (члены наблюдательных советов), **сотрудники, отвечающие за защиту данных** (консультанты), **сотрудники отделов, отвечающих за защиту информации от несанкционированного использования** (обеспечивающие безопасность платформы для обмена данными). Кроме этого, каждый из этих банков назначает **руководителей проекта,** которые посещают заседания наблюдательного совета, выступают в качестве связующего звена между разработчиком платформы/лицом, обрабатывающим личные данные, и банком, а также координируют внутреннюю деятельность. Конечными пользователями этой платформы являются сотрудники отделов банков, отвечающие за борьбу с преступностью (ПОД/ФТ/ФРОМУ, проверка по санкционным спискам, мониторинг операций, борьба с мошенничествами и т.д.), которые занимаются оперативной работой и обеспечивают постоянную обратную связь на платформе.

Виды данных, которые собирают и которыми обмениваются: с помощью этой платформы главным образом осуществляется обмен данными об операциях; обмен ими происходит практически в режиме реального времени. Набор данных может меняться; он определяется в зависимости от предполагаемого преступления отдельными участниками платформы. Обмен информацией с помощью «шаблонов ситуаций» позволяет участникам платформы указывать виды информации, необходимые ее получателю для выявления соответствующего субъекта (например, имя клиента, номер счета, идентификационный номер операции), а также для определения запрашиваемых данных (например, полного имени, даты рождения, источника благосостояния, причины осуществления платежа, уровня риска, возможных настораживающих признаков, копий документов и т.д.) Обмен информацией касается расследований и запросов информации, связанных с возможным ОД, уклонением от санкций, мошенничествами и связанных с ними ситуаций.

Правовое основание обработки персональных данных: будучи оператором персональных данных каждый банк должен иметь правовое основание для обмена данными с помощью платформы «Мост для ПОД». В большинстве случаев банки обмениваются информацией и обрабатывают ее на одном из двух оснований, предусмотренных в ОРЗД: «соблюдение закона» или «законный интерес» (пункт 6.1(e) ОРЗД). Кроме этого, Закон о недопущении ОД/ФТ Эстонии предусматривает определенные ограничения прав субъектов данных, касающихся ЗДЛЖ, на основании того, что деятельность в области ПОД/ФТ/ФРОМУ отвечает интересам общества. В частности, в этом законе говорится, что ФУ разрешается обмениваться персональными данными для осуществления сотрудничества (раздел 16) и что в этом случае определенные

права на неприкосновенность частной жизни могут ограничиваться в связи с тем, что деятельность в области ПОД/ФТ/ФРОМУ отвечает интересам общества (раздел 48). Для защиты данных в соответствии с ОРЗД каждый банк, использующий платформу, подписывает соглашение об обработке данных с ее разработчиком/лицом, обрабатывающим личные данные.

Оценка соразмерности: степень обмена данными и объем таких данных, географическая область, в пределах которой происходит обмен данными, и сроки их хранения устанавливаются банками, пользующимися этой платформой. Вместе с тем, платформа создана так, чтобы ограничивать объем и тип данных, которыми обмениваются банки, чтобы помочь им свести к минимуму обмен информацией. Платформа позволяет вести контрольные журналы, что помогает банкам осуществлять анализ, проводить проверки контроля качества и выявлять ненужные действия.

Другие факторы ЗДЛЖ, которые необходимо принять во внимание:

- **Прозрачность, информирование и права субъектов данных:** соглашения об обработке информации предусматривают, что разработчик платформы (лицо, обрабатывающее личные данные) обязуется оказывать обоснованное содействие оператору персональных данных (банку) для исполнения его обязанности по реагированию на запросы субъектов данных, касающихся осуществления их прав на защиту данных. В случае получения разработчиком (лицом, обрабатывающим личные данные) таких запросов, последние направляются в банк со всей соответствующей информацией.
- **Обеспечение конфиденциальности и защита данных от несанкционированного использования:** платформа «Мост для ПОД» снабжена системой защиты данных от несанкционированного использования, которая обеспечивает строгий контроль доступа (в т.ч. двухфакторную аутентификацию и наличие списка разрешенных IP), шифрование (во время передачи и во время хранения данных), аварийное восстановление (с созданием резервных копий и проведением регулярных проверок) и ведение контрольных журналов. Доступ к документации, касающейся защиты данных, в том числе к контрольным журналам имеют все банки, пользующиеся платформой. Безопасность платформы проверяется как минимум раз в год аккредитованной третьей стороной; все учреждения имеют право проводить собственную проверку на возможность проникновения в систему (один банк воспользовался этим правом и поделился результатами проведенной проверки с другими банками).

Используемые технологии: в платформе «Мост для ПОД» применяется сквозное шифрование с использованием паролей. Все сообщения зашифровываются с помощью закрытого и открытого ключа; для их дешифровки пользователь должен получить доступ к своему закрытому ключу с помощью ввода еще одного пароля, который отличается от основного пароля, использующегося для получения доступа к платформе. Доступа к этому ключу не имеет ни разработчик платформы, ни какое-либо другое лицо.

Дополнительные соображения и проблемы:

- **Самым серьезным препятствием для обмена данными между субъектами частного бизнеса является отсутствие четкости нормативных положений:** Банки намеревались начать обмениваться информацией таким образом, который был предусмотрен в соответствующих законах и подзаконных актах.

- **Наличие ОРЗД не является препятствием; он позволяет осуществлять обмен данными, касающимися финансовых преступлений:** единые правила для всех банков и регулирующего органа позволяют всем участникам и соответствующим организациям быстро договариваться о приемлемости конкретной формы обмена информацией о финансовых преступлениях между субъектами частного бизнеса.
- **Регулирующие органы (особенно надзорные органы и органы, отвечающие за защиту данных) должны участвовать в проекте с самого начала:** успех использования платформы «Мост для ПОД» частично основывается на управлении ею. Регулирующие органы зачастую конфликтуют с лицами, деятельность которых они регулируют. Реализация этого проекта позволила избежать серьезных неудач за счет того, что все заинтересованные лица имели необходимую информацию и активно участвовали в его осуществлении. Банки с готовностью участвовали в этой новаторской инициативе, поскольку они не боялись столкнуться с «сюрпризами» со стороны Управления по финансовому надзору или органа, отвечающего за защиту данных.
- **Необходимым обязательным условием для начала осуществления банками программ по обмену данных является участие в них руководителей таких банков:** для разработки и реализации программы по обмену данными, касающейся финансовых преступлений, необходимы серьезные усилия целого ряда отделов и сотрудников на протяжении нескольких месяцев. В разработке и реализации такой программы обязательно должно участвовать руководство банков.

Участие органов власти (отвечающих за ПОД/ФТ/ФРОМУ и за ЗДЛЖ): Контроль со стороны государства за функционированием «Мост для ПОД» осуществляется **Управлением по финансовому надзору** (которое является членом Наблюдательного совета и наблюдателем в нем), ПФР (является членом Наблюдательного совета) **и органом власти, отвечающим за защиту данных** (является наблюдателем в Наблюдательном совете).

Источник: Обсуждения с учреждениями, использующими платформу «Мост для ПОД», и полученная от них информация: документ, посвященный этой платформе, доступен по ссылке: https://salv.com/uploads/AML-Bridge-Estonia.pdf

Примечание:

1. Мошенничества, связанные с выманиванием денег, заключаются в том, что людей обманным путем вынуждают перечислять денежные средства на банковский счет, принадлежащий мошеннику. Зачастую это происходит в результате того, что мошенник получает информацию о будущей жертве (например, с помощью взлома электронной почты) и выдает себя за компанию, с которой пострадавший имеет деловые отношения. К такому типу мошенничества также относятся мошенничества на сайтах знакомств и инвестиционные мошенничества. Поскольку пострадавший сам совершает платеж, зачастую отозвать или отменить его бывает трудно или даже невозможно.

Вставка 4.7. Прототип безопасного кластера больших финансовых данных (ПБКБФД) (Германия): Начальный этап проекта по обмену информацией между субъектами частного бизнеса

Описание и цель проекта: прототип безопасного кластера больших финансовых данных (ПБКФД) является частью осуществляемого в Европе проекта GAIA-X, целью которого является создание единой экосистемы по оказанию облачных услуг и услуг по обработке и передаче данных, которая будет защищена европейским законодательством по защите данных. Он представляет собой платформу, на которой разрабатываются и предоставляются для использования приложения, связанные с искусственным интеллектом. Доступ к таким приложениям имеют ФУ Европы. Платформа, на которой хранятся финансовые данные, позволяет осуществлять обмен данными с одновременным обеспечением безопасности данных физических лиц. Для использования с целью ПОД направляемые банками финансовые данные поступают на платформу ПБКФД, и создаются приложения для борьбы с ОД.

Запланированные или достигнутые результаты: накопление финансовых данных, направляемых представителями финансового сектора, позволяет значительно улучшить работу алгоритмов искусственного интеллекта и повысить эффективность и прозрачность.

Участники: за функционирование этой системы отвечает немецкая компания Deutsche Borse Group, три поставщика технологий (Spotixx, HAWK:AI и Google), четыре ФУ (Commerzbank, Deutsche Bank, Helaba и ING и один государственный орган - Министерство экономики, энергетики, транспорта и жилищного строительства земли Гессен).

Способ обмена информацией: децентрализованная экосистема позволяет хранить данные в отдельных хранилищах, принадлежащих банкам, они объединяются только в закрытой среде на срок действия алгоритма. Объединенные данные уничтожаются сразу же после окончания обработки.

Виды данных, имеющие отношение к проекту: в начале будут использоваться операции, осуществляемые в рамках Единого европейского пространства платежей. Были выработаны соответствующие требования для минимально жизнеспособных данных; особое внимание уделялось поиску компромисса между цензурированием информации о конечных пользователях и необходимым функционированием обучения алгоритмов.

Использование технологий повышения уровня конфиденциальности или других инструментов: данные зашифрованы во время передачи и во время хранения данных. Статическая децентрализованная токенизация данных, позволяющих установить личность, обеспечивает безопасность даже в случае их утечки. Кроме того, инфраструктура этого прототипа не позволяет пользователям получать непосредственный доступ к данным. Доступ к данным имеют только алгоритмы, которые были предварительно одобрены владельцами данных.

Правовое основание: поскольку этот проект находится на ранней стадии функционирования, на которой пока не осуществляется передача данных, его участники все еще выбирают наиболее подходящее основание обмена данными. Владельцы данных должны предварительно одобрять алгоритмы, которые могут обрабатывать данные. Таким образом, владельцы данных полностью контролируют то, ка-

кие данные обрабатываются, каким образом они обрабатываются и что происходит с результатами такой обработки. Личные данные передаются, но не предоставляются другим субъектам в связи с применением токенизации и конструкцией закрытого банка данных. Кроме этого, специальные правила, например, требование осуществлять мониторинг в области ПОД и направлять СПО, создают более общее правовое основание.

Оценка соразмерности: эта система работает с использованием минимально жизнеспособного набора данных, создавая условия, основанные на принципе «доверять нельзя никому». В случае передачи данных их владелец теряет контроль за ними только на время их перенесения в защищенное закрытое пространства, после обработки они уничтожаются.

Другие факторы ЗДЛЖ, которые необходимо принять во внимание:

- **Качество и непротиворечивость/точность данных:** точность и полнота данных об операциях обеспечиваются за счет того, что банки направляют данные непосредственно на платформу. После этого особое внимание уделяется соблюдению высоких стандартов, касающихся проверки данных и тестирования алгоритмов, в т.ч. их тестирования на основании исторических данных. В целом, все это также обеспечивает непротиворечивость данных на выходе.
- **Прозрачность и информирование:** мониторинг для целей ПОД и направление сообщений встроены в рабочий процесс банка; это значит, что существующие системы могут и будут использоваться в качестве основополагающих элементов этого нового подхода.
- **Справедливость при принятии решений, основанных на автоматизированных процессах:** алгоритмы сообщают о подозрительных операциях, после чего такие сообщения подвергаются дальнейшему всестороннему изучению.
- **Передача и раскрытие данных:** функционирование алгоритмов контролируется владельцами данных; они препятствуют раскрытию конфиденциальной информации. После выявления подозрительных операций в рамках моделей генерируются предупреждения. Во всех остальных отношениях процесс раскрытия и передачи данных не меняется.
- **Обеспечение конфиденциальности и защита данных от несанкционированного использования:** личные данные покидают хранилище данных, принадлежащее владельцу данных, только после псевдонимизации. Соблюдаются все стандарты защиты от несанкционированного использования; каждый соответствующий владелец данных может управлять ключом защиты. Все изменения авторизации доступа фиксируются и могут быть проверены. Система приводит в действие алгоритмы только после того, как владелец данных ставит цифровую подпись.

Источник: Обсуждения с представителями соответствующих органов власти Германии и полученная от них информация.

Вставка 4.8. ЕвроДаТ (Германия): Начальная стадия функционирования системы по обмену информацией

Описание и цель проекта: ЕвроДаТ является проектом, финансируемым федеральным министерством Германии по экономической деятельности и борьбе с изменением климата. Задачей этого проекта является создание в Европе доверительного хранителя данных, который позволит обмениваться данными, главным образом финансовыми, таким образом, который соответствует GAIA-X (проекту, задачей которого является создание европейской федерации поставщиков инфраструктуры данных и поставщиков услуг, а также обеспечение цифрового суверенитета Европы). Одной из ее задач является выявление мошенничеств.

Запланированные или достигнутые результаты: задачей создания доверительного хранителя данных является обеспечение полу- или полностью автоматизированного обмена информацией при соблюдении требований в области ЗДЛЖ и обеспечении простоты доступа к ней.

Участники: в этом проекте будут принимать участие разные лица в зависимости от характера использования, сейчас к ним относятся представители государственного министерства (Министерство экономики, энергетики, транспорта и жилищного строительства земли Гессен), ученые (Центр ответственной цифровизации (ZEVEDI), Университет Саара, Университет им Гете, Франкфурт, Немецкий исследовательский центр по искусственному интеллекту (DFKI) и поставщики технологий (ATOS, Deloitte, d-fine, Lexemo).

Способ обмена информацией: ЕвроДаТ функционирует таким образом, что данные не объединяются и не хранятся в одном месте. Вместо этого ЕвроДаТ выступает в качестве информационной платформы, с помощью которой могут быть получены данные для выполнения индивидуальных запросов. Такой способ обращения с данными очень важен: этот доверительный хранитель не является местом, из которого соответствующие лица могут получать данные. Вместо этого он связывает поставщиков и пользователей данных. В соответствии с контрактными или другими правовыми обязательствами сторон, данные предоставляются для осуществления каждого отдельного процесса. Данные временно хранятся в хранилищах системы, доступ к которым не имеет даже сам хранитель. Находясь в них, данные могут анализироваться с помощью алгоритмов, предоставляемых либо теми, кто предоставил данные, либо теми, кто получил данные, или третьей стороной. Хранитель данных передает результаты таким сторонам в соответствии с достигнутыми договоренностями. После этого он уничтожает такие данные.

Виды данных, имеющие отношение к проекту: в настоящее время отсутствуют ограничения или предписания относительно типов или видов данных, которыми можно обмениваться с помощью ЕвроДаТ.

Правовое основание: поскольку этот проект находится на ранней стадии разработки и обмен данными пока не происходит, его участники еще определяют наиболее подходящее правовое основание для обмена информацией. Наличие широких возможностей, предоставляемых в рамках этого проекта, означает, что анализ каждой операции с данными должен осуществляться на отдельных условиях и что различные типы данных регулируются различными режимами ЗДЛЖ и основами для обмена данными.

Оценка соразмерности: в рамках ЕвроДаТ будет создана инфраструктура для анализа данных; эта система не будет принимать решений о самом процессе обработки данных. Ответственность за вопросы, связанные с ЗДЛЖ, несут главным образом те, кто ею пользуются; решения, касающиеся обработки данных, будут принимать они. Предполагается, что в рамках ЕвроДаТ будет осуществляться классификация данных, которая поможет распределять различные данные по группам, что будет способствовать выявлению рисков нарушения защиты данных и избегать их.

Анализ факторов, касающихся ЗДЛЖ:

- **Качество и непротиворечивость/точность:** ответственность за обеспечение точности и полноты данных лежит на предоставляющих их лицах. Конкретные варианты использования, возможно, потребуют разработки общих стандартов.
- **Прозрачность и информирование:** планируется, что осуществляемое в настоящее время использование с целью ПОД основывается на существующих системах и позволяет осуществлять более эффективное сотрудничество между банками без необходимости раскрытия данных. Таким образом, существующие модели, касающиеся прозрачности и информирования, должны быть использованы в будущем.
- **Передача и раскрытие данных:** в настоящее время проект предусматривает, что его участники осуществляют полный контроль своих данных. Это значит, что дальнейшая передача или раскрытие должны быть как юридически запрещены, так и в идеале быть технически невозможны, поскольку хранитель не должен иметь доступа к данным.
- **Обеспечение конфиденциальности и защита данных от несанкционированного использования:** в основе этого хранителя данных лежит принцип, согласно которому данные могут обрабатываться таким образом, который заранее определяется тем, кто их предоставляет. Хранитель обеспечивает абсолютно надежную и анонимную среду, которая гарантирует, что доступ к данным не получат посторонние лица. Хранитель также ведет контрольные журналы, которые касаются как соглашений между сторонами, так и доступа, предоставляемого различным сторонам на основании таких соглашений. Этот также означает, что хранитель не может гарантировать, что данные будут обрабатываться в соответствии с законом. Для этого потребовалась бы идентифицирующая информация о данных. Это противоречит основополагающему принципу этого хранителя.

Обсуждение других соображений, проблем и извлеченных уроков: По сути дела, этот хранитель не может принять на себя основной груз рассмотрения принципов, касающихся ЗДЛЖ, без участия тех, кто ими пользуется. Ответственные стороны (т.е. финансовые учреждения) всегда будут вынуждены обеспечивать законность владения и обработки данных. Это является проблемой. Большинство заинтересованных третьих сторон (в т.ч. финансовые учреждения) хотят, чтобы требования в области ЗДЛЖ были сформулированы этим хранителем. Хотя существует надежда на то, что в рамках хранителя операции с данными будут оптимизированы, а связанные с ними вопросы, касающиеся ЗДЛЖ, будут решены; пока ситуация носит другой характер. Вместо этого работа с хранителем, особенно

на этой ранней стадии, по-прежнему связана с трудностями для третьих сторон, включая финансовый сектор. Операторы личных данных находятся в положении, которое позволяет им сформулировать и понять свои проблемы, связанные с ЗДЛЖ, и принципы, которые они применяют к ним. Это должно привести к созданию хранителя и его функций. Существует надежда, что максимально тесное сотрудничество между разработчиками хранителя и заинтересованными третьими сторонами позволит в будущем стандартизировать и автоматизировать классификацию и обработку данных.

Источник: Обсуждения с представителями соответствующих органов власти Германии и предоставленная ими информация.

РАЗДЕЛ V.
Каковы потенциальные проблемные вопросы, возникающие в процессе обмена информацией в частном секторе в целях ПОД/ФТ/ФРОМУ в рамках нормативно-правовой базы и требований, касающихся защиты данных и конфиденциальности?[33]

29. В данном Разделе рассматриваются распространённые проблемы, возникающие при разработке и внедрении механизмов обмена информацией в частном секторе в целях противодействия отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения (ПОД/ФТ/ФРОМУ). Эти проблемы были выявлены на основании обратной связи, полученной по итогам обсуждения приведённых выше примеров и ситуационных исследований в рамках фокус-групп, комментариев государственных органов и консультаций с представителями отрасли[34]. В следующем Разделе (Разделе 6) содержатся рекомендации для государственного и частного сектора, которые могут помочь в решении этих проблем. ФАТФ надеется, что эта работа поможет странам, рассматривающим возможность внедрения механизмов обмена информацией в частном секторе, понять, как их партнёры выполняют обязательства, касающиеся защиты данных и конфиденциальности (ЗДЛЖ), при разработке проектов и инициатив по обмену информацией. Однако каждая такая инициатива должна рассматриваться отдельно с учётом уникальных характеристик и соответствующих требований ЗДЛЖ, существующих в разных странах.

Политические вопросы

30. Приведённые в предыдущем Разделе примеры и ситуационные исследования показывают, что участие государственных органов, похоже, является существенным фактором для успешной реализации инициатив по обмену информацией в целях ПОД/ФТ/ФРОМУ в частном секторе. При этом государственные органы могут играть разную роль и в разной степени участвовать в этих процессах[35], в зависимости

[33] В Разделе 6 Аналитического отчёта по итогам 1 этапа проекта, касающегося критической оценки объединения данных, совместного анализа и защиты данных, содержится общий обзор трудностей и проблем, связанных с использованием новых технологий в целях совместного анализа данных.

[34] В период с октября 2021 года по июнь 2022 года проектная группа ФАТФ провела шесть обсуждений и презентаций в рамках фокус-групп, в которых приняли участие разные юрисдикции, в том числе Эстония, Германия, Нидерланды, Сингапур, Великобритания и Соединённые Штаты Америки. Кроме того, Секретариат ФАТФ также провёл консультации и обсуждения этих вопросов с заинтересованными представителями государственного и частного сектора европейских стран.

[35] Например, в Великобритании органы, отвечающие за ПОД/ФТ, а также органы, отвечающие за ЗДЛЖ, объединили свои усилия для поддержки частного сектора по мере разработки и реализации проектов. В частности, представители Управления уполномоченного по информации Великобритании (ICO) приняли участие в предварительном тестировании технологий, что позволило компаниям, занимающимся обработкой данных, решить проблемы, свя+занные с защитой данных, перед началом разработки соответствующих новых продуктов и услуг. Орган финансового надзора Сингапура сыграл ведущую роль в объединении разных заинтересованных представителей государственного и частного сектора в процессе разработки инициативы по обмену данными. Министерство финансов Нидерландов (которое также отвечает за вопросы ПОД/ФТ) учло предложения, поступившие из частного сектора, и включило некоторые элементы инициативы по обмену информацией в свою пересмотренную стратегию в сфере ПОД/ФТ, которая будет обнародована в ближайшее время.

от целей инициатив по обмену информацией и их готовности и желания предоставлять руководящие указания (по крайней мере, на высоком уровне) своим поднадзорным учреждениям. При этом полная **отстранённость государственных органов от этого процесса**, **особенно на начальных этапах**, часто приводила к усугублению проблем обмена информацией в частном секторе.

31. При отсутствии четко определённого контактного органа или ведущего ведомства, возглавляющего инициативы по обмену информацией, данные, которыми обмениваются учреждения частного сектора, **необязательно соответствуют национальным целям и приоритетным задачам в области ПОД/ФТ/ФРОМУ**. Как видно из некоторых приведённых выше примеров (см., например, Проект КОСМИК во Вставке 4.2), участие в инициативах по обмену информацией лишь нескольких избранных или заинтересованных финансовых учреждений, а не всех учреждений, может потенциально привести к смещению рисков. Иными словами, преступники могут начать осуществлять свои операции через те финансовые учреждения, которые не участвуют в этих инициативах.

32. Кроме того, успешный обмен информацией может быть затруднён вследствие отсутствия взаимодействия между органами, отвечающими за ПОД/ФТ/ФРОМУ, и органами, отвечающими за ЗДЛЖ, или по причине **отсутствия связи и координации между ведомствами, занимающимися вопросами ПОД/ФТ/ФРОМУ, и ведомствами, занимающимися вопросами ЗДЛЖ**. Такое взаимодействие является важным для обеспечения уверенности/ясности относительно обмена информацией и повышения качества разработки инициатив по обмену информацией. Отсутствие взаимодействия между такими органами может привести к конфликтам вследствие взаимного непонимания важных общественных интересов, касающихся как защиты общества от преступности и терроризма, так и защиты персональных данных и конфиденциальности.

33. Участники проектов по обмену информацией (описанных в примерах, приведённых в Разделе 4) также подчеркнули, что без государственной поддержки субъекты частного сектора сталкиваются **с трудностями в получении поддержки со стороны партнёров и обратной связи от органов, отвечающих за ЗДЛЖ**. Такая поддержка и обратная связь необходимы для разъяснения практической пользы от инициатив по обмену информацией (например, для повышения качества сообщений о подозрительных операциях). Это также демонстрирует, как и почему обмен информацией в частном секторе отвечает более широким общественным интересам (то есть, как и почему это способствует, в том числе, решению задач в области ПОД/ФТ/ФРОМУ; снижению числа низкокачественных или недостаточно обоснованных СПО, которые не защищают права добросовестных клиентов/цели законных операций; или предупреждению случаев отказа в обслуживании под предлогом снижения рисков)[36].

34. Как отмечено и показано в приведённых выше примерах и ситуационных исследованиях, до **сих пор не создана «типовая модель» или «типовая схема» обмена информацией в частном секторе**, которая бы соответствовала и способствовала

[36] Отказ в обслуживании под предлогом снижения рисков состоит в том, что финансовые учреждения прекращают или ограничивают деловые отношения с клиентами или определёнными категориями клиентов во избежание рисков вместо того, чтобы реализовывать меры по управлению рисками в соответствии с риск-ориентированным подходом ФАТФ. (См. документ ФАТФ: «Разъяснение ФАТФ риск-ориентированного подхода: рассмотрение и учёт рисков в каждом конкретном случае, а не повальные отказы в обслуживании под предлогом снижения рисков» на сайте: https://www.fatfgafi.org/documents/news/rba-and-de-risking.html). Например, в определённых случаях дополнительная информация может помочь в прояснении подозрений и, таким образом, обеспечить равноправный и справедливый доступ к финансовым услугам.

выполнению требований как в сфере ПОД/ФТ/ФРОМУ, так и в области защиты данных и конфиденциальности. Как указано в Разделе 3, законодательство о защите данных основано в значительной степени на установленных принципах и правилах. Это означает, что реализация инициатив по обмену информацией зависит от конкретных обстоятельств и подразумевает нахождение баланса между разными политическими целями. Таким образом, органы, отвечающие за ЗДЛЖ, должны отдельно рассматривать каждое предложение по обмену информацией с учётом конкретных обстоятельств. Они могут не поддержать конкретный проект или подход, учитывая риск того, что их поддержка будет воспринята в качестве подтверждения того, что проект соответствует всем требованиям ЗДЛЖ. Отсутствие координации и сотрудничества между органами, отвечающими за ПОД/ФТ/ФРОМУ, и органами, отвечающими за ЗДЛЖ, может привести к ограниченному пониманию соответствующих политических целей. В этой связи органы, занимающиеся вопросами ЗДЛЖ, вряд ли порекомендуют финансовым учреждениям вкладывать средства и продвигать подобные инициативы.

35. В Разделе 6 содержится ряд рекомендаций, направленных на решение этих проблем. Это включает активную поддержку со стороны государственного сектора (пункты 51-52), поддержание постоянного диалога между органами, отвечающими за ЗДЛЖ, и органами, отвечающими за ПОД/ФТ/ФРОМУ (пункты 53-55), и постоянное взаимодействие между частным сектором и органами, отвечающими за ЗДЛЖ, начиная с самых ранних этапов реализации инициатив (пункт 60).

Правовые вопросы

36. Различные национальные и международные законодательные и нормативно-правовые акты в сфере защиты данных и конфиденциальности также представляют определённые проблемы и трудности для реализации проектов по обмену информацией между субъектами частного бизнеса. Заинтересованные финансовые учреждения потратили немало усилий на анализ законов, нормативных актов и других надзорных/регулятивных инструментов (включая международные законы и многосторонние договоры, упомянутые в Разделе 3) с тем, чтобы убедиться в законности таких механизмов обмена информацией в каждой конкретной юрисдикции. Имеется широкий спектр юридических требований и принципов, которые учреждения должны принимать во внимание (см. Раздел 3). Например, некоторые конкретные проблемные вопросы, поднятые участниками инициатив, описанных в ситуационных исследованиях, включают следующее:

- **Является ли обмен информацией в целях ПОД/ФТ/ФРОМУ с другими финансовыми учреждениями или трансграничный обмен такой информацией между разными субъектами, входящими в состав одной и той же группы (помимо надзорных или оперативных ведомств), законным, соответствующим и разрешённым в соответствии с правилами в сфере ПОД/ФТ/ФРОМУ и ЗДЛЖ? Соответствует ли такой обмен информацией контрактным договорённостям с клиентами, касающимся прав на данные/на использование данных?** В качестве первого шага учреждениям необходимо определить, являются ли сведения, которыми предлагается обмениваться, персональными данными или нет, и, следовательно, распространяются ли на них правила ЗДЛЖ. В правилах ЗДЛЖ часто установлено, что обмен данными должен быть «необходимым» или «соразмерным» для обеспечения «законных интересов» и/или быть чётко разрешён действующим законодательством (помимо ряда других возможных требований – см. Раздел 3). Некоторые участники вышеупомянутых инициатив (см. Раздел 4) указали на трудности с демонстрацией того, что обмен инфор-

мацией является «необходимым», перед проведением тестовых испытаний в рамках инициативы для получения чётких и определённых результатов. Субъекты частного бизнеса могут не захотеть брать на себя правовые риски, связанные с разработкой таких инициатив, ввиду юридической неопределённости, представляемой законами о ЗДЛЖ; или без поддержки соответствующих руководящих/ координирующих государственных политических ведомств; или если реализация таких инициатив не требуется для направления СПО согласно национальному законодательству (или в соответствующих Стандартах ФАТФ). Последнее соображение является особенно распространённым в случае обмена данными до возникновения подозрений в свете более жёстких требований, распространяющихся на такой обмен данными.

- **Является ли обмен данными о клиентах/операциях на основании совместного или автоматического анализа правомерным, необходимым и соразмерным, и не нарушает ли это законные интересы и права клиентов (в юрисдикциях, в которых установлены такие стандарты)?** В случае обмена персональными данными до возникновения подозрений установлены более жесткие ограничения, поскольку это касается широкого круга данных. В некоторых юрисдикциях обмен информацией на этом этапе может быть не разрешён в соответствии с законами о ЗДЛЖ. В этой связи учреждениям в определённых юрисдикциях может потребоваться тщательно проработать механизмы для исключения персональных данных при обмене информацией до возникновения подозрений (например, использовать технологии, повышающие конфиденциальность, или уточнять объём данных – см. Раздел 6). Что касается обмена информацией после возникновения подозрений, то некоторым финансовым учреждениям могут потребоваться дополнительные указания относительно того, как использовать сведения, полученные в рамках обмена информацией, в иных целях помимо направления СПО. Например, может ли такая информация использоваться для обновления сведений, полученных в результате надлежащей проверки клиентов, для оценки и управления рисками или для прекращения деловых отношений с клиентами, и будет ли такое дополнительное использование информации считаться правомерным/законным/необходимым/соразмерным основной цели, заключающейся в выявлении подозрительной деятельности.

- **Является ли согласие, полученное от клиентов, достаточным для обмена информацией в тех юрисдикциях и ситуациях, в которых согласие может служить законным основанием для обмена информацией?** Возможность полагаться на согласие подразумевает, что финансовое учреждение выполняет обычные требования ЗДЛЖ в целях обеспечения прозрачности в своей политике, касающейся конфиденциальности, в уведомлениях для клиентов и в других заявлениях, доступных для клиентов. Например, это может включать в себя предоставление информации о третьих сторонах, которые могут получить доступ к персональным данным, и то, как происходит обработка таких данных. Как правило, учреждения заранее получают общее согласие от клиентов, необходимое для выполнения обычных требований ЗДЛЖ, для последующего обмена информацией в целях ПОД/ФТ/ФРОМУ или в целях предотвращения/выявления преступной деятельности. Однако такая информация передаётся в основном оперативным ведомствам, таким как ПФР или правоохранительные органы, но не другим финансовым учреждениям. Кроме того, изменение положений в заявлении

о согласии на раскрытие персональных данных с целью внедрения новых практик обмена информацией может также представлять логистические проблемы (например, применительно к существующим услугам и клиентам). Помимо этого, последующий отзыв согласия может также представлять проблему (в плане соблюдения принципов ЗДЛЖ – см. пункт 22 в Разделе 3). Использование согласия может также оказаться проблематичным в некоторых юрисдикциях в ситуациях, когда такое согласие может быть расценено, как полученное в принудительном порядке или не добровольно. Например, в случаях, когда у клиента не остаётся никакого другого выбора для получения конкретных финансовых услуг или когда согласие требуется в качестве необходимого условия для обслуживания. По этим причинам согласие вряд ли будет являться наиболее целесообразным или единственным законным основанием для обмена информацией в целях ПОД/ФТ/ФРОМУ.

- **Представляют ли инициативы по обмену информацией риск нарушения запретов на разглашение или на раскрытие фактов направления СПО?** Как указано в отчёте по итогам 1-го этапа данной работы (см. подраздел 6.5 Аналитического отчёта по итогам 1 этапа проекта), учреждениям, участвующим в инициативах и проектах по обмену информацией, придётся разработать дополнительные меры для обеспечения того, чтобы любой обмен информацией о клиентах/операциях и вытекающие из этого возможные изменения в деловых отношениях с клиентами или в рейтинге риска не привели к разглашению или к противоречию с соответствующими Стандартами ФАТФ (например, с Рекомендацией 21). У некоторых участников инициатив, описанных выше (см. Раздел 4), возникла путаница относительно того, может ли любое предоставление информации третьей стороне (т.е. не клиенту) являться разглашением. Иногда субъекты частного сектора испытывают затруднения в разработке надлежащего набора мер, которые служат достижению целей обмена информацией и одновременно обеспечивают выполнение запрета на разглашение/соблюдение конфиденциальности, без получения соответствующих руководящих указаний от надзорных/регулирующих органов. В будущем в рамках инициатив по обмену информацией может быть дополнительно рассмотрено создание соответствующих платформ таким образом, чтобы исключать возможность разглашения (например, путём использования зашифрованных поисковых запросов при осуществлении поиска в массивах децентрализованных данных).

37. Хотя в некоторых случаях использование данных может оказаться актуальным для уголовных расследований, такое использование может ограничить возможность участвующих в инициативах финансовых учреждений обеспечивать прозрачность в отношениях с субъектами данных, а также ограничить возможность для внесения изменений в соответствии с правилами ЗДЛЖ. Предусмотренные ФАТФ правила о недопущении разглашения (Рекомендация 21) преследуют цель обеспечить конфиденциальность уголовных расследований, и должны быть установлены в национальных законах или нормативных актах. В Стандартах ФАТФ (в Рекомендации 2) также содержатся требования о сотрудничестве и взаимодействии в целях обеспечения совместимости требований ПОД/ФТ с правилами ЗДЛЖ. В зависимости от национальных законов в области ЗДЛЖ, могут также использоваться исключения из правил, касающихся конфиденциальности, в целях предупреждения, расследования, раскрытия или судебного преследования за преступную деятельность. Приведённые примеры указывают на необходимость наличия согласованных мер предосторожности (например, требование к финансовым учреждениям проводить

собственные расследования при получении сигналов от своих служб ПОД), а также на необходимость предоставления субъектам данных возможности для обжалования решений о лишении их доступа к финансовым услугам, для получения разъяснений или дополнительной информации.

38. В Разделе 6 содержится ряд рекомендаций, направленных на решение этих проблем. Это включает активную поддержку со стороны государственного сектора (пункты 51-52), обеспечение защиты данных на этапе проектирования (пункты 58-59), постоянное взаимодействие между частным сектором и органами, отвечающими за ЗДЛЖ, начиная с самых ранних этапов реализации инициатив (пункт 60), и разработку параметров и показателей для оценки успеха (пункт 61).

Операционные вопросы

39. Ряд проблем и трудностей, выявленных ФАТФ в ходе предыдущей работы (например, в Аналитическом отчёте по итогам 1 этапа проекта), продолжают оставаться актуальными применительно к новым инициативам по обмену информацией в частном секторе. Причём эти проблемы касаются как государственных органов, так и субъектов частного бизнеса, участвующих в проектах по обмену информацией. При этом субъекты частного бизнеса могут столкнуться с этими проблемами и трудностями как на уровне отдельных учреждений, так и на секторальном уровне. Рекомендации, содержащиеся в Разделе 6 данного Отчёта, направлены на обмен опытом, полученным по итогам изучения примеров и ситуационных исследований, для оказания содействия юрисдикциям в преодолении таких трудностей. Целью этих рекомендаций также является обеспечение эффективности, результативности и своевременности инициатив по обмену информацией в частном секторе и избежание задержек в выявлении подозрительных операций или клиентов/преступных сетей при соблюдении соответствующих требований ЗДЛЖ.

40. **Объём данных:** в некоторых примерах отмечены затруднения при определении объёма передаваемых данных для достижения целей инициатив. Для соблюдения требований ЗДЛЖ (например, обеспечения законности обмена информацией и минимизации объёма передаваемых данных до уровня необходимого для достижения конкретных целей проекта) в некоторые инициативы по обмену информацией были внесены корректировки для сокращения объёма и видов передаваемых данных. Эта проблема особенно актуальна для обмена информацией до возникновения подозрений. Для соблюдения соответствующих правил ЗДЛЖ и минимизации (или исключения) передачи персональных данных некоторые проекты были ограничены обменом конкретными видами информации (например, информацией об операциях, осуществляемых юридическими лицами), в которой, как правило, содержится меньший объём данных, позволяющих установить конкретных лиц, или вообще не содержится таких данных. В рамках других проектов было ограничено количество передаваемых единиц информации до уровня сведений, необходимых для достижения целей инициатив. В результате участники некоторых из этих инициатив по обмену информацией столкнулись с трудностями в плане достижения изначально заявленных целей и, как следствие, были вынуждены пересмотреть исходные задачи и ожидаемые результаты, связанные с обменом информацией. Хотя ограничение объёма и видов данных, передаваемых в рамках инициатив по обмену информацией, помогает обеспечить соблюдений правил ЗДЛЖ, некоторые субъекты частного бизнеса, участвующие в этих инициативах, указали, что это также может снизить или свести на нет полезность таких проектов. Кроме того, также могут возникнуть вопросы относительно того, являются ли передаваемые данные достаточными для реального содействия учреждениям частного сектора, участвующим в проектах, в понимании подозрительных операций, осуществляемых через разные учреждения.

41. **Точность и надёжность данных:** в некоторых примерах указывается на использование технологий, повышающих конфиденциальность (технологий ТПК) для того, чтобы завуалировать личность клиентов в рамках реализуемых мер по обеспечению конфиденциальности данных. При этом некоторые субъекты частного бизнеса, участвующие в таких проектах, отметили, что технологии ТПК могут представлять операционные трудности, в зависимости от того, как именно они используются. Например, определённые технологии ТПК, используемые в рамках некоторых проектов, могут не соответствовать установленным целям, что затрудняет определение точности получаемых/ передаваемых данных и, таким образом, снижает надёжность и качество информационного обмена. Кроме того, некоторые участники проектов были вынуждены потратить дополнительные ресурсы для отслеживания получаемых данных, прежде чем предпринять какие-либо последующие меры реагирования, такие как осуществление мониторинга или направление СПО. Эти трудности могут возрасти в случае наличия дополнительных проблем, связанных с подготовкой и совместимостью данных. Проблемы и затруднения также могут возрасти в случае невозможности эффективного объединения записей, что приводит к риску сомнительной связи записей (т.е. к ошибочной связи информации или данных, касающихся двух несвязанных субъектов).

42. **Защита данных:** в целом (независимо от того, используются ли технологии ТПК или нет) субъектам частного бизнеса, участвующим в инициативах, потребуется создать защищённые каналы для передачи информации друг другу. Это является одним из основополагающих условий, так как любая утечка данных, хранящихся или передаваемых в рамках инициатив по обмену информацией, может привести к серьёзным негативным последствиям. Например, это может привести к нарушению прав клиентов на конфиденциальность персональных данных, снизить эффективность мер ПОД/ФТ/ФРОМУ, подорвать общественное доверие к инициативам по обмену информацией и участвующим в них учреждениям, а также нанести финансовый и нефинансовый ущерб пострадавшим лицам.

43. **Готовность данных и систем:** как и в случае любых других инициатив, связанных с трансформацией данных и обменом информацией, отсутствие структурированности данных и различия в форматах и классификации данных (что не дает возможность обеспечить совместимость данных) замедлили запуск некоторых инициатив по обмену информацией, описанных в предыдущих Разделах. В случае некоторых проектов потребовалось от трёх до пяти лет для выверки и обеспечения сопоставимости данных, прежде чем такие данные были готовы для передачи или анализа. В других случаях недостаток ИТ-возможностей привел к задержке официальной реализации проектов по обмену информацией, так как участвующим в них учреждениям частного бизнеса потребовалось модернизировать свои ИТ-инструменты (а также повысить профессиональную подготовку и навыки своих сотрудников в области ИТ) для того, чтобы появилась возможность обмениваться информацией. В этой связи заинтересованным субъектам частного бизнеса необходимо заранее продумать и запланировать проекты по обеспечению совместимости данных для содействия успешному запуску инициатив по обмену информацией.

44. В Разделе 6 содержится ряд рекомендаций, направленных на решение этих проблем. К ним относятся: обеспечение защиты данных на этапе проектирования (пункты 58-59), применение технологий повышения конфиденциальности (пункт 56) и принятие мер для подготовки данных (пункт 57).

Другие вопросы

45. **Предоставление финансовых услуг пострадавшим клиентам/отказ в обслуживании под предлогом снижения рисков:** инициативы по обмену информацией в частном секторе могут помочь участвующим в них учреждениям выявлять определённых клиентов или определённые операции для дальнейшего мониторинга в соответствии с их требованиями ПОД/ФТ/ФРОМУ и обычной внутренней политикой и процедурами в целях расследования возможной преступной финансовой деятельности и принятия необходимых мер. Эти инициативы могут уменьшить число СПО, направляемых на основании случайных совпадений, снизив, тем самым, негативное воздействие на клиентов и нагрузку на государственные органы. Однако, как и в случае любого выявления сомнительной деятельности по результатам анализа конкретных операций, это также может привести к прекращению деловых отношений с клиентами или к отказу от предоставления определённых финансовых услуг конкретным физическим лицам в целях управления рисками. Как указано в Аналитическом отчёте по итогам 1 этапа проекта, *«Однако тут кроется вероятность искажения ситуации путем направления избыточных упредительных СПО. Если слишком полагаться на систему обмена подозрительной информацией, можно столкнуться с ситуацией, когда финансовое учреждение сочтет клиента сомнительным только лишь на основании информации третьей стороны, а она может быть неточной, или же мотивы возникновения подозрений могут быть полностью опровергнуты подразделением финансовой разведки. Это может повлечь отказ (непредвиденный и неэтичный в данном случае) добросовестному клиенту в доступе к финансовой системе, или же в отношении операций клиента могут производиться дальнейшие выяснения их характера и целей, с задержками в исполнении банковских операций»*[37].

46. Важно отметить, что даже при отсутствии обмена информацией между субъектами частного бизнеса могут иметь случаи отказа в обслуживании под предлогом снижения риска. В этой связи вероятность множества негативных последствий или возможная чрезмерная зависимость от инициатив по обмену информацией вызывает дополнительную озабоченность. Однако также имеются противоположные соображения, согласно которым обмен информацией может повысить точность и надёжность данных и, таким образом, улучшить понимание рисков и принятия решений на основании таких данных, а также снизить количество случаев отказа в обслуживании под предлогом снижения рисков[38].

47. **Конкуренция:** как указано в Аналитическом отчёте по итогам 1 этапа проекта, «Циркулирование больших блоков обрабатываемой клиентской информации между финансовыми учреждениями потенциально может вызвать проблемы, связанные с конкуренцией. Результатом может стать выборочный обмен данными лишь с участниками небольших групп «доверенных лиц», и, как следствие, — неравномерный обмен информации в рамках системы. Таким образом, может наблюдаться переход рисков ОД/ФТ от финансовых учреждений, располагающих механизмами обмена информацией, к тем, кто их не имеет. Ненадежные участники, исключенные из своей группы первого типа, могут затем тяготеть ко вторым, чтобы уменьшить

[37] Аналитический отчёт ФАТФ по итогам 1 этапа проекта, пункт 89.

[38] Институт финансовой стабильности отметил, что качественный обмен информацией может помочь снизить число случаев необоснованного отказа в обслуживании под предлогом снижения рисков и, таким образом, способствовать охвату финансовыми услугами всех слоёв населения. Институт финансовой стабильности (сентябрь 2020г.) «Closing the loop: AML/CFT supervision of correspondent banking» (Замыкая контур: Надзор за корреспондентскими банковскими отношениями в целях ПОД/ФТ); доклад доступен на сайте: www.bis.org/fsi/publ/insights28.pdf

вероятность выявления. Поэтому финансовые учреждения или секторы, не располагающие механизмами обмена информацией, могут столкнуться с дополнительными рисками ОД/ФТ, и, в связи с этим, может понадобиться рассмотрение дополнительных способов снижения этих рисков. Доступ к данным (и обмен ими) со стороны ограниченного числа финансовых учреждений не должен приводить к тому, чтобы они имели несправедливые преимущества, ведь конкурентоспособность на рынке финансовых услуг все более обуславливается возможностью доступа к большим массивам актуальных (в режиме реального времени) данных. Поэтому при оценке возможностей обмена данными в сфере ПОД/ФТ могут возникать соображения, направленные в сторону законодательства о защите конкуренции, позволяющие обеспечить одинаковые условия для всех участников рынка и исключить возможности для вытеснения потенциальных конкурентов. Так, при гарантированном доступе к данным он должен предоставляться на справедливых, разумных и равных для всех условиях, а также способом, исключающим тайные договоренности и не способствующим их формированию». Инициативы должны быть ограничены обменом или доступом к данным, необходимым в целях ПОД/ФТ/ФРОМУ.

48. **Трансграничный обмен информацией:** как видно из приведённых примеров и ситуационных исследований, правила ЗДЛЖ, действующие в юрисдикции/регионе, могут повлиять на формат и масштаб инициативы по обмену информацией в частном секторе, реализуемой в этом месте. Это касается видов данных, которыми разрешено обмениваться, целей, в рамках которых можно обмениваться такими данными,. По этой причине инициативы по обмену информацией, реализованные на данный момент (несмотря на значительные выделяемые ресурсы), редко могут быть повторены или воспроизведены в других юрисдикциях. А это, в свою очередь, снижает практическую ценность инициатив по обмену информацией, так как проекты часто ограничены лишь одной юрисдикцией, что затрудняет их расширение за пределы границ юрисдикции в целях выявления трансграничной подозрительной деятельности или трансграничных сетей. Например, это может не позволить таким инициативам оказаться полезными для выявления более сложных схем отмывания денег с использованием сетей корреспондентских банковских отношений или с помощью финансирования торговли. Как правило, учреждения, участвующие в таких инициативах, являются крупными международными или региональными банками, получающими информацию из нескольких юрисдикций, в которых расположены учреждения, входящие в их финансовую группу. При этом участие в системе обмена информацией в одной юрисдикции может вызвать опасения относительно соблюдения установленных правил другими членами финансовой группы, если на них распространяются другие стандарты ЗДЛЖ (или имеет место другое толкование этих стандартов).

49. В Разделе 6 содержится ряд рекомендаций, направленных на решение этих проблем. К ним относятся принятие мер для недопущения отказа в обслуживании под предлогом снижения рисков (пункт 62) и активная поддержка со стороны государственного сектора (пункты 51-52).

РАЗДЕЛ VI.
Каковы ключевые рекомендации для эффективной реализации инициатив по обмену информацией в частном секторе в целях ПОД/ФТ/ФРОМУ при соблюдении правил ЗДЛЖ?

50. Хотя преодоление затруднений и проблем, описанных в предыдущем Разделе, может оказаться нелёгким делом, наблюдается определённый прогресс в реализации как уже утвержденных, так и находящихся на пилотном этапе инициатив по обмену информацией. По итогам обсуждений примеров и ситуационных исследований в рамках фокус-групп, был выработан ряд общих рекомендаций для успешного обмена информацией и проведения совместного анализа в целях ПОД/ФТ/ФРОМУ, включая следующее:

    1. Проведение оценки воздействия на защиту данных. Оно включает в себя чёткое определение целей и задач обмена информацией, данных, подлежащих обработке, и обоснование необходимости и достаточности/соразмерности таких данных для достижения заявленных целей, а также определение правовых оснований и мер защиты, которые будут применяться.

    2. Осуществление взаимодействия с органами, отвечающими за ЗДЛЖ, с самого начала реализации проектов по обмену информацией, т.е. на этапе разработки. Учитывая, что у органов, отвечающих за ЗДЛЖ, не всегда имеются достаточные ресурсы для работы с каждой отдельной организацией, такое взаимодействие и информационно-разъяснительная работа могут осуществляться в рамках секторального или группового подхода. Это также может способствовать более быстрой передаче опыта соответствующим секторам. Кроме того, это может обеспечить, чтобы накопленный опыт и извлеченные уроки не рассматривались участвующими в проектах учреждениями в качестве информации, являющейся их исключительной собственностью.

    3. Рассмотрение мер, необходимых для надлежащей защиты данных клиентов, включая использование технологий, повышающих конфиденциальность, и обезличивания и псевдонимизации данных[39] при необходимости.

51. Не существует универсального решения для достижения целей ПОД/ФТ/ФРОМУ и ЗДЛЖ для всех финансовых учреждений в глобальном масштабе. Инициативы по обмену информацией, рассмотренные в рамках данного проекта и в Аналитическом отчёте по итогам 1 этапа проекта, имеют разные цели и задачи, на них распространяются разные правовые требования, касающиеся ЗДЛЖ, и в них используются разные технологии и режимы. В этой связи в их основе лежит разная законодательная база, и предусмотрены разные меры по снижению рисков для достижения целей ПОД/ФТ/ФРОМУ и ЗДЛЖ. Однако общим ключевым элемен-

[39] Следует помнить, что требования ЗДЛЖ будут различаться, в зависимости от степени анонимизации (обезличенности) данных. Например, на обезличенные данные (т.е. на данные, которые не могут быть отнесены или привязаны к конкретному лицу) не распространяется Общий регламент защиты данных, в отличие от псевдонимизированных данных.

том является привлечение ряда заинтересованных сторон (с учётом местных нормативных актов и условий), использование поэтапного подхода и повышение общественного доверия и понимания в процессе разработки решений. Приведённые ниже рекомендации являются дополнением к рекомендациям, направленным на поддержку применения технологий в целях ПОД/ФТ, выработанным на первом этапе проекта. Они предназначены для субъектов государственного и частного сектора, заинтересованных в разработке и реализации инициатив по обмену информацией в частном секторе.

Рекомендации для государственных учреждений

Государственным учреждениям следует рассмотреть возможность оказания более активного содействия

52. Результаты обсуждения в рамках различных фокус-групп показывают, что наличие национального ведомства, координирующего деятельность в сфере ПОД/ФТ/ФРОМУ, которое активно возглавляет и продвигает инициативы по обмену информацией, как правило, помогает учреждениям частного бизнеса преодолеть ряд трудностей, особенно трудностей правового характера. Такая ситуация также может способствовать вовлечению других соответствующих органов, в частности органов, отвечающих за ЗДЛЖ, или ведомств, отвечающих за защиту потребителей или конкуренцию[40]. Участие государственных органов также может способствовать сотрудничеству с зарубежными партнёрами, например, для проверки того, можно ли и каким образом можно реализовывать инициативы по трансграничному обмену информацией в соответствии с требованиями ЗДЛЖ. Сближение режимов ЗДЛЖ разных юрисдикций, например, в результате усилий, предпринимаемых в рамках многосторонних форумов (см. Раздел 3), может способствовать разработке инициатив по трансграничному обмену информацией с соблюдением правил и обязательств ЗДЛЖ. При этом активное участие государственных органов в этой деятельности является критически важным.

53. Хотя это и не является обязательным требованием в рамках действующих Стандартов ФАТФ, государственные органы, заинтересованные в осуществлении инициатив по обмену информацией между субъектами частного бизнеса для повышения эффективности режимов ПОД/ФТ/ФРОМУ (независимо от того, являются ли они компетентными органами в сфере ПОД/ФТ/ФРОМУ или нет), могут, например:

- **Рассмотреть возможность обновления существующих правовых или надзорных документов для того, чтобы разрешить обмен информацией, или сделать исключения из ограничений на обмен информацией.** Это касается тех юрисдикций, в которых отсутствуют конкретные законодательные акты или надзорные документы, определяющие законность обмена информацией в частном секторе в целях ПОД/ФТ/ФРОМУ. Такие базовые законы обеспечивают наиболее надежное правовое основание, позволяющее осуществлять обмен и обработку данных в целях ПОД/ФТ/ФРОМУ, и при этом предусматривают необходимые меры для защиты данных

[40] Обсуждения моделей и схем использования в рамках фокус-групп показывают, что государственные органы, такие как органы финансового надзора, ПФР, органы, отвечающие за ЗДЛЖ, а также государственные органы, такие как министерства финансов, безопасности или юстиции, как правило, участвуют во взаимодействии и обсуждениях с ведущими учреждениями, отвечающими за контроль данных, и нередко за обработку данных, в рамках проектов по обмену информацией. В некоторых случаях в таких обсуждениях также участвуют другие государственные органы, отвечающие, например, за расследование случаев мошенничества, внедрение цифровых инноваций, обеспечение конкуренции и защиту прав потребителей.

и личной жизни (ЗДЛЖ). В таких законодательных актах могут быть определены функции как органов, отвечающих за ПОД/ФТ/ФРОМУ, так и органов, отвечающих за ЗДЛЖ, применительно к инициативам по обмену информацией. Например, в ситуационном исследовании, касающемся проекта СПП (Вставка 4.4 в Разделе 4), продемонстрирована конкретная роль органа, отвечающего за ЗДЛЖ, в сертификации инициатив по обмену информацией в Нидерландах. Наличие базового законодательства и четкое определение роли и функций бизнеса, отвечающих за ЗДЛЖ, помогает снизить коммерческие и юридические опасения субъектов частного сектора при запуске/реализации инициатив по обмену информацией. Например, в Сингапуре орган, отвечающий за надзор за финансовым сектором (Денежно-кредитное управление Сингапура), разработал проекты нормативно-правовых актов для обмена информацией между финансовыми учреждениями в целях ПОД/ФТ/ФРОМУ с использованием защищённой цифровой платформы КОСМИК (Вставка 4.2 в Разделе 4). Кроме того, Денежно-кредитное управление также организовало проведение публичных консультаций перед тем, как предложенные нормативно-правовые акты вступили в силу. Аналогичным образом Министерство финансов Нидерландов инициировало внесение поправок в законодательство для обеспечения возможности полномасштабного коллективного мониторинга операций в рамках инициативы по обмену информацией МОН (Вставка 4.3 в Разделе 4). Пример, посвящённый Разделу 314(b) Закона об объединении и укреплении США путем обеспечения соответствующих мер, направленных на пресечение и предупреждение терроризма (Закон о борьбе с терроризмом США «Патриот») (Вставка 4.5 в Разделе 4), также показывает полезность наличия базового законодательства.

- **Использовать регулятивные песочницы, пилотные программы или другие механизмы для тестовых испытаний инициатив по обмену информацией (особенно с использованием новых технологий) в контролируемых условиях.** Регулятивные песочницы обеспечивают механизм, с помощью которого субъекты частного бизнеса (например, финансовые учреждения или разработчики технологий) могут осуществлять тестирование инноваций в области обмена информацией и проводить эксперименты под контролем регулирующих органов. Это позволяет государственным органам понять последствия различных политических решений и удостовериться в полезности реализации инициатив по обмену информацией. Кроме того, такие регулятивные песочницы могут помочь получить данные или иную информацию в рамках тестовых испытаний инициатив для четкой оценки и демонстрации необходимости и соразмерности информационного обмена. С учётом взаимосвязи между различными нормативными базами, **совместные регулятивные песочницы являются особенно полезными площадками для тестовых испытаний инициатив по обмену данными в целях ПОД/ФТ/ФРОМУ** (с участием и при поддержке компетентных органов, органов, отвечающих за противодействие отмыванию денег, и органов, отвечающих за обеспечение защиты данных и конфиденциальности).

- Аналогичным образом, пилотные программы дают возможность для начального ограниченного обмена информацией в целях оценки ожидаемой пользы и необходимости дальнейшего расширения инициатив. Пилотная программа «Три Банка» (Вставка 4.1 в Разделе 4) была запущена в Великобритании после первичных тестовых испытаний в рамках регулятивной

песочницы, проведённых учреждением, отвечающим за обработку персональных данных, и государственным органом, отвечающим за ЗДЛЖ, что позволило оценить ключевые аспекты, касающиеся защиты данных. Эта пилотная программа позволила участникам оценить результаты и рассмотреть возможности для усовершенствования в рамках будущих проектов. Примеры, касающиеся пилотных проектов ПБКБФД и ЕвроДаТ в Германии (Вставки 4.7 и 4.8 в Разделе 4), демонстрируют включение моделей ПОД/ФТ в более широкие государственные инициативы для пилотного тестирования цифровых моделей в целях обмена информации с соблюдением требований ЗДЛЖ. Пример, касающийся проекта «Мост для ПОД» в Эстонии (Вставка 4.6 в Разделе 4), также демонстрирует участие государственных органов в создании и реформировании государственных систем управления данными. **Органам, отвечающим за ПОД/ФТ, следует взаимодействовать с другими заинтересованными сторонами (в том числе с органами, отвечающими за выработку и реализацию политики в области инноваций, технологий или цифровизации, или с научным/экспертным сообществом) для понимания современных тенденций, а также содействовать реализации более широких пилотных программ по обмену информацией для рассмотрения вариантов их использования в целях ПОД/ФТ.**

- **Разработать национальную стратегию в области обмена информацией в целях ПОД/ФТ/ФРОМУ.** В этой стратегии должны быть определены финансовые преступления или типологии, которым следует уделять приоритетное внимание, или ключевые виды данных, обмен которыми будет наиболее полезным (например, с участием правоохранительных органов и ПФР). Это будет являться своего рода руководством для заинтересованных учреждений частного бизнеса при разработке инициатив по обмену информацией в соответствии с национальной стратегией ПОД/ФТ/ФРОМУ или с учётом результатов национальных оценок рисков. Например, проект КОСМИК в Сингапуре показывает, как обмен информацией направлен на снижение рисков в трёх приоритетных областях, определённых по результатам национальной оценки рисков и в стратегии ПОД/ФТ/ФРОМУ (Вставка 4.2 в Разделе 4). Аналогичным образом, проект по обмену информацией МОН в Нидерландах непосредственно соотносится с Национальным планом действий по противодействию отмыванию денег, который включает национальные инициативы по расширению обмена данными в целях более активного расследования и судебного преследования за мошенничество и легализацию преступных доходов (Вставка 4.3 в Разделе 4)[41].

- **Определить ведущее или координационное ведомство и создать контактный механизм по вопросам обмена информацией между заинтересованными субъектами частного бизнеса.** Например, это можно осуществить с помощью существующих контактных механизмов или форумов, в рамках которых осуществляется взаимодействие заинтересованных сторон, таких как механизмы государственно-частного партнёрства. Такой контактный центр должен участвовать в установлении связи и поддержании диалога с государственным органом, отвечающим за ЗДЛЖ, и другими государственными органами, например, отвечающими за внедрение цифровых инноваций, с целью выработки согласованных рекомендаций для заинтересованных субъектов частного сектора. Тес-

[41] www.rijksoverheid.nl/documenten/kamerstukken/2019/06/30/plan-van-aanpakwitwassen

ное взаимодействие также поможет определить, приводит ли инициатива по обмену информацией к любому переносу рисков на не участвующие в инициативе учреждения и позволяет ли государственным органам реагировать на такие риски (например, путём содействия участию в инициативе всех регулируемых субъектов). Обсуждения в рамках фокус-групп показали, что степень участия государственных органов может быть различной. Например, проект КОСМИК в Сингапуре (Вставка 4.2 в Разделе 4) показывает, как компетентный орган в сфере ПОД/ФТ/ФРОМУ (Денежно-кредитное управление, являющееся надзорным органом) возглавил разработку инициативы по обмену информацией. В примере, касающемся Великобритании (Вставка 4.1 в Разделе 4), показано, как орган, отвечающий за ЗДЛЖ (Управление уполномоченного по информации Великобритании), сыграл активную роль в налаживании взаимодействия с инициатором предложения по обмену информацией. В рамках проекта «Мост для ПОД» в Эстонии (Вставка 4.6 в Разделе 4), ряд эстонских государственных органов (в том числе, орган, отвечающий за ЗДЛЖ, подразделение финансовой разведки и орган финансового надзора) являются членами руководящего комитета и/или выступают в качестве консультантов в рамках этой инициативы.

- **Предоставлять руководства, контрольные перечни или другие справочные материалы, содержащие соответствующие законодательные/надзорные положения, регулирующие обмен информацией.** Это поможет учреждениям частного сектора разобраться в различных требованиях, установленных на национальном уровне. Обратная связь, получаемая от субъектов частного бизнеса, указывает на то, что руководства или пояснительные материалы также помогают прояснить степень любых исключений, особенно если это касается ОД. Например, если обмен информацией разрешён в целях выявления и расследования случаев мошенничества, то в какой степени учреждения могут обмениваться информацией, касающейся отмывания доходов от такого мошенничества. Или, наоборот, если обмен информацией разрешён в целях выявления и расследования случаев отмывания денег, то в какой степени учреждения могут обмениваться информацией, касающейся предикатных преступлений. В случае выпуска руководств органы, отвечающие за ПОД/ФТ/ФРОМУ и за ЗДЛЖ, должны обеспечить, чтобы такие руководства были последовательными и согласованными, а не разрабатывались по отдельности. Например, органы власти Эстонии, отвечающие за ПОД/ФТ/ФРОМУ и за ЗДЛЖ, выступают в качестве консультантов в рамках инициативы по обмену информацией «Мост для ПОД» и являются членами руководящей группы наряду с командой по управлению продуктом и другими субъектами частного бизнеса, также входящими в состав руководящей группы (Вставка 4.6 в Разделе 4). Если это разрешено в соответствии с действующим законодательством, государственные органы могут также рассмотреть возможность сертификации конкретных систем обработки данных помимо выпуска руководств. Например, в Нидерландах система предупреждения о возможных случаях мошенничества СПП функционирует на основании сертификата, выданного органом, отвечающим за защиту данных (Вставка 4.4 в Разделе 4). Аналогичным образом, Закон Канады о защите персональных данных потребителей даёт Управлению уполномоченного по защите частной информации возможность утверждать кодекс норм и правил, касающийся систем обработки данных.

- **Рассмотреть практическую возможность создания защищённой платформы для обмена информацией между субъектами частного бизнеса.** Это является самым прямым подходом к предоставлению необходимых финансовых и технологических ресурсов для обмена информацией. Этот подход также может помочь обеспечить приемлемость и доступность инициатив по обмену информацией для более мелких учреждений, в том числе учреждений нефинансового сектора. А это, в свою очередь, снижает вероятность переноса рисков, при которой инициативы по обмену данными ограничены только крупными учреждениями. Такая платформа может также создать условия и возможности для обмена информацией между государственным и частным сектором или для использования в целях трансграничного обмена информацией в долгосрочной перспективе (хотя в настоящее время это не является требованием Стандартов ФАТФ, за исключением обмена информацией в рамках финансовых групп). Например, в рамках проекта КОСМИК в Сингапуре (Вставка 4.2 в Разделе 4) и проекта «Мост для ПОД» в Эстонии (Вставка 4.6 в Разделе 4) используются защищённые цифровые платформы, которые позволяют (или позволят) поддерживать связь и обмениваться информацией между участвующими в этих проектах финансовыми учреждениями. В рамках проектов ПБКБФД и ЕвроДаТ в Германии (Вставки 4.7 и 4.8 в Разделе 4) государственные органы активно участвуют в инициативах с целью разработки платформы или создания доверительного хранителя данных для обеспечения возможности обмена информацией. При разработке таких платформ государственные органы и участники могут рассмотреть возможность использования стандартизированных или общедоступных технологий с целью обеспечения защиты данных и/или использования технологий, отвечающих государственным сертификационным требованиям, для укрепления доверия в безопасности данных.
- **Разработать проекты для обеспечения совместимости и согласованности данных.** Такие инициативы могут включать внедрение единых стандартов и определений, касающихся данных, или иные инициативы по очистке или структурированию данных для передачи информации в целях ПОД/ФТ/ФРОМУ или записей в СПО. Такие инициативы, реализуемые под руководством органов, отвечающих за ПОД/ФТ/ФРОМУ (например, надзорных органов или ПФР), и органов, отвечающих за цифровые инновации, могут сэкономить время и усилия на подготовку данных. Кроме того, они могут также обеспечить более быструю реализацию инициатив по обмену информацией заинтересованными учреждениями частного сектора. Исходя из опыта, полученного из практических примеров, в некоторых странах (например, в Сингапуре) проводились отдельные испытания в целях гармонизации форматов данных в течение нескольких лет перед началом практической реализации инициатив по обмену информацией.

Государственным учреждениям следует обеспечить и содействовать диалогу между органами, отвечающими за ЗДЛЖ, и органами, отвечающими за ПОД/ФТ/ФРОМУ

54. Помимо вышесказанного, регулярный открытый диалог между органами, отвечающими за ЗДЛЖ, и органами, отвечающими за ПОД/ФТ/ФРОМУ (и другими органами, отвечающими за регулирование финансовых услуг), является важным для предоставления заинтересованным субъектам частного бизнеса

большей ясности относительно того, как достичь гармонизации политических целей и задач на практике. В рамках многих более продвинутых инициатив по обмену информацией, рассмотренных в предыдущем Разделе, ведущие органы, отвечающие за ПОД/ФТ/ФРОМУ, привлекли или пригласили своих коллег, отвечающих за ЗДЛЖ, к участию в регулярных совещаниях для обсуждения решений или других мер, направленных на содействие реализации инициатив по обмену информацией в частном секторе, а также для определения областей, в которых имеют место потенциальные противоречия или неясности. Как указано в Аналитическом отчёте по итогам 1 этапа проекта и в Рекомендации 2 ФАТФ, для сотрудничества и координации в целях ПОД/ФТ/ФРОМУ на национальном уровне требуется взаимодействие между органами, отвечающими за ПОД/ФТ/ФРОМУ, и органами, отвечающими за ЗДЛЖ, в целях обеспечения совместимости требований ПОД/ФТ/ФРОМУ с правилами ЗДЛЖ или другими аналогичными нормами. Такой диалог также играет важную роль в образовательных целях с тем, чтобы органы, отвечающие за противодействие отмыванию денег, понимали охват, характер и важность целей и задач соответствующих нормативно-правовых актов в сфере ЗДЛЖ, и наоборот.

55. Сотрудничество и взаимодействие на международном уровне (как двустороннее, так и многостороннее) может содействовать обмену опытом и проведению обсуждений, а также обеспечить последовательность и согласованность трансграничного обмена информацией в соответствии с требованиями о защите данных. Помимо такого оперативного сотрудничества, информационно-разъяснительная работа и консультации, проводимые государственными органами, могут быть распространены на соответствующие группы гражданского общества (например, на НКО или другие организации, занимающиеся вопросами защиты данных и конфиденциальности или вопросами охвата финансовыми услугами всех слоев населения), чтобы убедить их в том, что принципы ЗДЛЖ будут соблюдаться при выполнении задач ПОД/ФТ/ФРОМУ, а также развеять любые опасения по поводу того, что обмен информацией приведёт к лишению определённых слоев общества доступа к финансовым услугам.

56. Другие практические соображения относительно взаимодействия государственных органов включают следующее:

- **Проведение регулярных форумов с участием представителей органов, отвечающих за ПОД/ФТ/ФРОМУ, органов, отвечающих за ЗДЛЖ, и учреждений частного бизнеса** для обсуждения политических и операционных вопросов, касающихся ПОД и ЗДЛЖ. Обмен мнениями по техническим и операционным проблемам позволит государственным органам разумно подойти к решению этих проблемных вопросов. Такие форумы также способствуют укреплению взаимоотношений между разными заинтересованными сторонами и содействуют расширению знаний о нормативно-правовых актах и задачах друг друга.

- Помимо обсуждения политических вопросов на высоком уровне, **органы, отвечающие за ПОД/ФТ/ФРОМУ и за ЗДЛЖ, могут также реализовывать совместные инициативы, такие как создание совместных регулятивных песочниц,** которые позволят участникам разобраться во взаимосвязи между законодательством в сфере ПОД/ФТ/ФРОМУ и законодательством в области ЗДЛЖ. Это также может помочь выработать общие руководства по вопросам взаимосвязи между законодательством в области ЗДЛЖ и законодательством в сфере ПОД/ФТ/ФРОМУ.

- Для продвижения отраслевых инициатив, **органы, отвечающие за ПОД/ФТ/ФРОМУ, могут разработать совместно с органами, отвечающими за ЗДЛЖ, стратегию информационного обмена** и содействовать обмену информацией в частом секторе с использованием надлежащих мер защиты (в плане цифровой безопасности, а также защиты данных и личной жизни).

- **Органы, отвечающие за ЗДЛЖ, могут предоставлять руководящие указания или оказывать иную поддержку,** например, в плане разработки технологических решений для обмена информацией, которые позволяют снижать риски несанкционированного раскрытия данных/нарушения конфиденциальности (например, сведение к минимуму объёма передаваемых персональных данных или обеспечение псевдонимизации данных). Они также могут проводить консультационные мероприятия в масштабе сектора по вопросам обмена данных для обеспечения целостного и комплексного понимания требований, касающихся защиты данных и конфиденциальности.

- **Органы, отвечающие за ПОД/ФТ/ФРОМУ, и органы, отвечающие за ЗДЛЖ, могут рассмотреть возможность выпуска совместных руководств,** указаний или иных информационных материалов для обеспечения большей гармонизации политики. Если в странах используются законодательные положения, разрешающие раскрытие непубличной информации, то органы, отвечающие за ПОД, должны тесно взаимодействовать с органами, отвечающими за ЗДЛЖ, в целях обеспечения согласованности законов и нормативных требований.

- **Органам, отвечающим за ПОД, следует содействовать развитию и расширению взаимодействия между субъектами отрасли и органами, отвечающими за ЗДЛЖ,** при необходимости. Может оказаться полезным включить вопросы, касающиеся защиты данных и конфиденциальности, в повестку консультационных форумов с субъектами частного бизнеса или иных секторальных мероприятий.

Рекомендации для субъектов частного бизнеса

Субъектам частного бизнеса следует рассмотреть целесообразность использования технологий, повышающих конфиденциальность

57. Технологии, повышающие конфиденциальность (технологии ТПК) могут содействовать соблюдению требований ЗДЛЖ, хотя они и не являются «волшебной палочкой», обеспечивающей выполнение этих правовых обязательств. Например, они могут способствовать снижению или прекращению перемещения данных, минимизации объема передаваемых персональных данных, а также обеспечить псевдонимизацию, обезличивание или зашифровку передаваемых данных. В Аналитическом отчёте по итогам 1 этапа проекта подробно рассмотрены виды технологий, которые могут применяться в этих целях, а также связанные с ними риски и возможности. Как указано в предыдущем Разделе, могут возникать проблемы, связанные с объёмом доступных и обрабатываемых данных, точностью и надёжностью таких данных, а также с хранением этих данных в стандартных форматах соответствующими заинтересованными сторонами. Привлечение экспертов в области ПОД/ФТ/ФРОМУ, разработчиков технологий и специалистов, занимающихся вопросами защиты данных и личной жизни, к любым обсуждениям инициатив по обмену информацией может содействовать обеспечению соответствия

технических решений и результатов таких инициатив установленным целям и задачам. Это включает обеспечение того, чтобы используемые технологии ТПК соответствовали целевому назначению, а также обеспечение надлежащего управления рисками, связанными с защитой данных[42]. Технологии ТПК также должны быть доступны для более мелких учреждений, которые составляют большинство подотчётных субъектов. Например, в Великобритании в платформе FutureFlows (Вставка 4.1 в Разделе 4) используются технологии псевдонимизации для удаления/очистки персональных данных, содержащихся в сведениях о финансовых операциях (таких как идентификационные номера счетов, суммы операций, идентификационные номера операций и временные метки), перед передачей данных для минимизации риска повторной идентификации. При рассмотрении возможностей применения технологий ТПК важно обратить внимание на совместимость разных технологий (например, использовать технологии, которые соответствуют признанным стандартам). Технологии повышения конфиденциальности и искусственного интеллекта, при условии их надлежащего использования в соответствии с правилами и обязательствами ЗДЛЖ, могут потенциально обеспечить более точную, надёжную, объективную и безопасную обработку данных.

Субъектам частного бизнеса следует принять меры для подготовки данных

58. Новые технологии, касающиеся объединения и обмена данными, особенно инструменты углублённого анализа данных, являются наиболее эффективными в применении при наличии единых стандартов и форматов данных. Взаимно совместимые структуры и форматы данных могут также содействовать повышению точности и надёжности данных, позволяя тем самым устранить некоторые проблемы, касающиеся данных, отмеченные в предыдущем Разделе. Учреждения частного бизнеса могут рассмотреть ряд стратегий, в том числе: использование имеющихся доступных данных в структурированном формате (например, таких как поля данных в сообщениях SWIFT); реализацию инициатив по очистке данных перед началом обмена информацией; или привлечение разработчиков технологий для планирования и реализации инициатив по очистке/ структурированию данных (особенно, если такие разработчики являются участниками инициатив по обмену информацией). В Великобритании в рамках инициативы «Три банка» (Вставка 4.1 в Разделе 4) финансовые учреждения потратили значительное количество времени на начальных этапах проекта для обеспечения того, чтобы все участники имели возможность беспрепятственно обмениваться данными с использованием цифровой платформы. В примере, касающемся проекта «Мост для ПОД» в Эстонии (Вставка 4.6 в Разделе 4), также отмечено, что было потрачено значительное количество времени и усилий на решение менее заметных трудностей и проблем, таких как подготовленность данных.

Субъектам частного бизнеса следует решать вопросы, касающиеся защиты данных, на стадии разработки

59. Учет принципов ЗДЛЖ на стадии разработки инициатив по обмену информацией является ключом к успеху. Поэтому оценки рисков нарушения конфиденциальности и/или оценки воздействия на защиту данных (ОВЗД) обеспечивают аналитическую основу, которая может помочь заинтересованным сторонам оценить степень выполнения требований ЗДЛЖ, а также выявить и снизить потенциальные риски, связан-

[42] См. Агентство Европейского союза по кибербезопасности (2021г.) «*Data Pseudonymisation: Advanced Techniques and Use Cases*» (Псевдонимизация данных: передовые методы и примеры использования); Агентство Европейского союза по кибербезопасности (2019г.) «*Pseudonymisation techniques and best practices*» (Методы псевдонимизации и передовая практика).

ные с ЗДЛЖ (см. Вставку ниже). Примеры более продвинутых инициатив также указывают на то, что правовая основа для обмена/обработки/хранения персональных данных и предусмотренные меры по снижению рисков должны соответствовать целям и задачам проекта и целям использования/обработки данных. В этой связи также следует проводить надлежащую оценку соответствующей правовой базы при необходимости. В большинстве случаев каждому отдельному финансовому учреждению потребуется провести собственную оценку воздействия на защиту данных с учётом собственной политики, касающейся сбора и обработки данных. Однако ОВЗД могут проводиться совместно участвующими в инициативах учреждениями, но также с учётом различий между учреждениями[43]. В рамках одного из описанных выше проектов ведущий участник (провайдер цифровой платформы) провёл консультации с органом, отвечающим за ЗДЛЖ, и разработал модель ОВЗД для снижения нагрузки на финансовые учреждения, участвующие в этом проекте[44]. Учёт вопросов, касающихся защиты данных, на начальном этапе проекта также позволяет участникам вносить изменения и коррективы в проекты с тем, чтобы они соответствовали установленным требованиям ЗДЛЖ, и тем самым экономить ресурсы.

Вставка 6.1: Что должна включать в себя оценка воздействия на защиту данных (ОВЗД)?

Конкретные требования в ОВЗД будут зависеть от соответствующего законодательства в области ЗДЛЖ и особенностей инициативы (инициатив) по обмену информацией, но могут включать следующее:

- Конкретные цели и задачи проекта.
- Определение правовых полномочий/оснований, разрешающих или обязывающих субъектов участвовать в таких схемах по выявлению и расследованию ОД/ФТ/ФРОМУ, и тщательная проверка условий, соответствующих правовым основаниям.
- Анализ того, могут ли другие схемы обеспечить достижение аналогичных результатов или установленных целей проекта.
- Уточнение того, какие стороны (участники) выполняют ключевые функции в отношении используемых данных (например, кто отвечает за контроль данных, совместный контроль данных и/или обработку данных), и учёт любых договоров между контроллерами и обработчиками данных.
- Описание того, как стороны (участники) будут осуществлять сбор, использование, раскрытие/передачу, хранение и последующее удаление или уничтожение данных.
- Определение конкретных единиц/элементов данных, которые будут передаваться, объединяться, анализироваться или иным образом обрабатываться для проекта, в том числе будут ли данные псевдонимизированы или обезличены на любом этапе проекта, и, если да, то возможна ли повторная идентификация, и если да, то когда и каким субъектом. При этом особое внимание следует уделить чувствительным

[43] В некоторых юрисдикциях на государственные органы также может быть возложена обязанность представлять отчёты об оценке воздействия на защиту данных, в зависимости от их роли и участия в инициативах по обмену информацией.

[44] Пример оценки воздействия на защиту данных в рамках платформы FutureFlow (Вставки 4.2 в Разделе 4) размещён на вебсайте ФАТФ.

данным или данным, отнесённым к специальной категории (в соответствии с действующей нормативно-правовой базой с области ЗДЛЖ).

- Наличие единых стандартов данных и совместимость данных.
- Как обеспечить необходимое качество, точность и достоверность данных в контексте инициативы и как минимизировать объём данных. В соответствии с принципами минимизации объёма передаваемых данных, в рамках инициатив может быть с самого начала использован дифференцированный подход при условии, что передаваемые данные являются надлежащими и достаточными для достижения целей информационного обмена. Например, учреждения могут рассмотреть модели или варианты, представляющие пониженный риск, в качестве тестовых проектов и затем расширять эти модели в той степени, в которой это необходимо и разрешено, исходя из их эффективности. Соблюдение принципа адекватности наряду с соответствующей минимизацией объёма данных может содействовать обеспечению эффективного обмена данными.
- Как будет осуществляться обмен или объединение и/или анализ или обработка данных.
- Если данные будут совместно объединяться или передаваться, как будет гарантирована защищённость данных с момента их исходного объединения в банк данных, в процессе их использования в банке и до момента их удаления/уничтожения в соответствующих случаях, а также в случае потери или несанкционированного раскрытия данных. Описание мер по снижению рисков, включая порядок уведомления соответствующих государственных органов и, возможно, субъектов данных, которые могут пострадать.
- Составление схемы потоков данных в целях чёткого понимания.
- Последствия для трансграничной или международной передачи данных.
- Риски нарушения конфиденциальности, представляемые схемой, и меры по снижению этих рисков.
- Любые последствия для уязвимых или маргинализированных (социально отчужденных) групп.
- Меры (например, техническое, правовые или организационные меры защиты) по снижению рисков, связанных с использованием новых технологий в отношении физических лиц, включая следующее:
  - Меры, которые могут быть или будут реализованы для минимизации рисков случайных совпадений.
  - Меры, направленные на снижение потенциального негативного воздействия на физических лиц (например, меры, необходимые для обеспечения недопущения несправедливого лишения физических лиц доступа к услугам и обеспечения их права на обжалование).
  - Другие меры, направленные на снижение рисков, касающихся нарушения прав/свобод субъектов данных.
- Вопросы, касающиеся прозрачности и предоставления данных физическим лицам, включая то, как не допустить нарушение запретов на предупреждение.

60. Помимо проведения оценки воздействия на защиту данных, субъекты, участвующие в проектах по обмену информацией, могут рассмотреть возможность:

- Заключения соглашений/договоров по обмену данными, в которых определены обязанности каждого участника, включая чёткую схему рассмотрения претензий клиентов и обеспечения соблюдения прав физических лиц (включая в рамках соответствующих законов в области ЗДЛЖ).

- Проведение оценки воздействия на права человека (ОВПЧ). Такая оценка обеспечит действенный механизм снижения рисков для физических лиц и обеспечит выполнение всеми субъектами обязательств, касающихся соблюдения прав человека (таких как право на конфиденциальность), например, в рамках инициатив по обмену информацией, включающих мониторинг с помощью искусственного интеллекта[45].

- Проведение оценки законных интересов (в случае, когда обмен данными осуществляется в «законных интересах»; см. Раздел 3). Это поможет контроллерам данных определять законный интерес, устанавливать, необходима ли обработка данных для соблюдения законного интереса, и затем обеспечивать баланс таких законных интересов и интересов, прав и свобод субъектов данных.

Субъектам частного бизнеса следует осуществлять постоянное взаимодействие с органами, отвечающими за ЗДЛЖ, начиная с самых ранних этапов

61. Участие органов, отвечающих за ЗДЛЖ, с самого начала реализации любого проекта по обмену информацией часто является критически важным и полезным для успеха проектов по обмену информацией в частном секторе в целях ПОД/ФТ/ФРОМУ. Регулярная и прозрачная связь с соответствующими органами, отвечающими за ЗДЛЖ, может помочь в решении неожиданно возникающих проблем и в оценке любых новых рисков по мере их появления. В идеале такое взаимодействие должно начинаться на этапе, когда финансовые учреждения разрабатывают подход к сотрудничеству и повышению эффективности выявления случаев ОД/ФТ/ФРОМУ, продолжаться в процессе подготовки и проведения оценки воздействия на защиту данных, а также осуществляться на постоянной основе по мере реализации проекта и начала сбора и анализа данных. Участие органов, отвечающих за ПОД/ФТ/ФРОМУ, также может являться важным для успеха инициатив, реализуемых под руководством субъектов частного бизнеса. Например, в Великобритании государственные органы, такие как Управление по финансовому регулированию и надзору, обязаны проконсультироваться с органом, отвечающим за обеспечение защиты данных, при разработке законодательных мер, предусматривающих обработку персональных данных (Статья 36(4) Общего регламента защиты данных Великобритании). Это обеспечивает возможность заблаговременного выявления рисков и принятия соответствующих мер для снижения этих рисков. В Эстонии в рамках инициативы по обмену информацией (проект «Мост для ПОД»: Вставка 4.6 в Разделе 4) органы, отвечающие за ЗДЛЖ, были привлечены к проекту и предоставляли консультации в качестве членов руководящей группы. На ранних этапах проекта совещания руководящей группы проводились каждые две недели для получения оперативной обратной связи, что позволило своевременно вносить поправки и коррективы в разработку инициативы по обмену информацией.

[45] См. Датский институт по правам человека (2020г.), Руководство по оценке воздействия цифровой деятельности на права человека.

Субъектам частного бизнеса следует разработать параметры и показатели для оценки успеха

62. Определение чётких показателей или параметров для оценки результатов и успеха является важным для обеспечения того, чтобы инициативы по обмену информацией достигли своих целей. Например, на момент завершения подготовки настоящего Отчёта участники проекта КОСМИК (Вставка 4.2 в Разделе 4) обсуждали конкретные ключевые показатели результативности для оценки успешности проекта. Эти показатели включали: количество направленных СПО/количество клиентов, с которыми были прекращены деловые отношения/ количество лиц, которым было отказано в приёме на обслуживание, на основании информации, получаемой с использованием защищённой цифровой платформы КОСМИК; своевременность принятия мер реагирования и выявления подозрительных сетей; количество эпизодов, выявленных, благодаря проекту КОСМИК, в отношении которых правоохранительными органами впоследствии были осуществлены расследования/ судебные преследования и т.д. Сбор чёткой качественной и количественной информации позволяет участникам определить, достигает ли инициатива своей цели, и постоянно по новой оценивать, является ли обмен информацией необходимым/разумным/соразмерным. Обнародование положительных результатов также содействует повышению доверия к инициативам и может помочь привлечению более широкого круга участников (если это соответствует правилам ЗДЛЖ).

Субъектам частного бизнеса следует принять меры для недопущения отказа в обслуживании под предлогом снижения рисков на основании обмена информацией

63. Данные, получаемые в рамках инициатив по обмену информацией, могут, в конечном итоге, сыграть роль в решении учреждений прекратить деловые отношения или не предоставлять определённые услуги в целях управления рисками ОД/ФТ/ФРОМУ. Если такие решения не принимаются отдельно в каждом конкретном случае или не основаны на дополнительных надёжных источниках информации, это может привести к нежелательному отказу в обслуживании под предлогом снижения рисков. В идеале надлежащее соблюдение требований ЗДЛЖ, особенно касающихся автоматического принятия решений, качества и точности данных и прав граждан на исправление неправильных/неточных данных, может помочь снизить эти риски. Каждое отдельное учреждение должно нести ответственность за принятие таких решений и проводить собственные расследования для принятия решений (например, финансовое учреждение само определяет, следует ли направить СПО или нет). Механизмы обмена информацией могут помочь в процессе принятия решений, но не должны использоваться для передачи полномочий на принятия решений третьим сторонам. Учреждениям, участвующим в инициативах по обмену информацией в частном секторе, необходимо заранее определить соответствующие процедуры и пороговые показатели для реализации мер по прекращению деловых отношений. Однако при этом им следует проявлять особую осмотрительность и осторожность, учитывая потенциальный вред и ущерб для клиентов, которые ошибочно установлены в рамках инициатив по обмену информацией в частном секторе.

ПРИЛОЖЕНИЕ А:
Дополнительная информация о требованиях ПОД/ФТ/ФРОМУ

64. Как подчеркивается в основном отчете, некоторые участники инициатив частного бизнеса по обмену информацией могут быть не знакомы с международными и национальными требованиями в области ПОД/ФТ/ФРОМУ. Целью данного Приложения является предоставление справочных сведений о Стандартах ФАТФ с точки зрения обмена информацией. Эти сведения шире, чем обмен информацией с частным бизнесом с целью выявления подозрительных операций, и охватывают целый ряд его форм, применимых для различных целей ПОД/ФТ/ФРОМУ.

Введение в стандарты ФАТФ, относящиеся к частному бизнесу (превентивные меры)

65. В целях соответствия Стандартам ФАТФ, страны должны возложить на частный бизнес[46] конкретные обязательства по снижению рисков ОД/ФТ – в совокупности известные как превентивные меры и включающие в себя Рекомендации ФАТФ с 9 по 23. Превентивные меры направлены на предотвращение, выявление и сообщение о клиентах и операциях, в отношении которых имеются подозрения в отмывании денег, в связи с предикатными преступлениями и финансировании терроризма. В целом, превентивные меры требуют от частного сектора следующее:

- понимать характер и уровень рисков ОД/ФТ и применять политики, правила внутреннего контроля и программы ПОД/ФТ, необходимые для адекватного снижения этих рисков (Р.1);

- знать, кто является их клиентами, и контролировать их счета и деятельность в целях ПОД/ФТ (Р. 10). Это предполагает применение мер по надлежащей проверке клиентов (НПК) для выявления и проверки личности клиентов (выполнение процедуры "Знай своего клиента" (ЗСК)) в момент установления с ними деловых отношений. От субъектов частного бизнеса также требуется понимание цели и предполагаемого характера деловых отношений с клиентом. Важно отметить, что НПК также включает в себя проведение постоянной комплексной проверки деловых отношений и тщательный анализ операций, осуществляемых в ходе этих отношений, чтобы исключить их неправомерное использование в целях ОД/ФТ.

- уметь выявлять подозрительные операции и сообщать о них (Р. 20), а также соблюдать другие требования ПОД/ФТ. Финансовые учреждения располагают соответствующими данными об операциях и, как правило, используют системы мониторинга операций (с автоматическими индикаторами риска) для выяв-

[46] Это относится к финансовым учреждениям, установленным нефинансовым предприятиям и профессиям (УНФПП) и провайдерам услуг виртуальных активов (ПУВА). Более подробную информацию см. в Глоссарии ФАТФ.

ления подозрительных операций в рамках своего учреждения. По мере усложнения деятельности, связанной с ОД/ФТ, способность этих систем эффективно выявлять масштабные или сложные схемы уменьшается при отсутствии цифровизации, машинного обучения и более широкого обмена информацией.

- хранить записи о НПК и другую информацию об операциях в течение, по крайней мере, 5 лет (Р.11), чтобы обеспечить возможность проведения расследований правоохранительными органами, поскольку финансовые преступления часто трудно обнаружить, а расследования могут занимать много времени при выявлении сложных сетей.

- гарантировать, что клиенты не будут проинформированы о том, что сообщение о подозрительной операции (СПО) или связанная с ним информация направляются в компетентные органы (Р. 21). Эти положения не преследуют цели воспрепятствовать усилиям частного бизнеса по обмену информацией, но конфиденциальность СПО гарантирует, что потенциальные преступники не будут предупреждены о проведении правоохранительными органами расследования, преследования и пресечения деятельности, связанной с ОД/ФТ. Данная рекомендация также обеспечивает безопасные условия для финансовых учреждений и их представителей в их добросовестных усилиях по сообщению о подозрительных операциях.

66. В целях выполнения своих обязательств по ПОД/ФТ частный бизнес обязан собирать, хранить и передавать соответствующие данные и информацию для выявления подозрительной деятельности, связанной с ОД/ФТ, и сообщения о них компетентным органам (при этом следует отметить, что органы власти, ответственные за ПОД/ФТ и за ЗДЛЖ, обязаны обеспечить соответствие этих данных требованиям как ПОД/ФТ, так и ЗДЛЖ). Такие данные и информация должны храниться надлежащим образом и передаваться по защищенным каналам связи (1) государственному сектору (т.е. надзорным и правоохранительным органам внутри страны и в некоторых случаях на международном уровне) и (2) частному сектору (т.е. внутри группы/зарубежным филиалам, другим финансовым учреждениям или установленным нефинансовым предприятиям или профессиям в стране) для своевременного и эффективного пресечения деятельности, связанной с ОД/ФТ. ФАТФ недавно разъяснила, что обмен информацией особенно необходим в контексте групповых программ по противодействию ОД/ФТ для выявления и сообщении о сложных профессиональных сетях отмывания денег, осуществляющих свою деятельность в разных организациях и юрисдикциях с целью содействия коррупции, незаконному обороту наркотиков и уклонению от уплаты налогов[47].

Стандарты ФАТФ по обмену информацией в рамках противодействия ОД, ФТ и ФРОМУ

Обмен данными по ПОД/ФТ/ФРОМУ между представителями частного сектора

67. ФАТФ ранее выпустила Руководство по типам данных и обмену информацией **внутри финансовых групп**, необходимое для эффективного применения риск-ориентированного подхода[48]. В таблице ниже подробно описаны типы информации, которой обмениваются внутри финансовых групп, и разъясняются конкретные цели ПОД/ФТ, которые преследует такой обмен.

---

[47] ФАТФ опубликовала Руководство по обмену информацией и применению стандартов ФАТФ в рамках групповых программ противодействия ОД/ФТ для финансовых учреждений и УНФПП.

[48] Руководство ФАТФ по обмену информацией в частном секторе (ноябрь 2017 г.)

Таблица A1. Типы информации, которой обмениваются внутри финансовых групп в целях ПОД/ФТ/ФРОМУ

Типы информации	Примеры элементов информации (при наличии, по мере необходимости)	Цели ПОД/ФТ/ФРОМУ для обмена информацией внутри группы
Информация о клиенте	Идентификационные и контактные данные клиента (имя и идентификатор), для юридических лиц и юридических образований: информация о характере деятельности и структуре собственности и контроля; организационно-правовая форма и доказательство существования; адрес зарегистрированного офиса и основного места ведения бизнеса; информация об идентификаторе юридического лица (LEI), данные о финансовых активах, налоговые документы, сведения о владении недвижимостью, источнике средств и богатства, экономической/профессиональной деятельности, досье счета, является ли клиент ПДЛ (включая близкое окружение или членов семьи) или нет, а также другие соответствующие элементы информации из документов, собранных при принятии клиента на обслуживание или обновлении записей, сведения о целевых финансовых санкциях и любая неблагоприятная информация, полученная из открытых источников или в ходе внутреннего расследования, связанная с ОД/ФТ, категоризацией клиентского риска и т.д.	Управление клиентскими и географическими рисками, выявление глобальных рисков в результате принятия на обслуживание одного и того же клиента несколькими организациями в рамках группы, более эффективное ведение учета информации о клиентах.
Информация о бенефициарных владельцах	Идентификационные и контактные данные бенефициарного владельца, сведения о владении недвижимостью, источнике средств и благосостоянии, экономической/профессиональной деятельности, досье счета, является ли бенефициарный владелец ПДЛ или нет, а также другие соответствующие элементы информации из документов, собранных при принятии клиента на обслуживание или обновлении записей.	Управление рисками, связанными с бенефициарными владельцами, и географическими рисками, идентификация одного и того же бенефициарного владельца нескольких организаций в рамках группы, более эффективное ведение учета информации о бенефициарных владельцах.
Информация о счете	Данные банковского/другого счета, включая целевое назначение счета, предполагаемое место проведения операций/деятельности по заявлению клиента, деловую переписку и т.д.	Эффективная комплексная проверка и мониторинг операций на уровне группы, обоснование шаблона операции в зависимости от финансового профиля, последующие действия в отношении любых оперативных оповещений или подозрительных торговых моделей в рамках группы.
Информация о финансовых операциях	Записи о финансовых операциях, данные об использовании кредитных и дебетовых карт, кредитная история, цифровой след (IP-адрес, информация об использовании банкоматов и т.д.), информация о попытках осуществления операций /неудачных операциях, отчеты о валютных операциях, информация о закрытии счета или прекращении деловых отношений в связи с возникшими подозрениями, анализ, проведенный с целью выявления необычных или подозрительных операций, и т.д.	Глобальный мониторинг финансовых операций, обработка оперативных оповещений и выявление подозрительных операций, представление сообщений и проверка наличия аналогичного поведения по всем направлениям деятельности в рамках группы.

68. ФАТФ требует, чтобы "существовали адекватные гарантии конфиденциальности при использовании информации, которой обмениваются, в том числе для предотвращения ее разглашения. Страны могут определять объем и степень такого обмена информацией, исходя из чувствительности информации и ее значимости для управления рисками ПОД/ФТ"[49]. Приведенная выше таблица иллюстрирует типы данных и обмен информацией внутри финансовых групп, однако эти типы данных могут также использоваться для обмена информацией между финансовыми учреждениями и финансовыми группами, известного как обмен данными по ПОД/ФТ/ФРОМУ между представителями частного сектора. Транснациональный характер деятельности, связанной с ОД/ФТ/ФРОМУ, как правило, может быть более эффективно выявлен и смягчен путем обмена информацией и скоординированных проверок, осуществляющихся несколькими ФУ и финансовыми группами.

Государственно-частные партнерства

69. Аналогичным образом, обмен информацией между представителями государственного и частного секторов в рамках государственно-частного партнерства (ГЧП) повышает эффективность мер по ПОД/ФТ/ФРОМУ за счет получения более полного представления об операциях и поведении клиентов. Такой обмен информацией часто происходит в защищенной среде, что позволяет частному сектору проводить дальнейшую обработку данных, оперативный анализ и сканирование для заполнения потенциальных пробелов в оперативной информации. Такие ГЧП позволяют обмениваться информацией между надзорными органами, ПФР, правоохранительными органами, контролируемыми представителями частного сектора, а в некоторых случаях и международными партнерами. Они подчеркивают некоторые из ощутимых преимуществ объединения информации, поступающей от представителей частного сектора, при расследовании серьезных преступлений.

70. В июле 2021 года ФАТФ рассмотрела механизмы обмена информацией, относящиеся к ГЧП, в своем отчете "Возможности и проблемы новых технологий в сфере ПОД/ФТ". В некоторых странах реализуется ряд инициатив ГЧП, подтверждающих свою полезность (см. ниже).

Вставка А1. Конкретные результаты работы государственно-частых партнерств

Результаты работы **Объединенной целевой группы по сбору оперативной информации об отмывании денег (JMLIT) в Великобритании:**

- Разработка оперативной финансовой информации по более чем 400 реальным делам.
- Результаты, достигнутые на основе оперативных данных, включая более 100 арестов, конфискацию миллионов фунтов стерлингов преступных активов, выявление тысячи ранее неизвестных банковских счетов и новых объектов, представляющих интерес.
- Тесное сотрудничество с ПФР Великобритании и банками для обеспечения круглосуточной оперативной поддержки в ответ на террористические нападения в Великобритании.
- Представление высококачественных СПД, ускоренная обработка которых ПФР Великобритании способствовала дальнейшему повышению эффективности расследований, осуществляющихся правоохранительными органами.

[49] Рекомендации ФАТФ, Пояснительная записка к Рекомендации 18.

Результаты работы **австралийской инициативы Fintel Alliance:**

- Разработка и распространение типологии рисков финансовых преступлений, связанных с «Панамским досье».
- Информирование Австралийской федеральной полиции (АФП) о лицах, подозреваемых в причастности к деятельности, связанной с эксплуатацией детей.
- Выявление новых подозреваемых в причастности к опасной организованной преступности.
- Предоставление АФП оперативной информации о лицах, представляющих интерес в связи с предотвращенным террористическим актом в отношении международного авиарейса из Сиднея.
- Предоставление финансовой информации АФП в отношении примерно 600 человек, признанных "пропавшими без вести".

Результаты работы **канадских ГЧП, основанных на проектах:**

- Разработка новых типологий и индикаторов в сотрудничестве с частным сектором.
- Новые оперативные оповещения, разработанные в сотрудничестве с частным бизнесом и другими государственными ведомствами в рамках инициатив ГЧП. Эти оперативные оповещения были доведены до сведения подотчетных субъектов. В их число входят актуальные индикаторы и факторы высокого риска, связанные с конкретными методами ОД/ФТ.
- Значительный рост количества и качества СПО, относящихся к приоритетным видам деятельности, и связанное с ним увеличение количества преступлений, раскрытых правоохранительными органами.
- Большое количество брифингов, проведенных FINTRAC для внутренней и международной аудитории, включая частный сектор, правоохранительные органы и другие государственные структуры.

Результаты работы **гонконгской Целевой группы по сбору оперативной информации о мошенничестве и отмывании денег (FMLIT):**

- Разработка оперативной финансовой информации по более чем 150 реальным делам.
- Результаты, достигнутые на основе оперативных данных, включая арест 394 преступников, предотвращение вывода 749 миллионов гонконгских долларов в виде преступных доходов и идентификацию тысячи ранее неизвестных правоохранительным органам организаций.
- Разработка и распространение типологий/индикаторов риска по широкому кругу часто встречающихся финансовых преступлений и ОД.

Результаты работы **сингапурского Отраслевого партнерства в сфере ПОД/ФТ (ACIP):**

- Разработка документов ACIP по передовым практикам снижения рисков отмывания денег, основанного на торговле (TBML), и неправомерного использования структур компаний в незаконных целях были хорошо приняты отраслью.
- Проведение семинаров, доступных для всех членов отрасли, целью которых являлось обсуждение вышеупомянутых материалов по передовым практикам, а также решений по преодолению ключевых проблем и вопросов в области анализа данных ПОД/ФТ.
- Публикация документа о перспективах развития отрасли для содействия эффективному внедрению инструментов анализа данных ПОД/ФТ и практического руководства по смягчению последствий операционных сбоев, вызванных пандемией COVID-19.

- Разработка рекомендаций ACIP для предупреждения отрасли о новых типологиях и проблемах, вызывающих озабоченность.
- Сотрудничество государственного и частного секторов в проведении приоритетных расследований, по результатам которых на сегодняшний день конфисковано 50 миллионов долларов США.

Результаты работы **российского Совета Комплаенс:**
- Сокращение использования электронных переводов в целях ФТ.
- Разработка системы идентификации, которая выявляет клиентов, соответствующих профилю иностранного боевика-террориста, путем анализа финансовых и поведенческих моделей.
- Разработка периодически обновляемой системы включения в региональные санкционные списки, которая предоставляет банкам информацию о лицах, разыскиваемых на территории СНГ, и удостоверениях личности, захваченных боевиками ИГИЛ в Ираке и Сирии, которые впоследствии тщательно отслеживаются.

Результаты работы **американской программы FinCEN Exchange:**
- В период с 2015 по 2018 год FinCEN организовано более десятка брифингов в пяти городах, в которых приняли участие более 40 ФУ, а также целый ряд правоохранительных органов.
- Результаты, полученные на основе разведданных, включая идентификацию банковских счетов, субъектов и сетей, а также информация для обоснования арестов, обвинительных заключений и ордеров на конфискацию.
- Разработка новых типологий, информацию о которых FinCEN распространяет в масштабах всей отрасли.
- Информирование о действиях Казначейства США, таких как наложение санкций и издание распоряжений о географическом таргетинге, или их поддержка.
- Содействие обмену информацией между представителями частного сектора в соответствии с разделом 314(b) Закона об объединении и укреплении США путем обеспечения соответствующих мер, направленных на пресечение и предупреждение терроризма (Закон о борьбе с терроризмом США «Патриот»).

Предварительные результаты работы единственного наднационального ГЧП, **государственно-частного партнерства Европола в сфере финансовой разведки (EFIPPP):**
- Использование специальной защищенной платформы для обмена оценками угроз и стратегическими отчетами членов.
- Совместная разработка трех типологий (из них две по инвестиционному мошенничеству и одна по «структуре корреспондентских банковских отношений с использованием встроенных счетов», целью которых является уклонение от санкций и ОД) на основе текущих трансграничных расследований, использующих конкретные географические индикаторы. Участники изучили типологии, чтобы запросить и/или добавить дополнительную информацию.

ПАРТНЕРСТВО В БОРЬБЕ С ФИНАНСОВЫМИ ПРЕСТУПЛЕНИЯМИ ЗАЩИТА ДАННЫХ, ТЕХНОЛОГИИ И ОБМЕН ИНФОРМАЦИЕЙ МЕЖДУ СУБЪЕКТАМИ ЧАСТНОГО БИЗНЕСА

Одно финансовое учреждение обладает лишь частичным пониманием финансовой операции и видит лишь небольшую часть того, что зачастую является большим и сложным явлением. Для структурирования незаконных финансовых средств злоумышленники используют недостаток информации, прибегая к услугам различных ФУ, находящихся в одной или нескольких странах.

Осуществляя совместный анализ, объединяя данные или реализуя другие программы по обмену информацией ответственным образом, ФУ могут получить более четкую картину существующего явления, которая позволит им глубже понимать, а также более эффективно оценивать и уменьшать риски ОД/ФТ.

Задачей этого отчета является оказание помощи юрисдикциям в повышении эффективности обмена информацией между представителями частного бизнеса, а также в ответственной разработке и применении таких программ в соответствии с правилами защиты данных и неприкосновенности частной жизни таким образом, чтобы риски, связанные с интенсификацией обмена личными данными, принимались во внимание надлежащим образом. Данный отчет дополняет отчет ФАТФ "Критическая оценка объединения данных, совместного анализа и защиты данных" (июль 2021).

www.fatf-gafi.org | Июль 2022