

FATF

Отчет ФАТФ

Обмен информацией в целях противодействия незаконной финансовой деятельности

Глобальный обзор партнерств государственного и частного секторов и механизмов защиты данных



Июль 2026 года



Группа разработки финансовых мер борьбы с отмыванием денег (ФАТФ) является независимым межправительственным органом, который разрабатывает и продвигает политику, направленную на защиту глобальной финансовой системы от отмывания денег, финансирования терроризма и финансирования распространения оружия массового уничтожения. Рекомендации ФАТФ признаны глобальным стандартом в сфере противодействия отмыванию денег (ПОД) и финансированию терроризма (ФТ).

Для получения дополнительной информации о ФАТФ посетите сайт: www.fatf-gafi.org.

Настоящий документ и/или любые включенные в него карты не затрагивают статус или суверенитет какой-либо территории, делимитацию международных границ и рубежей, а также наименование любой территории, города или района.

Неофициальный перевод выполнен МУМЦФМ

Ссылка для цитирования:

ФАТФ (2026), «Обмен информацией в целях противодействия незаконной финансовой деятельности: глобальный обзор партнерств государственного и частного секторов и механизмов защиты данных», ФАТФ, Франция,
www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/information-sharing-ppp-data-protection-arrangements

© 2026 ФАТФ/ОЭСР. Все права защищены.

Воспроизведение или перевод настоящей публикации без предварительного письменного разрешения не допускается.

Запросы на получение такого разрешения в отношении всей публикации или ее части следует направлять в Секретариат ФАТФ по адресу: 75775, Франция, Париж, 16-й округ, ул. Андре Паскаля, д. 2 (электронная почта: contact@fatf-gafi.org).

Фотография на обложке: © Shutterstock

Оглавление

Аббревиатуры и сокращения.....	2
Исполнительное Резюме.....	3
Цель, назначение и структура.....	4
Методология и участники.....	5
Предпосылки.....	6
Имеющиеся в Глобальной сети знания о механизмах обмена информацией (между государственным и частным секторами, между субъектами частного сектора).....	6
Механизмы обмена информацией.....	7
Механизмы обмена информацией.....	7
Государственно-частные партнерства как расширенный механизм обмена информацией.....	9
Определения, ключевые характеристики и принципы государственно-частных партнерств.....	9
Цели государственно-частных партнерств.....	10
Картирование и разнообразие практики внедрения государственно-частных партнерств в мире.....	13
Срок действия.....	14
Руководство.....	15
Правовые и регуляторные аспекты обмена информацией.....	28
Информационные потоки в рамках обмена информацией ГЧП.....	29
Внутренние государственно-частные партнерства по обмену информацией.....	34
Многоюрисдикционные и трансграничные государственно-частные партнерства по обмену информацией.....	35
Развитие государственно-частных партнерств.....	40
Защищенный обмен информацией с соблюдением конфиденциальности.....	42
Правовые и регуляторные вопросы.....	43
Конфиденциальность и целостность уголовных расследований.....	46
Операционные и институциональные проблемы.....	47
Технологические и инфраструктурные ограничения.....	47
Проблемы культуры и доверия.....	48
Обеспечение соблюдения основных прав (справедливое судебное разбирательство и презумпция невиновности, конфиденциальность) и предупреждение непреднамеренных последствий (например, прекращения деловых отношений и финансовой изоляции).....	49
Управление данными, хранение и удаление.....	50
Дерискинг и непреднамеренные последствия.....	51
Вопросы, относящиеся к трансграничным государственно-частным партнерствам.....	51
Почему эти проблемы сохраняются и чем различаются юрисдикции?.....	53
Достижения и добавленная стоимость государственно-частных партнерств.....	54
Доказательство повышения эффективности выявления ОД/ФТ и возврата преступных активов.....	54
Повышение качества СПО.....	55
Пресечение преступных сетей.....	56
Повышение возможностей финансовых учреждений и УНФПП по соблюдению требований.....	59
Обмен оперативной информацией и укрепление доверия.....	60
Операционные структуры, технологии и ресурсы.....	60
Государственно-частные партнерства как связующее звено между стратегическим и операционным сотрудничеством.....	61
Выводы.....	62

Аббревиатуры и сокращения

ИИ	Искусственный интеллект
ПОД	Противодействие отмыванию денег
API	Программный интерфейс приложения
НПК	Надлежащая проверка клиента
ПФТ	Противодействие финансированию терроризма
СТАФ	Тунисский комитет финансового анализа
DPA	Орган по защите данных
DPIA	Оценка воздействия на защиту данных
DRP	Конфиденциальность и защита данных
УНФПП	Установленные нефинансовые предприятия и профессии
ЕСААМЛГ	Группа по борьбе с отмыванием денег в Восточной и Южной Африке
ФАТФ	Группа разработки финансовых мер борьбы с отмыванием денег
РГТФ	Региональная группа по типу ФАТФ
ФУ	Финансовое учреждение
FinCEN	Сеть по борьбе с финансовыми преступлениями (США)
ПФР	Подразделение финансовой разведки
GDPR	Общий регламент по защите данных (ЕС)
ЗСК	«Знай своего клиента»
ISAs	Соглашения об обмене информацией
ПО	Правоохранительный орган
OVO	Отчет о взаимной оценке
ОД	Отмывание денег
MoB	Меморандум о взаимопонимании
НКО	Некоммерческая организация
НОР	Национальная оценка рисков
РЕТ	Технология повышения конфиденциальности
ГЧП	Государственно-частное партнерство
СПД	Сообщение о подозрительной деятельности
СПАК	Специальная структура по борьбе с коррупцией и организованной преступностью
СПО	Сообщение о подозрительной операции
ФТ	Финансирование терроризма
ООН	Организация Объединенных Наций
ИДКТООН	Исполнительный директорат Контртеррористического комитета ООН

Исполнительное резюме

1. В условиях усиливающейся цифровизации, а также высокой скорости и сложности трансграничных операций эффективный обмен информацией между государственным и частным секторами имеет ключевое значение для эффективности систем ПОД/ФТ. В настоящем документе подчеркивается настоятельная необходимость совместной работы органов власти и частного сектора по противодействию незаконной финансовой деятельности. Например, для борьбы с эпидемией мошенничества с учетом скорости, сложности и масштабов этой проблемы необходимы более тесное сотрудничество и более оперативный обмен информацией. Настоящая работа показывает, что государственный и частный секторы проявляют гибкость и привержены разработке совместных и усиленных мер противодействия преступности с использованием ГЧП и механизмов взаимодействия в режиме реального времени. За последнее десятилетие ГЧП получили все большее распространение во многих юрисдикциях, которые признают их способность значительно укреплять доверие между государственным и частным секторами, а также углублять понимание рисков ОД/ФТ/ФРОМУ и повышать эффективность мер по их снижению. Исследование также показывает, что операционные ГЧП могут создавать особую ценность благодаря быстрому обмену практически значимой оперативной информацией и способствовать более эффективному выявлению и расследованию ОД/ФТ/ФРОМУ и предикатных преступлений.
2. Универсальной модели ГЧП не существует. В разных юрисдикциях они принимают различные формы и различаются по целям, механизмам управления, видам передаваемой информации и результатам, отвечая собственным потребностям, возможностям и конкретным обстоятельствам юрисдикций.
3. В отчете также рассматриваются механизмы обмена информацией между субъектами частного сектора и международные механизмы обмена информацией. Для большинства юрисдикций эти направления все еще находятся на этапе развития, однако они имеют критически важное значение для принятия более превентивных мер и формирования комплексных ответных мер в отношении незаконной финансовой деятельности.
4. Помимо систематизации подходов юрисдикций, включая подходы, освещенные в предыдущих публикациях ФАТФ и других организаций, в отчете приводятся практические выводы о факторах устойчивости ГЧП и, в особенности, об их масштабируемости в различных регуляторных и культурных условиях, что призвано способствовать широкому внедрению таких механизмов в рамках ФАТФ и ее Глобальной сети.
5. На основе сравнительного анализа различных моделей обмена информацией и ГЧП, связанных с ними аспектов защиты данных и извлеченных уроков в отчете определены инструменты и технологии, позволяющие заинтересованным сторонам обеспечить баланс между операционной эффективностью и соблюдением требований в области защиты данных, конфиденциальности и прав человека. Эти практики содержат ценные рекомендации для юрисдикций, стремящихся разработать или укрепить механизмы, содействующие сотрудничеству при сохранении конфиденциальности данных.
6. ГЧП все чаще рассматриваются как эффективный механизм более раннего снижения рисков преступной деятельности, позволяющий перейти от реактивной модели, основанной на формальном соблюдении требований, к проактивной и совместной модели, поскольку они объединяют информацию, ресурсы, технологии и специализированные знания, которые могут отсутствовать у отдельного государственного органа или частной организации. ФАТФ намерена использовать результаты настоящего отчета и изучить возможности дальнейшей поддержки развития ГЧП, чтобы обеспечить полноценное использование этих инструментов.

Цель, назначение и структура

7. Настоящий документ представляет общую картину практики обмена информацией между государственным и частным секторами в рамках Глобальной сети ФАТФ и описывает различные модели и механизмы, применяемые в мире, с признанием того, что единой модели обмена информацией или ГЧП, подходящей для всех юрисдикций, не существует.
8. В отчете освещаются ключевые инновации, разрабатываемые как недавно созданными, так и более зрелыми и давно действующими ГЧП, которые демонстрируют возможности развития независимо от характера, масштаба или назначения конкретной модели.
9. В настоящем отчете рассматриваются основные проблемы и аспекты, с которыми сталкиваются развивающиеся и уже сформировавшиеся ГЧП, возможные решения и передовые практики, ключевые достижения и свидетельства добавленной стоимости совместного обмена информацией между государственным и частным секторами по широкому кругу количественных и качественных результатов.
10. Отчет призван содействовать усилиям по обмену информацией и побуждать юрисдикции взаимодействовать, обмениваться опытом и учиться друг у друга, облегчать сотрудничество, помогать юрисдикциям внедрять, воспроизводить или совершенствовать собственные модели, а также улучшать обмен информацией при четком согласовании с требованиями защиты данных, имеющими ключевое значение для эффективного обмена информацией.
11. В отчете также рассматриваются виды информации, которой обмениваются в рамках ГЧП, и пределы ее передачи за рамки ГЧП, в том числе на международном уровне.
12. Важно отметить, что отчет не преследует цели предписать единую модель ГЧП, а направлен на выявление общих принципов и адаптируемых элементов, которые юрисдикции могут приспосабливать к своим конкретным потребностям. Его задача состоит в предоставлении практических рекомендаций для разработчиков политики и практических специалистов, стремящихся создать или усовершенствовать механизмы ГЧП, обеспечивающие баланс между операционной эффективностью, подотчетностью и соблюдением основных прав.
13. Для целей настоящего документа и информационного обеспечения будущей работы ФАТФ ГЧП определяются следующим образом:

Блок 1. Определение ГЧП

Постоянно действующий механизм, обеспечивающий эффективный обмен информацией, совместную деятельность, сотрудничество и/или координацию между государственными органами, выполняющими функции в сфере ПОД/ФТ/ФРОМУ, и частным сектором, который также может обеспечивать обмен информацией между субъектами частного сектора в рамках этого механизма.

Методология и участники

14. Работу возглавляла разнопрофильная проектная группа, в которую вошли представители 14 членов ФАТФ, восьми членов региональных групп по типу ФАТФ (РГТФ) и пяти наблюдателей ФАТФ.
15. Выводы отчета основаны на следующих источниках:
 - обзор материалов из открытых источников, включая упоминаемые в отчете публикации ФАТФ и других организаций, в том числе отчеты о взаимных оценках;
 - ответы на опрос, проведенный в сентябре 2025 года, полученные от 78¹ делегаций ФАТФ и РГТФ, включая 55 юрисдикций, одну организацию и многочисленные органы, в том числе подразделения финансовой разведки (ПФР), что отражает разнообразие ведомств, отвечающих за обмен информацией. Хотя ответы были получены не от всех членов ФАТФ и РГТФ Глобальной сети, объединяющей более 200 юрисдикций, выборка является значительной и считается достаточно репрезентативной: она охватывает разные континенты и правовые системы, а также юрисдикции различного размера и профиля;
 - запросы информации у участвующих членов и заинтересованных сторон частного сектора, включая кабинетное исследование подходов к политике, отраслевых практик и примеров из практики, а также комментарии, полученные от членов ФАТФ и Глобальной сети в ходе подготовки и рассмотрения проекта;
16. Ответы на опрос и иные отзывы были проанализированы и включены в отчет без указания источника информации в соответствии с правилами ФАТФ в области защиты данных и конфиденциальности.

¹ Албания; Ангола; Австралия; Азербайджан; Бахрейн; Бельгия; Бенин; Ботсвана; Бразилия; Кипр; Китайская Народная Республика; Китайский Тайбэй; Дания; Эсватини; Европейская комиссия; Финляндия; Грузия; Гана; Гибралтар; Греция; Гонконг, Китай; Индия; Индонезия; Ирак; остров Мэн; Италия; Япония; Лаосская Народно-Демократическая Республика; Латвия; Лесото; Либерия; Люксембург; Мальта; Молдова; Маршалловы Острова; Мексика; Мьянма; Нигерия; Северная Македония; Палестина; Перу; Португалия; Саудовская Аравия; Южно-Африканская Республика; Сейшельские Острова; Сингапур; Испания; Швеция; Швейцария; Сирия; Гамбия; Нидерланды; Тунис; Объединенные Арабские Эмираты; Соединенное Королевство и Зимбабве.

Предпосылки

Имеющиеся в Глобальной сети знания о механизмах обмена информацией (между государственным и частным секторами и между субъектами частного сектора)

17. Настоящий отчет основан на предыдущей работе ФАТФ и других заинтересованных сторон, включая:
- работу ФАТФ по вопросам важности обмена информацией и внесенные в феврале 2018 года изменения в Рекомендации 18 и 21, а также руководство для частного сектора² по обмену информацией и ГЧП;
 - отчет ФАТФ 2022 года об обмене информацией³, содержащий дополнительные примеры повышения эффективности предупреждения финансовых преступлений;
18. В 2023 году Исполнительный директорат Контртеррористического комитета ООН (ИДКТК ООН) выпустил аналитическую записку⁴ о механизмах ГЧП в сфере противодействия финансированию терроризма, подчеркнув ценность сотрудничества с широким кругом заинтересованных сторон, включая социальные сети, в целях борьбы с преступностью. Это также было отмечено в «Комплексном обновлении информации о рисках финансирования терроризма» ФАТФ 2025 года⁵. Совет Безопасности ООН и его Контртеррористический комитет настоятельно призывают национальные органы создавать партнерства, в частности для эффективного выполнения требований к отчетности и раскрытию информации, использования соответствующей финансовой информации частного сектора и обмена ею, а также обмена информацией об изменении тенденций, источников и методов финансирования терроризма⁶. В тематической сводной оценке пробелов и направлений, требующих дополнительных действий для реализации ключевых положений соответствующих резолюций Совета по ПФТ, проведенной в 2022 году⁷, ИДКТК ООН отметил, что в большинстве государств, оцененных в отчетный период, отсутствовали устойчивые ГЧП, необходимые для обмена информацией, понимания развивающихся тенденций, в том числе взаимосвязи терроризма и организованной преступности, повышения знаний и компетенций соответствующих специалистов и укрепления целостности финансового сектора.

² ФАТФ (2017), «Руководство по обмену информацией в частном секторе», ФАТФ, Париж, доступно по адресу: <https://www.fatf-gafi.org/en/publications/Fatfgeneral/Guidance-information-sharing.html> (дата обращения: 17 сентября 2025 года).

³ ФАТФ (2022), «Партнерство в борьбе с финансовой преступностью: защита данных, технологии и обмен информацией в частном секторе», ФАТФ, Париж, Франция, <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf> (дата обращения: 22 октября 2025 года).

⁴ ИДКТК ООН (2023), «Создание эффективных государственно-частных партнерств в сфере противодействия финансированию терроризма», доступно по адресу: <https://www.un-ilibrary.org/content/books/9789211067910>. См. также материалы экспертных обсуждений, проведенных при запуске документа: <https://www.un.org/securitycouncil/ctc/news/cted-holds-multi-stakeholder-discussion-establishing-effective-public-private-partnerships>

⁵ ФАТФ (2025), «Комплексное обновление информации о рисках финансирования терроризма», доступно по адресу: <https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/comprehensive-update>.

⁶ Резолюция Совета Безопасности 2462 (2019), пункт 22; Делийская декларация о противодействии использованию новых и новейших технологий в террористических целях (октябрь 2022 года), пункты 15, 25; Алжирские руководящие принципы (январь 2025 года), S/2025/22, принципы 1(e), 2(g) и (j), 3(l) и (m), 4(e), (g) и (i).

⁷ ИДКТК ООН (2022), «Тематическая сводная оценка пробелов в реализации ключевых положений резолюций Совета Безопасности о противодействии финансированию терроризма», доступно по адресу: www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/cted_2022_cft_gaps_assessment_final.pdf.

Механизмы обмена информацией

Механизмы обмена информацией

19. Юрисдикции используют различные механизмы обмена информацией между компетентными органами и частным сектором, причем подавляющее большинство включает ГЧП в свой инструментарий обмена информацией. В некоторых юрисдикциях действует несколько ГЧП, созданных для разных целей; виды передаваемой информации также могут различаться, например, быть операционными или стратегическими. Лишь небольшая доля опрошенных юрисдикций — 6⁸ из 50 респондентов, что представляет значимую выборку участников Глобальной сети, — указали, что у них отсутствуют ГЧП и что они не планируют создавать их в ближайшем будущем. Общедоступные данные также свидетельствуют о широком использовании ГЧП в других странах, не участвовавших в опросе.
20. Юрисдикции, в которых отсутствуют механизмы ГЧП, сообщают, что защищенный обмен информацией регулярно осуществляется посредством ряда альтернативных механизмов с участием их ПФР, между правоохранительными органами, а в некоторых случаях — с частным сектором, с использованием зашифрованных каналов связи, включая защищенные программные платформы, а также платформы Европола и Защищенной сети Группы «Эгмонт» (ЗСЭ) для международного обмена информацией и сотрудничества (см. также таблицу 1 ниже). Респонденты, имеющие ГЧП, отметили, что некоторые из этих платформ также являются важными средствами обеспечения защищенного обмена информацией в рамках ГЧП.

Таблица 1. Основные механизмы обмена информацией, которые также могут обеспечивать деятельность ГЧП

Модель	Характеристики	Заинтересованные стороны
Защищенные платформы под руководством ПФР	Как правило, вводятся в действие и обслуживаются ПФР Используются ПФР для сбора информации и обмена ею, включая сведения СПО/СПД, данные о финансовых операциях и надлежащей проверке, результаты аналитики ПФР и стратегические отчеты Многонаправленные информационные потоки (между государственными органами; от государственного сектора частному и от частного государственному) Платформы, как правило, зашифрованы, обеспечивают возможность аудита, а доступ предоставлен ограниченному количеству соответствующих заинтересованных сторон	ПФР ПО/надзорные органы Подотчётные субъекты, включая ФУ/УНФПП/ПУВА
Судебные/правоохранительные каналы	Как правило, вводятся в действие и обслуживаются правоохранительными или прокурорскими органами либо судебной системой Используются для обмена результатами расследований и прокурорской деятельности, которые должны соответствовать доказательственным стандартам; обычно включают более конкретные операционные и персональные данные, такие как данные коммуникаций, метаданные и геолокационные сведения Преимущественно информационные потоки между государственными органами	ПО Прокуратура Судебные органы

⁸ Лесото, Либерия, Мьянма, Северная Македония, Португалия и Испания.

Модель	Характеристики	Заинтересованные стороны
Международные защищенные сети	Как правило, вводятся в действие и обслуживаются международной организацией, например, Группой «Эгмонт» Используются главным образом для трансграничного обмена стратегической и/или операционной информацией Преимущественно информационные потоки между государственными органами в нескольких юрисдикциях	ПО Надзорные органы ПФР
Защищенные системы отдельных учреждений	Как правило, вводятся в действие и обслуживаются надзорными органами Используются надзорными органами для сбора информации и обмена ею с учетом особенностей их институционального устройства и функций, например, надзорные порталы центральных банков и системы регуляторов рынка ценных бумаг Многонаправленные информационные потоки (от государственного сектора к частному и от частного к государственному) Платформы, как правило, зашифрованы, обеспечивают возможность аудита, а доступ предоставлен ограниченному количеству соответствующих заинтересованных сторон	Надзорные органы Подотчётные субъекты, включая ФУ/УНФПП/ПУВА

Источник: ответы на опрос.

Государственно-частные партнерства как расширенный механизм обмена информацией

Определения, ключевые характеристики и принципы государственно-частных партнерств

21. Рекомендации ФАТФ в целом предусматривают обмен информацией в ряде случаев. Стандарты не требуют создания ГЧП, однако отчеты о взаимных оценках и предыдущие исследования ФАТФ показывают, что такие партнерства представляют собой комплексный способ более быстрого и эффективного обмена информацией и обычно понимаются как расширенная форма добровольного сотрудничества государственного органа и частной организации. Хотя единого окончательного универсального определения ГЧП не существует, в «Руководстве ФАТФ по обмену информацией в частном секторе»⁹, а затем в отчете ФАТФ «Партнерство в борьбе с финансовой преступностью» они определяются как механизмы, содействующие обмену информацией между заинтересованными сторонами государственного и частного секторов таким образом, чтобы повысить эффективность мер ПОД/ФТ/ФРОМУ за счет формирования более полного представления о финансовых операциях и поведении клиентов¹⁰.
22. В другом исследовании инициативы Future of Financial Information Sharing¹¹ ГЧП названы механизмами, обеспечивающими регулярно проводимый динамичный диалог между государственным и частным секторами об угрозах финансовой преступности на основе общих согласованных целей и приоритетов. Рабочее определение ГЧП, используемое в настоящем документе (блок 1), основано на приведенных выше определениях.
23. С учетом ответов на опрос и результатов предыдущей работы ниже перечислены некоторые характеристики, в различной степени присущие ГЧП в зависимости от целей и характера конкретного партнерства:
 - **Взаимная выгода и добавленная стоимость.** ГЧП должны обеспечивать получение преимуществ как государственным, так и частным сектором от результатов деятельности, осуществляемой в рамках партнерства, в том числе посредством содержательного и взаимного обмена информацией. Эффективное сотрудничество требует двустороннего взаимодействия, при котором все стороны предоставляют соответствующую информацию и взамен получают практически применимую обратную связь, стратегические выводы или операционную ценность. ГЧП также должны расширять уже существующие возможности обмена информацией, а не создаваться ради самого факта создания.
 - **Совместная деятельность.** ГЧП должны быть направлены на выявление, сокращение, снижение или пресечение деятельности, создающей угрозу, либо на устранение уязвимостей посредством повышения устойчивости или обучения.
 - **Благоприятствующая основа.** Необходимы механизм или совокупность обеспечивающих условий, согласованные со Стандартами ФАТФ, например, с усилиями по повышению качества СПО, международными рекомендациями и передовыми практиками и определяющие мандат, охват и цели, а также политическая поддержка высокого уровня, гарантирующая необходимые ресурсы для деятельности ГЧП (подробнее см. отдельный раздел об управлении и бюджете).
 - **Показатели.** Для оценки воздействия следует предусматривать показатели результативности, поскольку они необходимы для отслеживания эффективности ГЧП.

⁹ ФАТФ (2017), «Руководство по обмену информацией в частном секторе», ФАТФ, Париж, доступно по адресу: <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Private-Sector-Information-Sharing.pdf.coredownload.pdf>.

¹⁰ ФАТФ (2022), «Партнерство в борьбе с финансовой преступностью», ФАТФ, Париж, доступно по адресу: <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf>.

¹¹ RUSI (2017), «Роль партнерств по обмену финансовой информацией в пресечении преступности», доступно по адресу: https://www.future-fis.com/uploads/3/7/9/4/3794525/ffis_report_-_oct_2017_web_1.pdf.

- **Правовая основа обмена.** Для обмена информацией необходимы прямо предусмотренные законом полномочия, определение компетентных субъектов и четкие правовые нормы, устанавливающие, какой информацией и при каких условиях можно обмениваться.
- **Конфиденциальность и защита данных.** Любой обмен информацией должен соответствовать стандартам защиты данных и конфиденциальности, включая законность обработки, ограничения сроков хранения, обезличивание и минимизацию данных, а также административные, технические и договорные гарантии.
- **Разграниченные каналы и доступ по принципу служебной необходимости.** Информационные потоки должны разграничиваться по назначению, например, на стратегические и операционные, а уровни доступа предоставляться в соответствии с ролью и строгими критериями служебной необходимости.
- **Обязанности, ответственность и подотчетность.** Участники должны нести взаимные обязанности по предоставлению соответствующей информации, ограничению ее использования разрешенными целями, уведомлению о нарушениях и соразмерной ответственности за несоблюдение требований.
- **Управление рисками и риск-ориентированный подход.** Участники должны периодически проводить оценку рисков, согласовывать деятельность с национальными приоритетами и динамично адаптироваться к возникающим угрозам и изменениям профилей риска.
- **Инклюзивное управление и представительство.** Структуры управления должны обеспечивать участие соответствующих государственных органов и доверенных субъектов частного сектора — ФУ, УНФПП, ПУВА, организаций гражданского общества и, при необходимости, иных организаций и предприятий — при наличии четких правил приема и урегулирования споров. В зависимости от потребностей и условий конкретной юрисдикции к участию могут привлекаться провайдеры технологических или коммуникационных услуг, включая социальные сети, платформы мгновенного обмена сообщениями и потокового вещания, а также НКО и научно-образовательные организации.
- **Операционные возможности и кибербезопасность.** Участники и используемая для обмена информацией платформа должны соответствовать минимальным техническим и операционным стандартам, включая шифрование, аутентификацию, управление доступом и безопасность, а также располагать учебными и аналитическими ресурсами для эффективного реагирования.
- **Совместимость и стандартизация.** При обмене информацией должны использоваться общие форматы, обеспечивающие эффективную, контролируруемую и машиночитаемую передачу данных между организациями.

Цели государственно-частных партнерств

24. ГЧП повышают способность компетентных органов и частного сектора быстро и масштабно выявлять, анализировать и пресекать финансовые преступления. Они создают структурированную, зачастую защищенную и зашифрованную среду, в которой органы власти обмениваются информацией о приоритетных угрозах, пробелах в оперативной информации на ранних этапах, значимых моделях поведения и целевых операционных рекомендациях. На практике это позволяет частным организациям проводить целевой анализ данных о клиентах и операциях, отвечать на запросы о проведении финансового анализа и финансового мониторинга и выявлять деятельность, связанную с текущими уголовными расследованиями или расследованиями в сфере национальной безопасности. В некоторых случаях такие механизмы включают целевые или тактические инструменты, предназначенные для своевременных и согласованных параллельных действий правоохранительных органов и подотчетных субъектов.
25. Помимо регулярного обмена информацией, уже ожидаемого и предусмотренного Стандартами ФАТФ в рамках режимов ПОД/ФТ, ГЧП могут выполнять операционную функцию укрепления

доверия и уверенности посредством регулярного взаимодействия, обеспечивая более эффективные и быстрые результаты в сфере ПОД/ФТ/ПРОМУ за счет более глубоких и разнообразных форм взаимодействия между государственным и частным секторами. Ниже приведены примеры Франции, Индонезии и Саудовской Аравии, демонстрирующие различные формы такого взаимодействия.

Блок 2. Защита страны с помощью высокотехнологичной платформы ГЧП

SIPENDAR (Sistem Informasi Terduga Pendanaan Terorisme) — защищенная онлайн-платформа ГЧП, созданная ПФР Индонезии (PPATK) в 2021 году для выявления террористической деятельности и ее финансирования, а также для незамедлительного реагирования. Через SIPENDAR преимущественно передаются три вида информации: 1) типологии, текущие тенденции и стратегический анализ в сфере ФТ (конфиденциальная версия); 2) перечень наблюдения за деятельностью, связанной с ФТ; и 3) платформа для инициативных и взаимных запросов.

Доступ к SIPENDAR предоставляется органам, связанным с противодействием ФТ, включая PPATK, Национальную полицию (POLRI), Национальное агентство по борьбе с терроризмом (BNPT), Государственное разведывательное агентство (BIN), таможенные и иммиграционные органы, а также частному сектору после прохождения проверки специально назначенными сотрудниками по линии разведки. SIPENDAR: 1) сформировала перечень наблюдения за деятельностью, связанной с ФТ, сочетающий машинное обучение и данные из человеческих источников, распространяет этот перечень среди участников частного сектора, требует от них дополнять информацию о включенных в перечень физических и юридических лицах и своевременно сообщать ее PPATK; 2) обеспечила незамедлительное реагирование на любые террористические инциденты, включая потенциальные, менее чем через 24 часа после опубликования информации компетентными органами.

Как ГЧП изменило ситуацию

- о ГЧП способствовало раннему выявлению входящих и исходящих переводов виртуальных активов, связанных с ИГИЛ, что позволило компетентным органам незамедлительно отреагировать, в том числе оперативно обмениваться информацией с зарубежными партнерами.
- о Технологическая платформа ГЧП сокращает бюрократические процедуры при внутренней координации и обмене информацией. Распространение информации между государственным и частным секторами происходит быстрее и эффективнее.
- о Разработка перечней наблюдения в сфере ФТ помогает частному сектору выявлять соответствующие операции и направлять СПО о ФТ.
- о Своевременное получение информации позволяет как государственному, так и частному сектору незамедлительно реагировать, что обеспечивает раннее выявление, которое может помочь компетентным органам предотвращать террористическую деятельность.

Источник: Индонезия

Блок 3. «Комитет по ПФТ» — французское ГЧП, посвященное противодействию финансированию терроризма

Финансовая информация, особенно предоставляемая ФУ, является ключевым источником оперативных сведений, которые после сбора, анализа, обогащения, использования и перекрестной проверки Tracfin помогают выявлять террористические сети, предупреждать кампании по финансированию терроризма и террористические акты.

В 2019 году Tracfin создало ГЧП по ПФТ — Comité LFT, в состав которого вошли 16 финансовых учреждений: 7 банков, 6 платежных организаций, 2 ПУВА и 1 краудфандинговая компания. Комитет, совместно возглавляемый двумя представителями частного сектора, внедрил новую форму ГЧП на основе доверия и конфиденциальности в соответствии с законодательством Франции.

Комитет собирается три-четыре раза в год и позволяет участникам получать информацию, делиться сведениями, совместно вырабатывать идеи и обмениваться мнениями о новых угрозах, тенденциях и типологиях ПФТ. Обсуждаемые темы варьируются от использования криптовалют террористическими группами до выявления передовых и ненадлежащих практик подготовки СПО в сфере финансирования терроризма. Темы для обсуждения могут предлагать Tracfin или члены Комитета. Регулярно привлекаются партнеры — разведывательные службы и ведомства, в том числе Министерство финансов Франции и Национальная антитеррористическая прокуратура Франции (PNAT).

Источник: Tracfin (ПФР Франции)

Блок 4. Доверие, обеспечивающее результат

Первоначально действия в рамках неформального ГЧП Саудовской Аравии были инициированы после того, как банк выявил большой объем международных операций, не соответствовавших заявленной клиентом цели (например, основной деятельностью компании была продажа телефонов и других технологических товаров, однако переводы направлялись биохимической компании).

До начала сотрудничества государственного и частного секторов в рамках ГЧП обмен информацией и партнерское взаимодействие были медленнее. ГЧП ускорило процесс и создало более четкий порядок противодействия рискам ПОД/ФТ. После предупреждения банка активы компании были заморожены, а в отношении одного лица продолжается судебное преследование. Дело использовалось на семинаре, после которого другие банки начали применять усиленные меры НПК к компаниям с аналогичным характером деятельности.

Как ГЧП изменило ситуацию

- о ГЧП ускорило коммуникацию между государственным и частным секторами благодаря сложившимся доверительным отношениям и сократило сроки, устранив бюрократические барьеры между ними.

Источник: Саудовская Аравия

26. Органы власти могут использовать ГЧП для своевременного направления предупреждений подотчётным субъектам, помогая им выявлять значимую деятельность и повышая полезность СПО. Через ГЧП организации получают заблаговременную информацию о новых типологиях, например, о схемах и методах мошенничества, что способствует проактивному снижению рисков и непосредственно улучшает результаты в сфере ПОД/ФТ/ФРОМУ. В этом смысле ГЧП и партнерства между субъектами частного сектора следует рассматривать во взаимосвязи на стратегическом уровне. Например, в сфере мошенничества обмен информацией между субъектами частного сектора может способствовать предупреждению, тогда как ГЧП могут сосредоточиться на расследовании деятельности сложных преступных сетей¹².
27. ГЧП создают безопасную среду для анализа массивов данных, операционного анализа и проверки данных государственным и частным секторами. Такая модель помогает устранять пробелы в оперативной информации при соблюдении национальных правовых основ и обязательств конфиденциальности, а также может обеспечивать структурированные циклы обратной связи, повышающие как оперативность тактического реагирования, так и эффективность долгосрочного сбора стратегической финансовой информации и правоохранительной деятельности.

Картирование и разнообразие практики внедрения государственно-частных партнерств в мире

28. Согласно ответам на опрос и данным из открытых источников¹³, в мире действует не менее 84 ГЧП, находящихся на различных этапах развития и зрелости, включая транснациональные партнерства, такие как EFIRPP (см. ниже). Несмотря на предпринятые усилия по охвату максимально возможного числа ГЧП, картирование может не отражать весь перечень существующих в мире партнерств, в том числе из-за сроков проведения опроса, который мог не охватить механизмы, созданные после октября 2025 года. Пятьдесят два респондента сообщили о наличии как минимум одного внутреннего ГЧП, а восемнадцать — более чем одного внутреннего ГЧП в своей юрисдикции.

¹² Обзор платформ совместной аналитики для борьбы с мошенничеством (FFIS, май 2026 года), доступно по адресу: <https://www.future-fis.com/fraudplatforms.html>. См. также инструментарий УНП ООН по ГЧП в борьбе с организованным мошенничеством (УНП ООН, май 2026 года), доступно по адресу: https://www.unodc.org/res/organized-crime/GFS/publications/UNODC_PublicPrivate_Partnership_Toolkit_Against_Organized_Fraud_EN.pdf.

¹³ Например, в Техническом приложении к [Европейскому обзору ГЧП](#), подготовленному EFIRPP, подробно задокументированы успешные примеры того, как ГЧП способствовали устранению пробелов в оперативной информации — от увеличения количества СПО до конкретных мер правоприменения. Приведены как результаты партнерств с более чем десятилетним опытом, например, Объединенной оперативной группы по противодействию отмыванию денег Соединенного Королевства (JMLIT/JMLIT+), так и более новых ГЧП, например, партнерства Латвии.

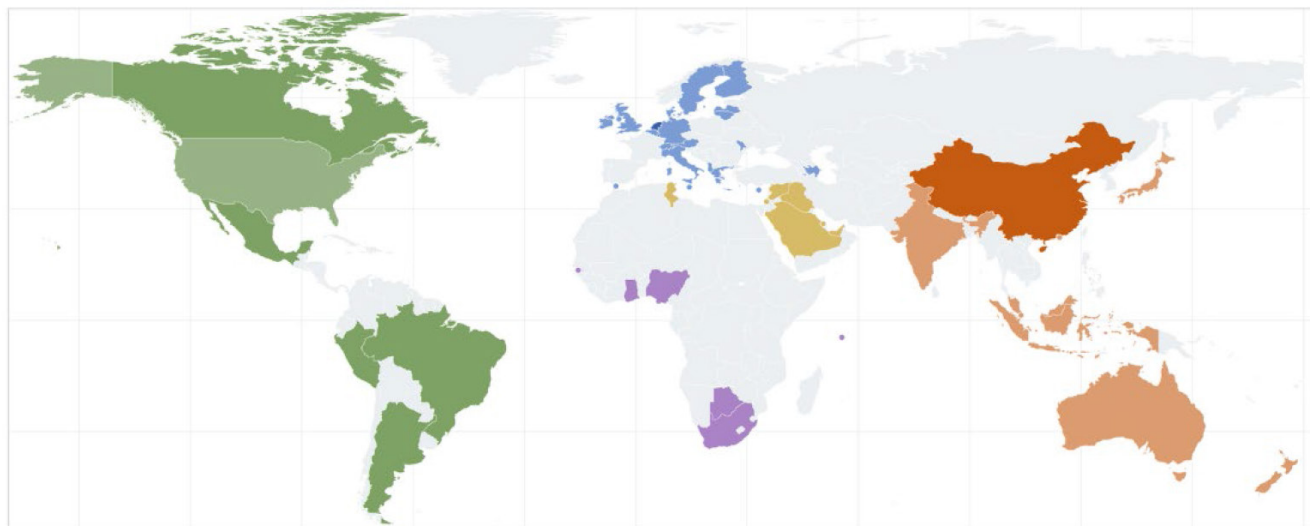
Рисунок 1. Глобальная карта государственно-частных партнерств или внедрения механизмов ГЧП

FATF

Доклад о государственно-частных партнерствах

Глобальная карта ГЧП и внедрения ГЧП

По данным опроса и открытых источников, в мире действует 84 ГЧП в 51 юрисдикции (на разных этапах развития и зрелости), включая многоюрисдикционные ГЧП, такие как EFIPPP.



Европа (23) Америка (6) АТР (9) BECA (7)
Африка (6) О ГЧП не сообщалось

Многоюрисдикционные ГЧП

EFIPPP - европейское ГЧП ПФР
Europol (3 PPPs) - инициативы уровня ЕС
Quad Island Forum - многоюрисдикционное ГЧП
United for Wildlife - многоюрисдикционное ГЧП

84 ГЧП в мире

51 юрисдикция

Примечание 1. Цветами обозначены различные юрисдикции мира, в которых действуют ГЧП.

Примечание 2. Оговорка. Настоящий документ и/или любые включенные в него карты не затрагивают статус или суверенитет какой-либо территории, делимитацию международных границ и рубежей, а также наименование любой территории, города или района.

Источник: ответы на опрос.

29. ГЧП различаются по видам, структуре, составу участников и организации деятельности. В аналитической записке ИДКТК ООН, содержащей картирование ГЧП в сфере финансирования терроризма, отмечается значительное разнообразие моделей ГЧП, большинство из которых имеет широкий охват.

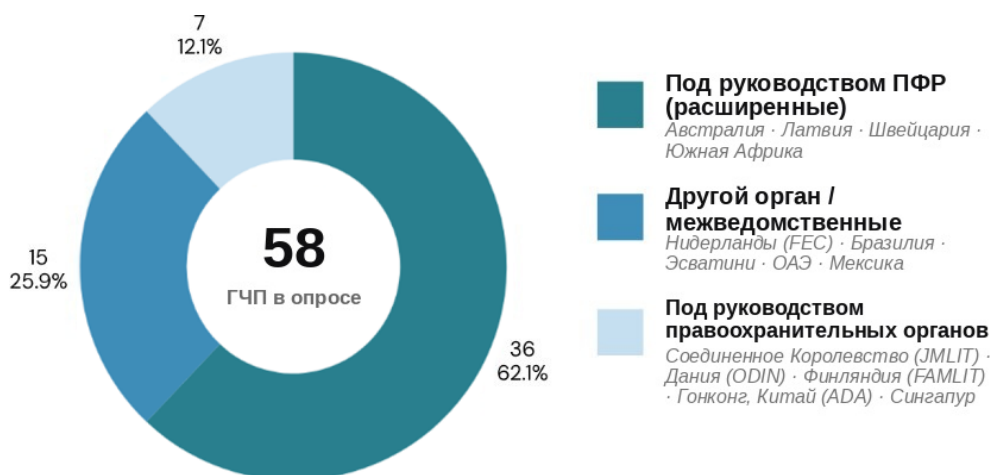
Срок действия

30. Большинство выявленных ГЧП являются постоянно действующими элементами системы ПОД/ФТ соответствующей юрисдикции. Вместе с тем некоторые механизмы, которые их управляющий орган относит к ГЧП, представляют собой динамичные, ограниченные по времени формы сотрудничества, созданные для достижения конкретной краткосрочной цели. В других случаях в рамках более широкого ГЧП действуют ограниченные по сроку подгруппы или функции, сосредоточенные на целевой деятельности в течение ограниченного периода или на конкретном направлении.

Руководство

31. Различные заинтересованные стороны могут стоять во главе ГЧП. Как показано ниже, большинство внутренних ГЧП координируются и/или размещаются на базе подразделений финансовой разведки (ПФР)¹⁴, однако ими могут руководить и другие ведомства¹⁵.

Рисунок 2. Руководство государственно-частными партнерствами



Источник: ответы на опрос.

32. Восемь ГЧП возглавляются правоохранительными органами, хотя в их состав входят представители нескольких государственных ведомств:
- Датская оперативная разведывательная сеть (ODIN), возглавляемая Национальным подразделением полиции Дании по борьбе с особо опасными преступлениями.
 - Оперативная группа Финляндии по финансовой разведке в сфере противодействия отмыванию денег (FAMLIT), возглавляемая подразделением финансовой разведки Национального бюро расследований.
 - Антимошеннический альянс Гонконга, Китай (ADA), объединяющий десять банков-участников, которые взаимодействуют с сотрудниками Координационного центра по противодействию мошенничеству Полиции Гонконга (ADCC). Некоторые лицензированные компании, работающие с ценными бумагами, также согласовали с ADCC протокол, обеспечивающий круглосуточный механизм приостановления платежей для ускоренного перехвата и возврата преступных доходов. Оперативная группа по финансовой разведке в сфере виртуальных активов (VAIT) представляет собой механизм сотрудничества правоохранительных органов, регуляторов и ключевых ПУБА. Инструмент обмена результатами оценки финансовой разведывательной информации (FINEST) администрируется Полицией Гонконга в партнерстве с Управлением денежного обращения Гонконга и Ассоциацией банков Гонконга.

¹⁴ Рабочая группа по информационному обмену Группы «Эгмонт» (РГИО) в настоящее время реализует проект по выявлению, документированию и распространению международных передовых практик государственно-частного партнерства в сфере ПОД/ФТ. Опираясь на глобальные модели, материалы ЭгмонтФАТФ и отраслевые руководства, проект направлен на разработку практического инструментария, включая шаблоны, правовые основания для обмена и показатели результативности, который поможет ПФР и партнерам из частного сектора создавать и совершенствовать эффективные ГЧП. Подготавливаемый доклад также будет содержать практическое руководство по проектированию, управлению и организации операционной деятельности ГЧП в условиях быстро меняющихся рисков ОД/ФТ. Проект находится на этапе картирования; его руководителями выступают FINTRAC, ПФР Сальвадора и ПФР Бермудских Островов.

¹⁵ В некоторых странах ПФР возглавляют иные механизмы обмена информацией, которые могут официально не называться ГЧП.

- Национальный центр реагирования на мошенничество Малайзии (NSRC) действует под руководством Королевской полиции Малайзии (RMP) и надзором Министерства внутренних дел (МОНА). NSRC объединяет финансового регулятора (Банк Негара Малайзия), регулятора телекоммуникаций (Малайзийскую комиссию по коммуникациям и мультимедиа), Национальный центр по противодействию финансовым преступлениям, банки и провайдеров телекоммуникационных услуг для совместного использования ресурсов и информации и оперативных межведомственных действий по борьбе с мошенничеством.
 - Новозеландскую сеть предупреждения финансовых преступлений (NZ-FCPN) возглавляет ПФР полиции Новой Зеландии.
 - Отраслевое партнерство Сингапура по ПОД/ФТ (ACIP) совместно координируют Департамент по коммерческим делам (CAD) Полиции Сингапура (SPF) и Денежно-кредитное управление Сингапура (MAS). SPF также обеспечивает деятельность Сингапурского центра по противодействию мошенничеству (ASC), созданного SPF как основной координационный центр полиции по расследованию преступлений, связанных с мошенничеством.
 - Американский механизм CI-FIRST (обратная связь в ответ на стратегические угрозы), возглавляемый Управлением уголовных расследований Налоговой службы США (IRS-CI), обеспечивает постоянное взаимодействие между IRS-CI и финансовыми учреждениями.
 - Объединенная оперативная группа Соединенного Королевства по финансовой разведке в сфере противодействия отмыванию денег (JMLIT+), действующая наряду с функцией взаимодействия ПФР Соединенного Королевства (UKFIU), возглавляется Национальным центром по борьбе с экономической преступностью — подразделением Национального агентства по борьбе с преступностью Соединенного Королевства — и Национальным ведущим подразделением Полиции лондонского Сити, в состав которого входят ГЧП Специализированного подразделения по борьбе с преступлениями в сфере банковских карт и платежей (DCPCU), Полицейского подразделения по борьбе с преступлениями в сфере интеллектуальной собственности (RIPCU) и Департамента правоприменения в сфере страхового мошенничества (IFED).
33. Пятнадцать ГЧП координируются иными органами. Некоторые из них имеют более узкую цель обмена информацией, например, бразильское подразделение Coordenação de Repressão à Corrupção («Координация по противодействию коррупции»), занимающееся борьбой с договорными матчами. В то же время британская сеть FIN-NET (Сеть информации о финансовых преступлениях), имеющая широкий мандат по противодействию мошенничеству и финансовой преступности с участием внутренних и международных представителей государственного и частного секторов, действует под эгидой регулятора финансовых услуг Соединенного Королевства.
34. Государственный и частный сектор также могут совместно возглавлять ГЧП (см. пример ниже).

Блок 5. Разнообразные модели государственно-частного партнерства Канады в сфере ПОД/ФТ

В Канаде некоторые ГЧП совместно возглавляются ПФР (FINTRAC) и частным сектором. Это обеспечивает активное взаимное участие частного сектора и получение им преимуществ, а также создает канал передачи информации из частного сектора государственному. Такая модель позволила FINTRAC участвовать в процессе, результатом которого стало предоставление правоохранным органам проактивной финансовой разведывательной информации на основе сведений, полученных от частного сектора. Она повысила оперативность и способность канадской системы проактивно выявлять более сложные преступления без внесения изменений в законодательство Канады. В свою очередь, благодаря обмену информацией регулируемые организации получают дополнительные сведения и данные, которые помогают выявлять подозрительные операции, точно оценивать риски, обосновывать риск-ориентированные меры и соблюдать свои обязанности, включая направление сообщений о подозрительных операциях в FINTRAC.

Агентство налоговых поступлений Канады возглавляет Канадское финансовое партнерство (CFP) — внутреннее ГЧП, объединяющее крупнейшие финансовые учреждения, представителей отрасли и федеральных партнеров для противодействия уклонению от уплаты налогов и рискам ОД. Посредством регулярного взаимодействия, включая виртуальные обсуждения и ежегодные встречи, CFP обеспечивает обмен информацией на стратегическом уровне, совместную оценку угроз и разработку типологий, одновременно укрепляя связи между государственным и частным секторами. Такая модель сотрудничества повышает способность Канады выявлять угрозы финансовой преступности и реагировать на них, а также способствует более широким международным усилиям.

Консультативный комитет Канады по вопросам отмывания денег и финансирования терроризма (ACMLTF) является дискуссионной площадкой высокого уровня для рассмотрения возникающих вопросов и подготовки рекомендаций по канадской системе ПОД/ФТ как во внутреннем контексте, так и в поддержку международного развития ПОД/ФТ. В ACMLTF входят представители государственного сектора из Министерства финансов, FINTRAC, Управления суперинтенданта финансовых учреждений (OSFI) и Министерства общественной безопасности Канады. Частный сектор представлен финансовыми организациями, компаниями по страхованию жизни, дилерами по ценным бумагам, компаниями, предоставляющими денежные услуги, дилерами виртуальных валют, бухгалтерами, нотариусами, представителями сектора недвижимости, казино, торговцами драгоценными металлами и камнями и строительными компаниями.

19 февраля 2025 года Правительство Канады провело первое рабочее совещание нового Интегрированного партнерства по обмену оперативной информацией об отмывании денег (IMLIP). Это ГЧП обеспечивает допустимый законом обмен оперативной информацией об отмывании денег и организованной преступности между правоохранными органами и внутренними системно значимыми банками Канады (DSIB) и усиливает меры Канады по противодействию организованной преступности и сложным схемам отмывания денег, в том числе связанным с оборотом фентанила. Партнерство также будет способствовать установлению прочных рабочих отношений между правоохранными органами и сектором финансовых услуг для более глубокого понимания угроз отмывания денег, с которыми сталкивается Канада. Правительство объявило о намерении внести изменения в Закон о доходах от преступной деятельности (отмывании денег) и финансировании терроризма и связанные с ним изменения в Закон о защите персональной информации и электронных документах, чтобы уточнить положения об обмене информацией от государственного к частному сектору, повысить эффективность выявления и предупреждения отмывания денег и поддержать недавно созданное IMLIP между банками и правоохранными органами.

Источник: Канада

Состав

35. 22% (18) ГЧП считаются межведомственными. Наиболее показательны ГЧП Нидерландов, действующие в рамках Центра финансовой экспертизы (FEC) — объединения Управления Нидерландов по финансовым рынкам (AFM), Общей службы разведки и безопасности, Налоговой и таможенной администрации, Центрального банка Нидерландов, Службы фискальной разведки и информации и Службы экономических расследований, Прокуратуры, Полиции Нидерландов и ПФР Нидерландов.
36. Восемь респондентов — Ангола, Бахрейн, Бенин, Эсватини, Маршалловы Острова, Саудовская Аравия, Сирия и Соединенные Штаты — сообщили, что их ГЧП, возглавляемые ПФР, регулярно проводят очные и виртуальные встречи с подотчетными субъектами и/или выпускают отраслевые руководства для них. Такое взаимодействие может рассматриваться как форма ГЧП, поскольку выходит за рамки обычного взаимодействия ПФР с частным сектором.

Блок 6. Комитеты Эсватини по ПОД/ФТ (межведомственное ГЧП) для обмена информацией

В Эсватини действует Оперативная группа по ПОД/ФТ, включающая Совет и Технический комитет, которым поручены разработка национального стратегического плана ПОД/ФТ, обеспечение его реализации и утверждения, а также другие функции. В Технический комитет входят представители государственного и частного секторов. Государственный сектор представлен Министерством финансов, ПФР, надзорными органами ПОД/ФТ, саморегулируемыми организациями, правоохранительными органами, директором прокуратуры и Управлением генерального прокурора. Частный сектор представлен Ассоциацией банкиров, Обществом юристов и Институтом бухгалтеров Эсватини. Комитет заседает ежемесячно и содействует обмену информацией в сфере ПОД/ФТ между заинтересованными сторонами.

Источник: Эсватини

Блок 7. Группа сотрудничества и координации Латвии (ССГ): оперативная, гибкая поддержка по конкретным делам

Группа сотрудничества и координации Латвии (ССГ) была создана в 2018 году как партнерство государственного и частного секторов, а также государственных органов между собой, на основе гибкой и адаптивной модели. Заседания ССГ могут созываться незамедлительно, обеспечивая быструю операционную или стратегическую координацию между ПФР, правоохранительными органами, прокуратурой, надзорными органами и подотчётными субъектами. Состав участников заседания меняется в зависимости от потребностей и целей встречи.

К числу успешных результатов относятся:

- о увеличение количества СПО и вклад в подготовку стратегических материалов;
- о обсуждение сложных дел с правоохранительными органами и подотчётными субъектами для определения дальнейших действий;
- о Пример 1. В 2021 году ПФР в рамках ССГ объединило экспертов ПФР, прокуратуры, Бюро по предупреждению коррупции и борьбе с ней (СРСБ), а также четырех крупнейших кредитных организаций Латвии. Эксперты разработали индикаторы коррупции и ОД и дополнили их соответствующими практическими примерами. Материал предназначен для использования кредитными организациями, а также другими подотчётными субъектами и правоохранительными органами при выявлении и расследовании коррупции. Документ содержит перечень риск-индикаторов («красных флагов») для операций, которые могут быть связаны с коррупцией, и иных факторов, способных вызвать подозрения в коррупции. По итогам исследования было завершено и опубликовано на веб-сайте ПФР. После публикации исследования количество СПО, связанных с предикатным преступлением коррупции, значительно увеличилось: с 67 в 2021 году до 104 в 2022 году.
- о Пример 2. В 2020 году Государственная полиция начала расследование торговли людьми. Для обеспечения быстрого и согласованного реагирования было незамедлительно созвано заседание ССГ. Государственная полиция проинформировала участников об обстоятельствах дела и запланированных мероприятиях при соблюдении конфиденциальности. ПФР через защищенный канал goAML направило ФУ распоряжения о мониторинге операций по счетам лиц, подозреваемых в совершении преступления, предоставив каждому ФУ только информацию, касающуюся его клиентов; оперативное сотрудничество с зарубежными ПФР привело к временному замораживанию средств за рубежом до направления запроса о взаимной правовой помощи. В результате значительные активы были арестованы и заморожены. В мае 2024 года уголовное дело в отношении 10 физических лиц и одного юридического лица по обвинению в торговле людьми и отмыывании денег при отягчающих обстоятельствах было передано в Суд по экономическим преступлениям, где судебное разбирательство продолжается.

Латвия называет четкую устойчивую правовую основу и адаптируемую модель ключевыми факторами успеха.

Источник: Латвия

Структуры управления, обеспечивающие деятельность государственно-частных партнерств

37. Для деятельности ГЧП необходимы политическая приверженность высокого уровня, административная поддержка и поддержка частного сектора, особенно в части обмена данными. Для их работы также могут потребоваться бюджетные ассигнования; четверть респондентов указала на наличие специальных бюджетов, включая совместное финансирование различными участниками ГЧП, что является положительным фактором.
38. Управление ГЧП представляет собой совокупность обеспечивающих механизмов, определяющих мандат, охват и цели партнерства в соответствии с международными стандартами, прежде всего Рекомендациями ФАТФ об обмене информацией¹⁶. Установление четких целей с самого начала создает правовую, политическую и/или операционную основу, позволяющую ГЧП эффективно действовать в пределах национального законодательства, и одновременно способствует прозрачности, например в отношении того, какой информацией можно и нельзя обмениваться.
39. ГЧП могут иметь формальные или неформальные структуры и механизмы управления, как показано ниже. Некоторые партнерства начинали деятельность неформально, но впоследствии достигли определенного уровня формализации на основе механизмов, закрепленных в политике. Разнообразие применяемых структур отражает потребности, а также правовой и институциональный контекст различных юрисдикций.

Рисунок 3. Модели управления ГЧП



Источник: ответы на опрос.

¹⁶ Рекомендации 2, 20, 29 и 31 и пояснительные записки об обмене информацией.

Формальные ГЧП

40. Более половины респондентов (58%) указали, что используют формализованную модель ГЧП, основанную на институциональных механизмах управления, таких как:
 - меморандумы о взаимопонимании, протоколы или соглашения о сотрудничестве;
 - внутренние стандартные операционные процедуры (СОП) и механизмы управления;
 - защищенные системы связи или платформы управления делами;
 - отраслевые законы и нормативные акты, определяющие роли и пределы полномочий.
41. Даже в юрисдикциях с формальными ГЧП неформальный обмен также допускается и нередко имеет решающее значение для раннего предупреждения или получения информации до направления СПО.
42. К отдельным характеристикам формальных ГЧП относятся:
 - **Формат.** ГЧП организуют работу различными способами; периодичность и вид встреч зависят от механизмов управления и/или операционного характера партнерства. Встречи могут проводиться с разной периодичностью: ежеквартальные стратегические совещания, ежемесячные или проводимые раз в два месяца заседания операционных рабочих групп, а в отдельных случаях — ежедневный обмен или обмен почти в режиме реального времени.
 - Например, в давно действующих формальных ГЧП Сингапура и Южной Африки встречи проводятся примерно три-четыре раза в год. Аналогично десять рабочих групп ГЧП, деятельность которых обеспечивает ПФР Соединенного Королевства, встречаются три-четыре раза в год в соответствии с согласованным регламентом; в их состав входят участники из небанковских секторов, включая страхование, бухгалтерские услуги, аукционные дома и недвижимость.
 - В некоторых операционных ГЧП, например, в австралийском Fintel Alliance и британском JMLIT+, проводятся многочисленные заседания рабочих групп при ежедневном взаимодействии, ежемесячных тактических совещаниях, ежедневном поступлении информации и непрерывном обмене данными. В Латвии действует совместный операционный центр, где аналитики ПФР и сотрудники правоохранительных органов совместно работают над наиболее сложными и приоритетными уголовными делами, обеспечивая быстрый обмен информацией и согласованные операционные действия (OpCEN). В Южной Африке экспертные и тактические группы проводят совместные операционные совещания, обеспечивающие взаимодействие по делам в режиме реального времени. В Нидерландах операционные группы дважды в неделю рассматривают дела с высокой частотой возникновения. К другим важным характеристикам формальных ГЧП относятся:
 - о **Четкая правовая основа.** Наиболее распространенным препятствием для эффективного обмена информацией является правовая неопределенность. ГЧП функционируют наиболее эффективно, когда законодательство четко определяет роли, мандаты и разрешенные каналы обмена данными, а не только запреты.
 - о **Защита по принципу «безопасной гавани».** Развитые ГЧП, такие как COSMIC в Сингапуре, FLINT в Гибралтаре, JMLIT+ в Соединенном Королевстве и ряд инициатив ЕС, предусматривают положения о «безопасной гавани», защищающие частные организации, действующие добросовестно, от ответственности в соответствии с правилами банковской тайны или защиты данных.
 - о **Формальная документация.** Высокоэффективные ГЧП используют меморандумы о взаимопонимании, технические задания и письменные процедуры, устанавливающие гарантии конфиденциальности, порядок эскалации, структуры управления и ограничения использования данных.
 - о **Согласование с требованиями защиты данных.** Несмотря на то что нормы конфиденциальности часто называют ограничивающим фактором, около трех четвертей юрисдикций сообщили о наличии гарантий — шифрования, контроля доступа и журналов аудита, — позволяющих законно передавать конфиденциальную информацию.

43. Надежное управление обеспечивает предсказуемость, снижает институциональную склонность к избеганию рисков и формирует доверие, необходимое для операционного сотрудничества.

Неформальные ГЧП

44. Неформальные ГЧП действуют без меморандумов о взаимопонимании, формальных каналов или специально установленных ограничений на обмен данными. В рамках правовой среды каждой юрисдикции они опираются на гибкие механизмы, позволяющие ведомствам эффективно взаимодействовать без структурированного управления, административной поддержки или специально предусмотренной инфраструктуры обмена данными. Для таких механизмов характерны негласные договоренности между ведомствами, специальные консультации, личные рабочие контакты и координационные группы без формальных правовых документов.
45. Неформальные ГЧП опираются на доверенные сети и действуют через рабочие группы, отраслевые круглые столы, защищенные чаты и брифинги, разовые звонки с участием ПФР и правоохранительных органов, комитеты и очные встречи, на которых стороны могут обсуждать проблемы и совместно определять способы их решения. Ботсвана, Эсватини, Гана, Индонезия и Сейшельские Острова в настоящее время развивают неформальный обмен и ожидают, что их ГЧП расширятся до контролируемых неформальных форм взаимодействия. Коммуникация осуществляется через постоянные неформальные каналы, защищенные чаты, непосредственные контакты между аналитиками или офицеров связи.

Участники

46. Большинство ГЧП наряду с основным оператором партнерства включают внутренние ФУ. В другие входят зарубежные ФУ, центральный банк, регуляторы и надзорные органы и/или представители иных государственных ведомств, таких как таможенные органы, органы по интеллектуальной собственности, судебные и налоговые органы, а также организации более широкого финансового сектора: страховые, инвестиционные компании, участники рынка ценных бумаг, торговые организации, ПУВА и сторонние провайдеры платежных услуг. В меньшее число ГЧП входят представители других отраслей, включая бухгалтерские услуги, игровой бизнес и онлайн-игры, юридические услуги, онлайн-площадки, недвижимость, социальные сети, технологии, телекоммуникации, а также научно-образовательные организации и НКО/гражданское общество. Решение о принятии в состав ГЧП обычно принимает ведущая организация с учетом ряда факторов, включая:
- долю рынка;
 - склонность к риску;
 - значимость для возникающих угроз и подверженность им;
 - регуляторный статус;
 - способность содействовать достижению целей ГЧП;
 - готовность и способность предоставлять необходимую информацию и/или экспертные знания, относящиеся к угрозам и целям, а также объем такого вклада.
47. Для участия в ГЧП может потребоваться согласие, оформленное меморандумом о взаимопонимании или обязательством о конфиденциальности; в отдельных случаях оно сопровождается инструктажем по вопросам доступа к информации и информационным системам, их использования и обращения с ними. Австралия, Сингапур, Соединенные Штаты и британское JMLIT+ требуют проверки участников на благонадежность. В Перу, Ботсване, Гибралтаре и Соединенном Королевстве предусмотрены специальные процедуры или положения в меморандумах о взаимопонимании либо иных документах ГЧП, позволяющие при определенных обстоятельствах исключать участников.

48. По мере изменения потребностей и регуляторной среды ГЧП могут расширяться, включая новые отрасли и услуги. Например:

- в связи с регуляторными изменениями, ожидаемыми в июле 2026 года, Австралия сообщила, что рассмотрит возможность партнерства со специалистами по недвижимости, торговцами драгоценными металлами и камнями (ДМДК), юристами и провайдерами услуг траста или компаний (ПУТК);
- модели Кипра и Гибралтара предусматривают возможность включения в ГЧП провайдеров услуг виртуальных активов;
- в ОАЭ предполагается расширить механизм ГЧП за счет дополнительных компетентных органов и секторов, включая ПУВА, кибербезопасность, охрану окружающей среды и регулирование игровой деятельности;
- в Австрии ГЧП действуют в финансовом секторе — для банков и ПУВА/провайдеров услуг криптоактивов, — в юридических профессиях, для агентов по недвижимости, торговцев ДМДК и ПУТК в соответствии с законом о предпринимательской деятельности, а также для НКО. Планируется создание дополнительного ГЧП по вопросам игровой деятельности и партнерской инициативы между государственными органами с участием ПФР, правоохранительных органов — следователей различных специализаций — и судебной системы.

49. В «Комплексном обзоре рисков финансирования терроризма» ФАТФ и необязательных для исполнения руководящих принципах [по предупреждению, выявлению и пресечению использования новых и перспективных финансовых технологий в террористических целях \(Алжирские руководящие принципы\)](#) также рекомендуется расширять взаимодействие с секторами, которые в настоящее время не относятся к регулируемым субъектам, особенно с цифровыми и онлайн-платформами, например приложениями мгновенного обмена сообщениями, платформами онлайн-игр и развлечений, краудфандинговыми площадками и социальными сетями. Это необходимо для углубления взаимного понимания отраслевых угроз и включения стратегий снижения рисков ФТ и иных рисков в разработку продуктов. В данном контексте участники государственного и частного секторов могут совместно испытывать рыночные инновации, в том числе в регуляторных «песочницах», совместно выявлять риски, формировать общее понимание возникающих угроз и апробировать соразмерные регуляторные меры. Такое сотрудничество может поддерживаться структурированным диалогом с соответствующими провайдерами финансовых технологий и цифровых платформ для укрепления операционного и тактического анализа.

50. Разнообразный состав участников, вероятно, обеспечивает более значительную информационную отдачу, однако эту ценность необходимо сопоставлять с ресурсами, требуемыми для выполнения дополнительных управленческих обязанностей. Имеющиеся данные свидетельствуют о том, что технологии, например, дистанционное или виртуальное участие, могут облегчать участие в ГЧП.

Виды передаваемой информации

51. Информация, передаваемая через ГЧП, подразделяется в зависимости от цели на три широкие категории: i) стратегическая информация; ii) операционная информация; iii) информация о целях или лицах, представляющих интерес.

Блок 8. Виды и формы партнерств в зависимости от типа передаваемой информации

Партнерство по обмену стратегической информацией предполагает передачу между государственным и частным секторами агрегированных, контекстуальных и риск-ориентированных моделей для углубления общего понимания рисков ПОД/ФТ/ФРОМУ. В отличие от операционного или относящегося к конкретному делу обмена стратегический обмен сосредоточен не на идентифицируемых лицах или операциях, а на тенденциях, типологиях, которые, например, могут совместно разрабатываться в рамках ГЧП, уязвимостях и возникающих угрозах, наблюдаемых в различных секторах или юрисдикциях. Он может включать анализ развивающихся методов преступной деятельности, отраслевые оценки рисков или обезличенные модели подозрительной деятельности, направленные на формирование общего понимания среды рисков. Обмен стратегической информацией способствует разработке более эффективных риск-ориентированных подходов, укрепляет превентивные меры контроля и позволяет органам власти и подотчётным субъектам лучше предвидеть и снижать риски при соблюдении применимых требований защиты данных и конфиденциальности. Положения о «безопасной гавани» могут стимулировать участников ГЧП к обмену информацией, повышая эффективность противодействия незаконной финансовой деятельности.

Партнерства по обмену операционной информацией обеспечивают передачу своевременной, практически применимой и часто связанной с конкретным делом информации об инцидентах, лицах, организациях и связанной с ними финансовой деятельности. Такие механизмы обычно предусматривают обмен более конфиденциальной информацией, включая, если это разрешено, персональные и финансовые данные и сведения о подозреваемых, которые могут способствовать формированию финансовой разведывательной информации и в отдельных случаях использоваться в расследованиях. В этом контексте частный сектор выходит за рамки исключительно комплаенс-функции и становится участником выявления и анализа возможной незаконной деятельности. Операционный обмен помогает подотчётным субъектам повышать эффективность надлежащей проверки клиентов, совершенствовать мониторинг операций и выявлять клиентов повышенного риска и характерные модели их деятельности. Структура операционных ГЧП может различаться: одни объединяют широкий круг финансовых учреждений, другие используют более целевой подход, основанный на угрозах и возможностях, и сосредоточиваются на ключевых секторах или организациях, которые особенно подвержены риску либо лучше всего способны внести вклад в работу по конкретным направлениям риска. С учетом чувствительности и возможного использования такой информации операционный обмен в рамках ГЧП должен иметь четкую правовую основу и сопровождаться надлежащими гарантиями, включая конфиденциальность, защиту данных и, при необходимости, судебный или регуляторный контроль. В частности, когда информация предназначена для использования в следственных или прокурорских процедурах, надлежащим каналом остаются формальные механизмы обмена, установленные национальным законодательством. Таким образом, операционные ГЧП следует рассматривать как дополнительные инструменты, повышающие оперативность и качество финансовой разведывательной информации, но не заменяющие формальные процедуры, необходимые для доказательственных или судебных целей.

Гибридные партнерства: ГЧП, обменивающиеся как стратегической, так и операционной информацией.

Формы партнерств

- Специализированные совместно размещенные рабочие пространства с доступом только для назначенного персонала или ключевых участников, обеспечивающие сотрудничество в режиме реального времени по делам или операциям
- Специализированные коммуникационные платформы для обмена информацией
- Более целевое сотрудничество (включая двусторонние протоколы обмена информацией)
- Внутренний обмен информацией
- Наднациональный уровень; более постоянная структура
- Региональные инициативы РГТФ по государственно-частному сотрудничеству

Стратегическая информация

52. Большинство ГЧП обмениваются стратегической информацией. Поскольку такой обмен менее сложен с правовой точки зрения, он часто служит отправной точкой и механизмом укрепления доверия, помогая сформировать общее понимание рисков (см. пример Перу ниже). В дальнейшем юрисдикции могут переходить к обмену более чувствительной операционной информацией, способному существенно повысить эффективность расследований ОД/ФТ. К основным категориям стратегической информации относятся:

- **Типологии и риск-индикаторы («красные флаги»).** Они широко распространяются, чтобы помочь организациям выявлять подозрительные модели. Об обмене такой информацией сообщили более 75% юрисдикций.
- **Тенденции рисков и возникающие угрозы.** Многие юрисдикции обмениваются отраслевыми оценками рисков и тематическими выводами о развивающихся угрозах, таких как виртуальные активы и преступления с использованием цифровых технологий. Такой проактивный обмен помогает организациям предвидеть и снижать возникающие риски.
- **Информация о бенефициарных собственниках (владельцах).** Около трети участвовавших делегаций предоставляют доступ к данным о бенефициарных собственниках (владельцах), нередко через открытые источники или реестры, для повышения прозрачности и проведения надлежащей проверки.
- **Отчеты о деятельности и обратная связь по СПО.** Многие ПФР распространяют годовые отчеты, обратную связь по СПО и отраслевые оценки уязвимостей. Такой обмен повышает качество отчетности и укрепляет механизмы соблюдения требований.

Блок 9. ГЧП по обмену стратегической информацией

Механизм обмена финансовой информацией между государственным и частным секторами Перу (MERIF) был создан в сентябре 2024 года как постоянно действующий специализированный технический механизм без статуса юридического лица. Он предназначен **для защищенного, эффективного и совместного обмена стратегической и операционной информацией** между участниками государственного и частного секторов.

Для укрепления доверия и формирования эффективных рабочих механизмов между участниками MERIF первоначально отдал приоритет обмену **стратегической информацией**, такой как статистические данные, тенденции и модели. В этом контексте участники единогласно решили, что первыми результатами станут **Каталог типологий и Руководство по риск-индикаторам («красным флагам»)**, посвященные **незаконным финансовым потокам, связанным с торговлей людьми**. Такое решение **было обусловлено, в частности, национальной ситуацией, характеризующейся** растущим присутствием организованной преступности и ее операционным и финансовым сближением с торговлей людьми; **низкой результативностью правоприменения в отношении незаконных финансовых потоков, полученных от этого преступления**; а также необходимостью объединить ранее разрозненные усилия заинтересованных сторон частного сектора для углубления понимания **экономических и финансовых аспектов торговли людьми**. Цель инициативы — увеличить количество и повысить качество СПО, связанных с торговлей людьми, **а также укрепить возможности системы ПОД/ФТ по предупреждению и выявлению** в соответствии с установленными рисками.

Источник: Перу

53. Одним из важных направлений использования ГЧП является их вклад в национальные оценки рисков (НОР), а также другие оценки и стратегии, между которыми существует постоянный цикл обратной связи, показанный на рисунке 4 ниже. ГЧП могут выявлять и оценивать угрозы для включения в НОР, а деятельность ГЧП может инициироваться в ответ на риски, установленные в НОР. НОР, в свою очередь, способствует дальнейшему и постоянному выявлению рисков и углублению их понимания, что влияет на меры ПОД/ФТ/ФРОМУ, включая надзор. Создание и корректировка ГЧП должны отражать национальные приоритеты.

Рисунок 4. Цикл обратной связи между ГЧП и национальной оценкой рисков



Источник: ответы на опрос

Операционная информация

54. Операционный обмен обеспечивает практически применимую информацию, которая ускоряет расследования и укрепляет соблюдение требований, и может включать следующие категории:

- информация по конкретным делам;
- информация об операциях: обычно передается юрисдикциями через защищенные платформы, такие как Защищенная сеть Группы «Эгмонт» (ЗСЭ), THEMIS, например, защищенная платформа ПФР Гибралтара, или специализированные платформы, созданные для конкретной юрисдикции либо координирующего органа ГЧП;
- данные надлежащей проверки клиентов (НПК/ЗСК): обмениваются юрисдикциями в контролируемой среде, как правило, для расследования конкретных дел;
- требования правоохранительных или судебных органов;
- финансовые метаданные для поддержки сетевого анализа и отслеживания незаконных потоков;

- геолокационные данные: предоставляются отдельными юрисдикциями по делам высокого риска;
- данные коммуникаций: передаются некоторыми юрисдикциями, включая Гонконг, Китай и Гибралтар, как правило, на основании судебных постановлений;
- массовые массивы данных: доступны в ограниченных случаях при соблюдении дополнительных процедур и правил;
- биометрические данные: считаются особой категорией данных в соответствии с Общим регламентом ЕС по защите данных (GDPR) и передаются только при соблюдении строгих условий.

55. Более половины юрисдикций участвуют в «углубленном» операционном обмене, который может включать информацию по конкретным делам, данные об операциях или сведения о подлежащей проверке клиентов (НПК) (см. примеры в блоке 10 ниже).

Блок 10. ГЧП по обмену операционной информацией, устраняющие информационные пробелы

Албания

В Албании действует несколько ГЧП в целях ПОД/ФТ/ФРОМУ. Как правило, они предусматривают сотрудничество между СПАК (Специальной структурой по борьбе с коррупцией и организованной преступностью), ПФР Албании (DPPP), банками, УНФПП и другими соответствующими заинтересованными сторонами частного сектора для достижения различных целей.

К основным ГЧП Албании относится проект iPROCEEDS, созданный 30 января 2019 года и сосредоточенный на борьбе с киберпреступностью и преступными доходами в интернете. Операционная деятельность включает целевые совместные встречи, обмен оперативной информацией и обучение. Первоначально проект был посвящен одному вопросу, однако постепенно охватил более широкий круг рисков, связанных с финансовыми преступлениями в интернете и сотрудничеством между государственным и частным сектором.

Источник: Албания

Малайзия

В 2017 году Малайзия создала Малайзийскую сеть финансовой разведки (MyFINet). В рамках MyFINet действуют шесть тематических рабочих групп, распределенных по видам преступлений: коррупция, контрабанда, преступления на рынке ценных бумаг, налоговые преступления, ФТ и ФРОМУ. Основная цель MyFINet — обеспечить более системный обмен оперативной информацией по конкретным уголовным делам и актуальным вопросам между ПФР, правоохранительными органами и ФУ. В период с 2019 года по февраль 2025 года на заседаниях рабочих групп MyFINet было рассмотрено 61 дело, а ПФР передало 44 материала финансовой разведки, в том числе о выявлении нелегальной деятельности с виртуальными активами (см. блок 6.6 в отчете о взаимной оценке Малайзии 2025 года).

Источник: Малайзия

Правовые и регуляторные аспекты обмена информацией

56. Юрисдикции назвали три основные причины, по которым обмен информацией иногда ограничивается:

- **правовые препятствия или отсутствие правовых оснований** — отсутствие законодательной или иной правовой основы для передачи закрытых/операционных данных субъектам частного сектора за пределами традиционных каналов правоохранительных органов и ПФР;
- **институциональные ограничения** — недостаток ресурсов, отсутствие ИТ- и технической инфраструктуры, фрагментированность государственных органов, приводящая к несогласованности ролей и ожиданий; и
- **ограничения, связанные с доверием и культурой** — опасения заинтересованных сторон государственного и частного секторов по поводу ненадлежащего использования или компрометации информации, а также консервативный подход государственных органов к передаче закрытых/операционных данных.

57. Многие респонденты отметили важность постоянного взаимодействия с органами по защите данных для разработки устойчивой и надлежащей правовой основы, устраняющей препятствия (см. блок 11 ниже), в то время как многие другие еще не наладили взаимодействие с такими органами. В части преодоления проблем доверия ответы на опрос указывают на целесообразность начинать со стратегического обмена информацией, а затем переходить к более глубокому взаимодействию.
58. В случаях, когда проблемами являются отсутствие ИТ- и технической инфраструктуры и ресурсов, а также в целом при создании первых ГЧП, некоторые юрисдикции обращались к провайдерам технического содействия.

Блок 11. Взаимодействие с органами по защите данных для успешной деятельности ГЧП

Ботсвана

В рамках своего ГЧП (Оперативной группы и Форума государственно-частного партнерства Ботсваны) ПФР сотрудничает с органом по защите данных — Комиссией по защите данных, обеспечивая соблюдение законодательства о защите данных, а также участвует в информационно-разъяснительных программах, в ходе которых Комиссия представляет положения Закона о защите данных и повышает осведомленность о них.

Источник: Ботсвана

Информационные потоки в рамках обмена информацией ГЧП

59. Обмен информацией в рамках ГЧП включает три основных направления: 1) от государственного сектора к частному; 2) от частного сектора к государственному; 3) между субъектами частного сектора. Первые два рассматриваются в других разделах отчета при описании видов ГЧП. Механизмы обмена между субъектами частного сектора иногда обеспечиваются ГЧП или действуют в его рамках. В большинстве юрисдикций такой обмен является наименее зрелым направлением деятельности ГЧП и может требовать благоприятствующей правовой основы и соответствующей инфраструктуры данных.
60. Практический пример и некоторые примеры развития этого направления в отдельных странах приведены в блоке 12 ниже.

Механизмы обмена между субъектами частного сектора

61. В Соединенном Королевстве обмен информацией между субъектами частного сектора обеспечивается двумя законодательными актами:

- Закон об уголовных финансах 2017 года позволяет банкам и другим организациям регулируемого сектора добровольно обмениваться информацией при наличии подозрений о том, что лицо занимается отмыванием денег, либо подозрений в причастности лица к совершению преступления финансирования терроризма, а также в связи с выявлением имущества террористов, его перемещением или использованием. Обмен может быть инициирован как организацией регулируемого сектора, так и Национальным агентством по борьбе с преступностью Соединенного Королевства (НСА). Любой участник регулируемого сектора вправе отказаться от такого обмена. При добросовестной передаче информации состав преступления, связанного с предупреждением клиента, отсутствует. Любые обязанности по направлению сообщений об отмывании денег или финансировании терроризма, возникающие в ходе обмена, исполняются путем направления в ПФР Соединенного Королевства обычного сообщения о подозрительной деятельности (СПД). Вместе с тем данное положение законодательства применяется редко: в 2020–2021 годах оно использовалось лишь шесть раз, а после этого не применялось.
- Отдельно Закон об экономической преступности и корпоративной прозрачности 2023 года (ЕССТА) предусматривает добровольный обмен информацией, позволяющий организациям регулируемого сектора Соединенного Королевства напрямую передавать сведения друг другу в целях предупреждения, выявления или расследования экономических преступлений. Рабочие группы ПФР Соединенного Королевства активно совершенствуют обмен между своими участниками; предстоящие межотраслевые заседания рабочих групп, организуемые ПФР, отдельно сосредоточены на формировании отношений, способствующих межотраслевому обмену между субъектами частного сектора. Результаты по всему финансовому сектору Соединенного Королевства демонстрируют практическую ценность обмена в соответствии с ЕССТА для управления рисками экономической преступности. В выборке из шести финансовых учреждений 65% расследований, начатых на основании переданной оперативной информации, привели к принятию получившей ее организацией положительных мер по управлению рисками.

Блок 12. Практический пример и механизмы обмена информацией между субъектами частного сектора

Практический пример обмена между субъектами частного сектора в Соединенном Королевстве

Банк А передал Банку В информацию в соответствии со статьей 188 британского Закона об экономической преступности и корпоративной прозрачности (ЕССТА), предупредив о подозрении в отмывании денег. Предупреждение касалось клиента, который за короткий период внес несколько крупных сумм наличными и быстро перевел средства на счет в Банке В.

Сопоставив эту информацию с внутренними данными, Банк В установил, что клиент является частью крупной взаимосвязанной сети физических лиц и компаний. Было оценено, что сеть оказывает услуги подпольного банкинга.

Расследование установило, что через сеть прошло более 10 млн фунтов стерлингов, включавших как законные, так и незаконные средства. В результате Банк В направил сообщения о подозрительной деятельности и ограничил операции на сумму свыше 1 млн фунтов стерлингов по счетам, связанным с сетью. Впоследствии правоохранительный орган обеспечил замораживание 159 000 фунтов стерлингов на основании постановлений о замораживании счетов; уголовные расследования продолжаются.

Обмен оперативной информацией позволил Банку В принять более масштабные меры по пресечению. Банк В направил другим финансовым учреждениям еще семь предупреждений об обмене информацией в соответствии с ЕССТА, содействуя дополнительным мерам во всей финансовой системе.

Банк В также разработал правила мониторинга операций для выявления аналогичной деятельности. Только в ходе тестирования новое правило сформировало более 200 предупреждений, что привело к направлению более 80 дополнительных сообщений о подозрительной деятельности, замораживанию еще 515 000 фунтов стерлингов на основании постановлений о замораживании счетов и выявлению пяти новых возможностей обмена информацией с другими организациями в соответствии с ЕССТА.

Этот пример показывает, что своевременный и целевой обмен информацией при противодействии организованным преступным сетям может создавать мощный мультипликативный эффект, позволяя финансовым учреждениям и правоохранительным органам выявлять скрытые сети, пресекать преступную деятельность и защищать финансовую систему в целом.

Источник: Соединенное Королевство

Механизмы обмена между субъектами частного сектора

Канадская модель обмена информацией между субъектами частного сектора

В Канаде обмен информацией между субъектами частного сектора в целях предупреждения отмывания денег, финансирования терроризма (ПОД/ФТ) и обхода санкций разработан с надлежащими ограничениями и надзором, обеспечивающими надежную защиту данных и конфиденциальности, и одновременно достаточно гибок для организаций, добровольно решивших участвовать.

В 2024 году изменения в канадское законодательство о ПОД/ФТ и Закон о доходах от преступной деятельности (PCMLTFA) предоставили регулируемым субъектам частного сектора возможность добровольно обмениваться информацией друг с другом в целях

ПОД/ФТ и обхода санкций. Нормативные акты, обеспечивающие практическое применение законодательных изменений, вступили в силу 4 марта 2025 года и установили параметры использования механизма регулируемые организациями, включая обязанность разработать и соблюдать утвержденный кодекс практики, регулирующий обмен информацией.

Благодаря обмену информацией регулируемые организации получают дополнительные сведения и данные, поддерживающие их способность выявлять подозрительные операции, точно оценивать риски, обосновывать риск-ориентированные меры и соблюдать обязанности, включая направление СПО в FINTRAC.

Защита конфиденциальности персональной информации обеспечивается обязательными кодексами практики, которые рассматриваются и утверждаются федеральным органом Канады по вопросам конфиденциальности — Управлением комиссара по вопросам конфиденциальности. Кодекс должен подтверждать, что обмен информацией соответствует всем применимым законам и обеспечивает гарантии конфиденциальности, предусмотренные федеральным законодательством Канады. До начала любого обмена Управление комиссара должно официально утвердить кодекс практики; установленный законом срок рассмотрения и принятия решения составляет до 135 календарных дней.

Источник: Канада

Германия: SafeAML

По оценкам, в 2021 году отмывание денег и финансовое мошенничество обошлись ЕС в 133 млрд евро. Для предупреждения такой деятельности нормативные акты Германии и ЕС требуют от банков контролировать финансовые операции на предмет подозрений в ОД. Однако правила защиты данных запрещают им напрямую обмениваться данными об операциях, что затрудняет выявление преступной деятельности. Запросы информации обеспечивают ограниченный обмен между финансовыми учреждениями, но действующий ручной процесс является дорогостоящим и длительным.

Проект SafeAML помогает финансовым учреждениям противодействовать ОД посредством цифровизации существующих коммуникационных процессов обмена информацией. Это должно сократить расходы и ускорить выявление преступной деятельности. Кроме того, SafeAML позволяет анализировать связи между потенциально подозрительными операциями. Результаты такого межорганизационного анализа передаются только участвующим организациям. Ни EuroDaT, ни третьи лица не имеют доступа к данным об операциях. Соответствующая процедура согласована с органом земли Гессен по защите данных.

Инициатива функционирует в рабочем режиме с конца апреля 2025 года, то есть участники уже обмениваются актуальной информацией через доверенного посредника.

В настоящее время к сети подключены три немецких банка. SafeAML открыта для всех кредитных организаций Германии и Европы.

Деятельность инициативы обеспечивает EuroDaT, принадлежащая земле Гессен; ее цель — цифровизация запросов информации. EuroDaT выступает «доверенным посредником» информации: все остальные участники, которым требуются сведения, направляют запрос через посредника, который затем сопоставляет получателей с необходимыми им данными. Федеральное управление финансового надзора Германии (BaFin) непосредственно не участвует в инициативе, но следит за ее развитием, особенно в контексте будущего европейского регулирования в соответствии со статьей 75 Регламента о ПОД. Инициатива рассматривает себя как возможную форму партнерства в смысле данного положения.

Источник: Германия

Сингапурская платформа совместного обмена информацией и материалами дел об отмытии денег/финансировании терроризма (COSMIC)

В Сингапуре действует цифровая платформа «Совместный обмен информацией и материалами дел об отмытии денег/финансировании терроризма» (COSMIC), совместно разработанная Денежно-кредитным управлением Сингапура (MAS) и шестью крупнейшими коммерческими банками. В настоящее время COSMIC сосредоточена на трех ключевых рисках, определенных национальным руководящим комитетом по ПОД/ФТ как приоритетные для снижения: 1) неправомерное использование юридических лиц; 2) отмытие денег через торговые операции; 3) финансирование распространения оружия массового уничтожения. COSMIC позволяет банкам-участникам безопасно обмениваться информацией о клиентах, счета которых вызывают опасения в связи с возможными финансовыми преступлениями, что облегчает выявление и предупреждение преступной деятельности. MAS имеет доступ ко всей информации, передаваемой через платформу, чтобы контролировать надлежащее использование COSMIC банками-участниками и выполнять более широкие надзорные и контрольные функции, обеспечивая наличие у финансовых учреждений надежных механизмов защиты от финансовой преступности.

Источник: Сингапур

Французская платформа обмена информацией между субъектами частного сектора о счетах, предположительно используемых в мошеннических схемах

6 ноября 2025 года Парламент Франции принял закон о совершенствовании мер по борьбе с мошенничеством в банковском секторе, создавший правовую основу для обмена между субъектами частного сектора информацией о счетах, вызывающих подозрения в связи с мошенничеством.

На этой основе 7 мая 2026 года был запущен Национальный реестр счетов, отмеченных как несущие риск мошенничества. Новая система, размещенная в Банке Франции — центральном банке страны, — позволяет банкам и, в более широком смысле, провайдером платежных услуг обмениваться сообщениями об IBAN, признанных подозрительными, тем самым укрепляя коллективную способность сектора предупреждать мошенничество с банковскими переводами. После внесения IBAN в базу данных уведомление может быть направлено всему банковскому сообществу, которое соответствующим образом корректирует процедуры проверки перед переводом. Таким образом, частные субъекты могут взаимно сообщать о рисках мошенничества и совместно совершенствовать его выявление и предупреждение.

Система разработана с применением строгих гарантий защиты персональных данных. В базе не фиксируется информация, позволяющая установить личность: передаются только IBAN. Кроме того, данные хранятся ограниченный срок — 13 месяцев, — соразмерный потребностям борьбы с мошенничеством. Эти положения направлены на обеспечение баланса между операционной эффективностью системы и соблюдением прав владельцев счетов.

Источник: Франция

Индийский реестр счетов подставных лиц

Национальный портал сообщений о киберпреступлениях (NCRP). Индийский координационный центр по борьбе с киберпреступностью (I4C) разместил на портале негативный реестр всех счетов подставных лиц и связанных с ними идентификаторов ЗСК. Все финансовые учреждения могут использовать реестр как индикатор риска. Они применяют его при установлении деловых отношений, а также в ходе постоянной надлежащей проверки и усиленного мониторинга.

Источник: Индия

Другие соответствующие механизмы, указанные в ответах на опрос

Американский «механизм статьи 314(b)» FinCEN представляет собой добровольную программу обмена информацией между финансовыми учреждениями на условиях «безопасной гавани», обеспечивающей защиту от ответственности, для более эффективного выявления деятельности, которая может быть связана с ОД/ФТ, и направления соответствующих сообщений.

В рамках британского ГЧП Data Fusion Тактическая разведывательная группа банковского сектора осуществляет обмен информацией между субъектами частного сектора. В Мексике также действует механизм, поддерживаемый Ассоциацией банков Мексики.

Внутренние государственно-частные партнерства по обмену информацией

62. В настоящем разделе рассматривается обмен информацией ГЧП внутри страны. Примерно половина ГЧП может передавать сведения за пределы основного состава участников, однако с некоторыми ограничениями: передаваемые данные могут ограничиваться стратегической информацией; получателями могут быть только доверенные организации или секторы, куда могут входить не все подотчётные субъекты, поскольку доверие является предварительным условием; данные могут обезличиваться; могут применяться дополнительные меры защиты, гарантии и условия обращения, ограничивающие последующую передачу информации; либо может требоваться правовое разрешение или письменное согласие владельцев информации и/или участников ГЧП.
63. Информация, полученная в рамках ГЧП, при необходимости также может публиковаться. Например, Латвия размещает на веб-сайте ПФР отчеты стратегического анализа, подготовленные в рамках или в связи с деятельностью ГЧП, а Люксембург распространяет оценки рисков по подсекторам или отдельным направлениям. Национальное агентство по борьбе с преступностью Соединенного Королевства публикует на своем веб-сайте предупреждения JMLIT+ и журнал ПФР Соединенного Королевства, который также широко распространяется каждые четыре месяца и содержит статьи о тенденциях, предупреждения и рекомендации по передовым практикам. ПФР Соединенного Королевства также публикует обезличенные практические примеры, демонстрирующие, как сообщения о подозрительной деятельности способствовали расследованиям, и активно использует социальные сети для распространения информации среди более широкой аудитории.
64. Как координатор обмена информацией JMLIT+ Национальное агентство по борьбе с преступностью Соединенного Королевства вправе в соответствии с законом передавать полученную от участников JMLIT+ информацию любому другому лицу, которое считает надлежащим, при условии, что передача осуществляется для выполнения функции агентства и разрешенной цели. При этом оно всегда запрашивает согласие основного участника, предоставившего ин-

формацию. Канада публикует операционные предупреждения и бюллетени на сайте своего ПФР, распространяя через инициативы ГЧП типологии и индикаторы, связанные с приоритетными направлениями высокого риска.

65. Канадская модель ГЧП создает прямой канал передачи информации от частного сектора государственному, позволяя ПФР Канады готовить проактивную финансовую информацию по ряду преступлений высокого риска, включая торговлю людьми, сексуальную эксплуатацию детей в интернете, романтическое мошенничество, незаконный оборот фентанила, незаконную деятельность с каннабисом и незаконную торговлю объектами дикой природы. Благодаря этой модели ПФР может проактивно передавать правоохранительным органам финансовую информацию на основе сведений, полученных от частного сектора. Она повысила скорость работы и способность канадской системы проактивно выявлять более сложные преступления в рамках различных ГЧП.

Многоюрисдикционные и трансграничные государственно-частные партнерства по обмену информацией

66. Трансграничное сотрудничество широко признается необходимым для пресечения транснациональных сетей ОД/ФТ и предикатных преступлений, а ГЧП обеспечивают структурированный канал такого взаимодействия. Ответы на опрос свидетельствуют об устойчивом прогрессе на стратегическом уровне, особенно в обмене типологиями, тенденциями и индикаторами риска, тогда как операционное сотрудничество между юрисдикциями остается неравномерным.
67. Страны сообщают об углублении понимания типологий финансовых преступлений, повышении качества оценки рисков и эффективности расследований благодаря согласованным действиям, таким как совместный сбор доказательств и двустороннее сотрудничество. Успешные модели показывают, что для преобразования стратегической информации в операционные результаты необходимы четкие правовые основания, например, меморандумы о взаимопонимании с установленными гарантиями, защищенные многоуровневые платформы обмена информацией, стандартизированные типологии и каналы оперативного реагирования по срочным делам. Кроме того, для обеспечения эффективного сотрудничества критически важны меры укрепления доверия, такие как совместное обучение, прикомандирование сотрудников и регулярное тактическое взаимодействие. В целом стратегический обмен информацией уже хорошо развит, однако расширение трансграничных операционных ГЧП потребует дальнейшего правового, технического и институционального развития, чтобы превратить эти механизмы в надежные инструменты пресечения транснациональной преступности.
68. Некоторые ГЧП изначально охватывают несколько юрисдикций, например, EFIPPP, исходя из общих потребностей и интересов. Другие внутренние ГЧП допускают разовый или осуществляемый по конкретному делу трансграничный обмен с государствами, не входящими в партнерство.
69. Новейший пакет нормативных актов ЕС в сфере противодействия отмыванию денег, в частности статья 75 Регламента (ЕС) 2024/1624, создает значительные возможности для обеспечения и облегчения обмена и обработки информации между подотчетными субъектами и, при необходимости, компетентными органами через специализированные партнерства. В поддержку этой работы EFIPPP под руководством председателя Рабочей группы EFIPPP по правовым основаниям обмена информацией (LGWG) и в консультации с различными партнерами создало экспертную платформу. Она призвана содействовать обмену идеями для подготовки практического руководства по созданию группы в соответствии с правовой основой статьи 75 Регламента ЕС о ПОД.

70. Трансграничные ГЧП чаще всего возглавляются ПФР. Соответственно, они обмениваются информацией через Группу «Эгмонт» и другие доступные ПФР платформы, что является преимуществом.
71. Инициативы, подобные региональному ГЧП, разрабатываемому при поддержке региональной группы по типу ФАТФ — Группы по борьбе с отмыванием денег в Восточной и Южной Африке (ЕСААМЛГ), — также опираются на существующее взаимодействие между ПФР, как указано в блоке 13 ниже.

Блок 13. Региональное государственно-частное партнерство ЕСААМЛГ

ЕСААМЛГ в настоящее время создает государственно-частное партнерство по обмену финансовой информацией (FISP) как гибридное партнерство, объединяющее стратегические и операционные элементы и позволяющее разрабатывать типологии и взаимодействовать по конкретным делам в отношении распространенных в регионе финансовых преступлений высокого риска. Его цели — повысить качество, актуальность и своевременность СПО; укрепить аналитические возможности ПФР; поддержать проактивные расследования; и в конечном счете способствовать устойчивости и целостности финансовых систем региона.

Источник: ЕСААМЛГ

72. Несколько ГЧП обмениваются информацией с международными партнерами по конкретным делам через различные механизмы, а не только каналы ПФР, в соответствии с законодательством, политиками в отношении данных и гарантиями конфиденциальности. Другие выявленные ГЧП передают информацию на международном уровне чаще или регулярно в рамках формальных и неформальных механизмов. К значимым примерам относятся:

- **Проект Сингапура FRONTIER+** показывает, как различные внутренние ГЧП могут взаимодействовать друг с другом на транснациональном уровне. FRONTIER+, инициированный Сингапурским центром по противодействию мошенничеству в октябре 2024 года, является транснациональным альянсом органов по борьбе с мошенничеством из 13 юрисдикций по состоянию на конец 2025 года, объединяющим стратегии противодействия мошенничеству на транснациональном уровне. Через этот альянс каждый орган, занимающийся противодействием мошенничеству (который сам может являться внутренним ГЧП), может взаимодействовать с другими организациями посредством обмена тенденциями мошенничества и передовыми практиками. Особенно важно, что альянс создает основу для обмена оперативной информацией в режиме реального времени, совместных операций и согласованного правоприменения в отношении транснационального мошенничества и уже обеспечил положительные результаты. Две совместные операции участников FRONTIER+ в 2025 году привели к задержанию 2 100 лиц во всех юрисдикциях и изъятию около 28,2 млн сингапурских долларов с более чем 36 000 замороженных банковских счетов.
- **Австралийский Fintel Alliance и механизм «Пять глаз»** проводят круглый стол государственного и частного секторов с участием ПФР государств — участников «Пяти глаз»¹⁷. ПФР обмениваются выводами о текущих тенденциях финансовой преступности, углубляют понимание новых и возникающих рисков и укрепляют региональные связи. Международный обмен разрешен законодательством Австралии в сфере ПОД/ФТ.

¹⁷ Австралия, Канада, Новая Зеландия, Соединенное Королевство и Соединенные Штаты.

- **Гибралтар** активно участвует в международном обмене благодаря членству своего ГЧП в EFIRPP и отношениям по обмену информацией с британским JMLIT+. Через эти платформы партнерство передает выводы, типологии и тематическую оперативную информацию, а также получает ценные сведения от международных партнеров, включая предупреждения JMLIT+, новые типологии, риск-индикаторы («красные флаги») и исследовательские документы EFIRPP. При необходимости они распространяются среди участников ГЧП Гибралтара, повышая их осведомленность о ситуации и понимание рисков. Такой взаимный обмен укрепляет внутренние возможности Гибралтара в сфере финансовой разведки и его вклад в более широкое международное сообщество ПОД/ФТ/ФРОМУ, обеспечивая соответствие деятельности Гибралтара международным стандартам и учет последних международных событий и передовых практик. ПФР также входит в Форум четырех — региональное стратегическое объединение ПФР, через которое распространяет передовые практики посредством рабочей группы по ГЧП.
- **Форум четырех островных юрисдикций.** Хотя он не является многоюрисдикционным ГЧП в строгом смысле, Форум подразделений финансовой разведки Гибралтара, Гернси, острова Мэн и Джерси обеспечивает обмен опытом и передовыми практиками. Участники совместно подписали меморандум о взаимопонимании с Национальным агентством по борьбе с преступностью Соединенного Королевства, чтобы облегчить обмен информацией между ПФР четырех островных юрисдикций и британским ГЧП JMLIT+. Это интересный пример того, как региональное ГЧП может стать шагом к многоюрисдикционному партнерству.
- **Финансовая оперативная группа United for Wildlife** включает систему обмена информацией о последних тенденциях, риск-индикаторах («красных флагах») и типологиях, которая помогает участникам определять и реализовывать конкретные меры финансового сектора по борьбе с незаконной торговлей объектами дикой природы. В группу входит более 60 финансовых учреждений, преимущественно из банковского сектора — корпоративного, инвестиционного, онлайн-, розничного и оптового банкинга — и организаций, оказывающих услуги денежных переводов. United for Wildlife создала семь региональных отделений, чтобы:
 - о сосредоточиться на проблемах, характерных для конкретных регионов, и разрабатывать передовые практики и решения с учетом местных условий;
 - о укреплять межотраслевое доверие с участием экспертов правоохранительных органов, финансовых учреждений, природоохранных и транспортных организаций.

Южноафриканское отделение сотрудничало с SAMLIT, ГЧП Южной Африки, при проведении финансовых расследований, включая возобновление ранее закрытых расследований, по делам о крупномасштабной незаконной торговле объектами дикой природы.
- **ПФР Канады (FINTRAC)** содействовало запуску проекта Anton — международного ГЧП, объединяющего внутренних и международных заинтересованных участников для повышения осведомленности о незаконной торговле объектами дикой природы и улучшения выявления отмывания доходов от этого преступления. В рамках инициативы FINTRAC подготовило операционное предупреждение на основе внутреннего стратегического анализа, международных исследований и информации партнеров проекта Anton. В предупреждении опубликованы индикаторы и типологии, помогающие выявлять предполагаемую незаконную торговлю объектами дикой природы и поддерживающие организации и органы как в Канаде, так и в других юрисдикциях при выявлении соответствующей финансовой деятельности. Канада под руководством Агентства налоговых поступлений также участвует в J5 — Объединении руководителей налоговых правоохранительных органов — и Глобальном партнерстве финансовых учреждений (GFIP), международном ГЧП по противодействию транснациональным налоговым преступлениям и ОД. В GFIP входят представители налоговых органов, ФУ и ПФР.

- **EFIRPP**. В Европейском союзе действует одно транснациональное ГЧП — Государственно-частное партнерство Европола в области финансовой разведки (EFIRPP), которое считается первым транснациональным механизмом обмена информацией, созданным в сфере ПОД/ФТ. EFIRPP, учрежденное в 2017 году, обеспечивает среду для трансграничного сотрудничества и обмена информацией между Европолом, компетентными органами, включая ПФР и правоохранительные органы, и регулируемые провайдером финансовых услуг, такими как банки. В настоящее время оно объединяет 98 организаций из более чем 31 государства ЕС и третьих стран, включая 17 правоохранительных органов, 28 ПФР и 30 ФУ, а также наблюдателей — международные организации, банковские ассоциации и аналитические центры. EFIRPP ставит следующие задачи:
 - o формирование общей картины оперативной информации и понимания рисков финансовой преступности;
 - o содействие обмену операционной или тактической информацией, связанной с текущими расследованиями;
 - o выявление правовых оснований для обмена информацией и содействие уточнению регуляторных ограничений;
 - o продвижение новых инструментов противодействия финансовой преступности;
 - o поддержка внутренних и аналогичных площадок сотрудничества в соответствующих юрисдикциях.

Одним из недавних значимых результатов стала публикация «Практического руководства EFIRPP по операционному сотрудничеству между следственными органами и финансовыми учреждениями»¹⁸.

- **Тунис** в 2021 году создал платформу Hannibal как программный интерфейс приложения (API) и ГЧП для понимания, выявления и мониторинга национальных рисков ОД/ФТ, связанных с физической трансграничной перевозкой валюты, с использованием технологии блокчейн, объединяющей несколько баз данных, в том числе банков и обменных пунктов¹⁹. Тунисский комитет финансового анализа (СТАФ), являющийся ПФР Туниса, может передавать полученную через Hannibal информацию зарубежным ПФР. Ниже приведен пример того, как платформа помогла выявить сеть контрабандистов наличной валюты.

¹⁸ Доступно по адресу: <https://www.europol.europa.eu/publications-events/publications/efirpp-practical-guide-for-operational-cooperation-between-investigative-authorities-and-financial-institutions>.

¹⁹ ФАТФ (2021), «Возможности и проблемы новых технологий в сфере ПОД/ФТ», ФАТФ, Париж, Франция, с. 33, <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf.coredownload.inline.pdf> (дата обращения: 5 мая 2026 года).

Блок 14. Государственно-частное партнерство и технология блокчейн для выявления трансграничной контрабанды наличной валюты

СТАФ получил от таможенных органов запрос о сотрудничестве в связи с текущим расследованием в отношении двух граждан Туниса, ввозивших из-за рубежа в Тунис значительные суммы иностранной валюты наличными и зачислявших их на счета тунисских компаний. Предположительно эти компании осуществляли фиктивные экспортные операции и не репатриировали экспортную выручку, чтобы пополнять свои счета и уклоняться от судебного преследования. Расследование, проведенное ПФР Туниса с использованием платформы Hannibal и номеров паспортов, предоставленных таможенными органами, позволило установить: операции по ввозу иностранной валюты, совершенные двумя подозреваемыми, включая номер таможенной декларации, пограничный пункт, заявленную сумму, дату декларации и сумму, урегулированную по каждой операции (под урегулированной суммой понимается ввезенная из-за рубежа валюта, которая была обменена или внесена на банковские счета); урегулированные суммы; неурегулированные суммы; две компании, на счета которых вносились ввезенная валюта, номера их счетов, даты внесения и отделения, в которых проводились операции; конечное назначение средств, зачисленных на счета компаний. Исследование показало, что один из подозреваемых подал две таможенные декларации с использованием недавно выданного паспорта, сведения о котором отсутствовали у таможенных органов Туниса на момент запроса о сотрудничестве. Были также выявлены другие лица, действовавшие в тот же период и не являвшиеся предметом запроса о сотрудничестве, которые ввозили иностранную валюту и затем вносили ее на банковские счета тех же тунисских компаний. Расследование с использованием платформы Hannibal позволило определить общую сумму и назначение иностранной валюты, ввезенной двумя подозреваемыми, установить бенефициаров и раскрыть сеть лиц, причастных к незаконному трансграничному перемещению наличной валюты.

Источник: Тунис

73. Соединенные Штаты создавали с Мексикой и Канадой несколько ГЧП для конкретных целей. Для уточнения правовой основы в 2025 году FinCEN выпустило руководство «Трансграничный обмен информацией финансовыми учреждениями и конфиденциальность сообщений о подозрительной деятельности», разъясняющее, что Закон о банковской тайне не запрещает трансграничный обмен. Налоговая служба США также участвует в Глобальном партнерстве финансовых учреждений J5^{20, 21} и кибер-/криптовалютном испытании J5.
74. Хотя единого международного ГЧП не существует, информация может передаваться из внутреннего ГЧП международным партнерам. Например, сведения, которыми обмениваются группы британского JMLIT+, нельзя передавать за пределы участвующих субъектов частного сектора, однако каждый участник может распространять их внутри собственной глобальной группы. Операционная группа JMLIT+ передавала отдельные запросы операционной информации другим ГЧП, включая австралийский Fintel Alliance, а также получала и поддерживала запросы из Соединенных Штатов. JMLIT+ в настоящее время испытывает обмен операционной и стратегической информацией с партнерскими ГЧП в коронных владениях и заморских территориях Соединенного Королевства — Гибралтаре, Гернси, на острове Мэн и Джерси. Страте-

²⁰ Как отмечалось выше, разведывательный альянс, объединяющий Австралию, Канаду, Новую Зеландию, Соединенное Королевство и Соединенные Штаты.

²¹ J5 означает Объединение руководителей налоговых правоохранительных органов — партнерство Австралийского налогового управления (ATO), Агентства налоговых поступлений Канады (CRA), Нидерландской службы фискальной разведки и расследований (FIOD), Налогово-таможенной службы Его Величества Соединенного Королевства (HMRC) и Управления уголовных расследований Налоговой службы США (IRS-CI).

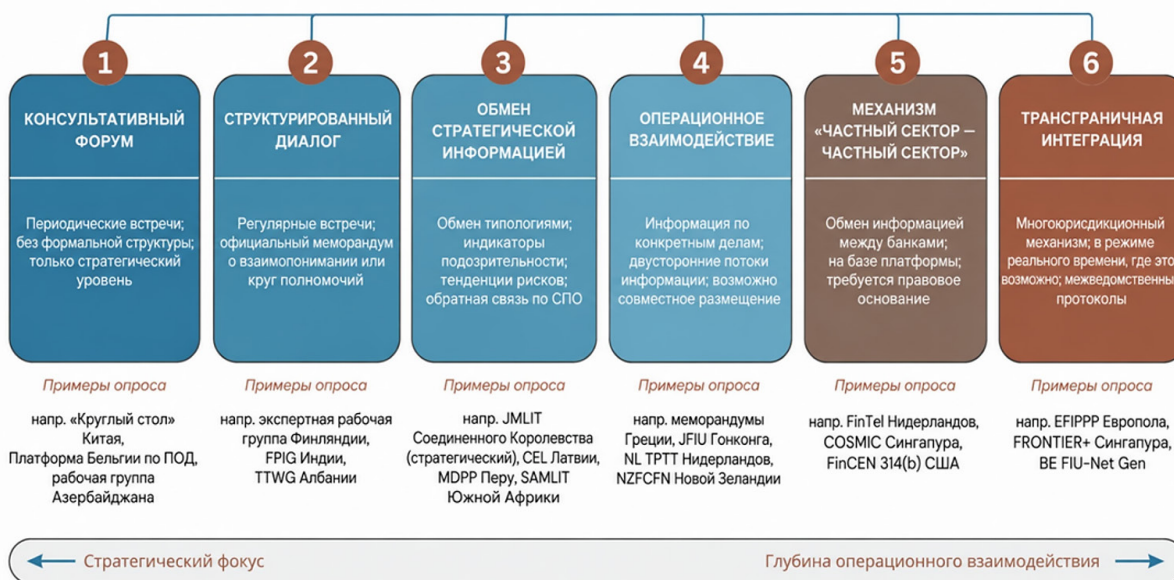
гические предупреждения JMLIT+ желтого и красного уровней регулярно передаются EFIPPP, коронным владениям и заморским территориям Соединенного Королевства, партнерам по «Пяти глазам» и международным ГЧП по запросу.

75. К трансграничным успехам, указанным респондентами, относятся улучшение коммуникации и обмена информацией, совместные расследования, включая международное отслеживание активов, стратегический диалог, наращивание потенциала и углубление понимания новых и возникающих рисков финансовой преступности посредством сотрудничества и передачи знаний. Взаимные визиты для проведения расследований и сбора доказательств также осуществляются в рамках трансграничного сотрудничества ГЧП и содействуют судебному взаимодействию. Более широкое глобальное понимание рисков финансовой преступности и мер по их снижению помогает оптимизировать ресурсы, объединяя возможности государственного и частного секторов разных ГЧП для более эффективных финансовых расследований и обеспечения соблюдения требований.

Развитие государственно-частных партнерств

76. ГЧП во всем мире развиваются собственными темпами, но в целом совершенствуются, оптимизируют деятельность и укрепляют коллективные возможности в сфере ПОД/ФТ. Новые ГЧП используют стратегический обмен как механизм укрепления доверия, тогда как зрелые партнерства расширяют границы возможного и изучают более инновационные способы передачи и использования конфиденциальных данных для поддержки конкретных дел. Некоторые направления такого развития показаны на рисунках ниже.

Рисунок 5. Возможные направления развития государственно-частных партнерств: от консультативных площадок к углубленной и трансграничной интеграции



Источник: ответы на опрос.

77. ГЧП в опрошенных юрисдикциях находятся на разных стадиях зрелости: для одних первоначальными шагами являются формирование доверия и отношений, другие уже перешли к поощрению и/или облегчению обмена информацией.

Рисунок 6. Шкала зрелости государственно-частных партнерств



78. Например, ГЧП на ранних этапах развития на Кипре, в Грузии, Нигерии и Зимбабве только начинают свой путь.
79. Характер и масштаб отдельных угроз, например, мошенничества, стимулируют создание инновационных ГЧП, таких как национальные центры по противодействию мошенничеству, которые часто опираются на правовые основания, обеспечивающие беспрепятственный обмен информацией между государственным и частным секторами. Более зрелые ГЧП, например, Сингапурский центр по противодействию мошенничеству, продолжают расширять стратегические партнерства по мере роста масштабов, скорости и сложности мошеннических угроз. Так, проект FRONTIER, созданный в 2020 году с участием 30 заинтересованных сторон, к концу 2025 года, как уже отмечалось в разделе о трансграничных ГЧП, расширился более чем до 180 участников из традиционных и нетрадиционных секторов ПОД, включая финансовые учреждения, финтех-компании, телекоммуникационные организации и онлайн-площадки. Это сократило сроки замораживания банковских счетов и позволило возвращать больше средств, переведенных мошенникам. В 2025 году сингапурский ASC вернул более 140 млн сингапурских долларов из заявленных потерь от мошенничества, превышавших 900 млн сингапурских долларов.
80. Британская модель JMLIT+ Data Fusion предусматривает масштабный обмен массивами данных, которые затем анализирует Совместная аналитическая группа (JAT). В нее входят специалисты государственного и частного секторов по данным, инженеры данных, сотрудники финансовой разведки и аналитики, которые выявляют цели, формируют оперативную информацию, распространяют информационные пакеты среди партнеров государственного и частного секторов, готовят аналитические материалы и разрабатывают инструменты автоматизации процессов и повышения эффективности использования данных.
81. Развитие также наблюдается в многоюрисдикционной сфере: ПФР Гибралтара, Гернси, острова Мэн и Джерси в рамках Форума четырех островных юрисдикций уже взаимодействуют между собой и с британским JMLIT+ по обмену стратегической информацией и приступают к пилотному обмену операционной информацией.
82. Для некоторых ГЧП развитие означает переход к сотрудничеству с небанковскими партнерами, например, в рамках британского JMLIT+ PPCF — Государственно-частного криптовалютного форума, где сектор виртуальных активов проактивно взаимодействует с правоохранительными органами, регуляторами Соединенного Королевства и участниками более широкой отрасли для противодействия преступному использованию виртуальных активов. См. раздел 5.3.5 об участниках.
83. Для других развитие выражается в расширении охвата или создании новых ГЧП для реагирования на приоритетные возникающие угрозы. Например, Департамент телекоммуникаций Индии запустил Цифровую разведывательную платформу (DIP) для противодействия рискам мошенничества (см. ниже).

Блок 15. Развитие государственно-частных партнерств для реагирования на приоритетные риски

Департамент телекоммуникаций Индии запустил Цифровую разведывательную платформу (DIP), доступную подотчётным субъектам, включая банки и другие финансовые учреждения. Платформа предоставляет доступ к двум индикаторам риска: перечню аннулированных мобильных номеров (MNRL) и индикатору риска мошенничества (FRI). MNRL представляет собой список мобильных номеров, аннулированных Департаментом телекоммуникаций по результатам расследования жалоб на мошеннические звонки с этих номеров. FRI присваивает мобильным номерам низкий, средний или высокий уровень риска с учетом их связи с операциями интернет-банкинга по счетам подставных лиц, указанным в сообщениях о кибермошенничестве, жалоб на спам с соответствующих номеров и других факторов.

Источник: Индия

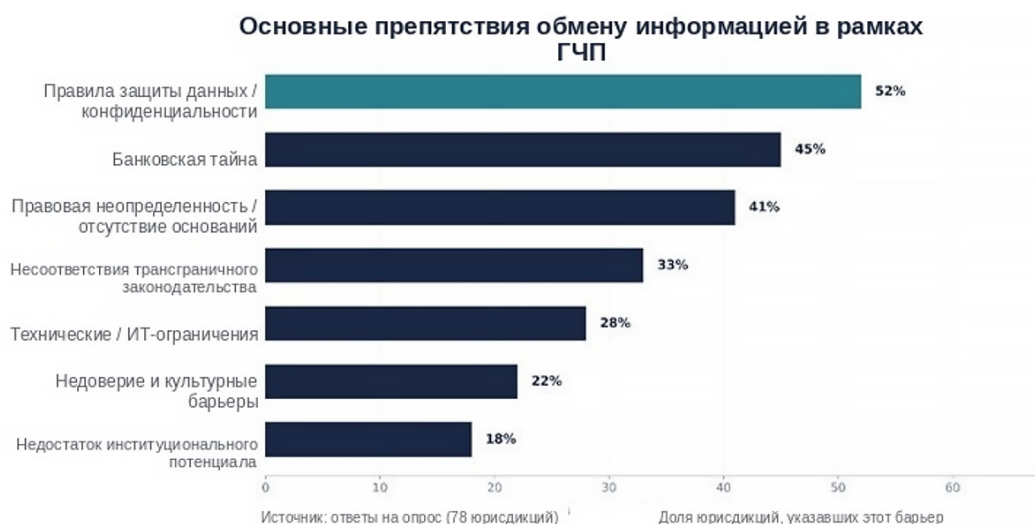
Среди многочисленных ГЧП Канада создала Интегрированное партнерство по обмену оперативной информацией об отмывании денег (IMLIP). Его цель — содействовать прочным рабочим отношениям между крупными финансовыми учреждениями и правоохранительными органами и обеспечивать допустимый законом обмен оперативной информацией о сложных и изощренных схемах отмывания денег.

Источник: Канада

Защищенный обмен информацией с соблюдением конфиденциальности

84. Возможности ГЧП по обмену данными иногда ограничиваются правилами защиты данных и конфиденциальности, законодательством о банковской тайне, техническими ограничениями и другими важными факторами, отраженными ниже.

Рисунок 7. Основные препятствия для обмена информацией



Источник: ответы на опрос

85. В целом ответы на опрос показали значительные различия в деятельности ГЧП и возникающих проблемах, связанных не только с данными, но и с другими ограничениями; некоторые из них особенно остры в странах с ограниченными возможностями.
86. В ответах регулярно упоминаются правовые и операционные ограничения, технологические недостатки, дефицит культуры и доверия, вопросы управления данными и их хранения, а также трансграничные препятствия; некоторые из них подробнее рассмотрены в следующем разделе.

Правовые и регуляторные вопросы

87. Многие юрисдикции сообщили, что законы о конфиденциальности, банковская тайна и установленные законом обязательства конфиденциальности иногда ограничивают передачу в рамках ГЧП информации на уровне клиентов или конкретных дел. Около 41% стран-респондентов указали, что правовые основания влияют на степень детализации передаваемых сведений, и отметили строгие требования защиты данных и банковской тайны, из-за которых до передачи любой информации о клиентах необходимо тщательно сопоставлять возможные последствия обмена. В некоторых случаях это приводит к тому, что, по крайней мере на начальном этапе, ГЧП сосредотачиваются на стратегической, а не на клиентской информации.
88. ГЧП, предусматривающие обработку персональных данных, должны соблюдать применимые требования защиты данных и конфиденциальности. Соответствующие механизмы должны обеспечивать соблюдение принципов необходимости, соразмерности, ограничения цели и прозрачности при обмене данными²².
89. Для этого инициативы в области ГЧП должны сопровождаться оценкой воздействия на защиту данных (DPIA), позволяющей определить и документально подтвердить необходимость и соразмерность обработки персональных данных преследуемой цели. Требования защиты данных могут предотвращать прекращение деловых отношений и финансовую изоляцию, обязывая операторов данных ГЧП учитывать риски для физических лиц, особенно при обработке операционных данных, специальных категорий данных и конфиденциальных сведений.

²² См. также: Глобальный договор ООН по координации контртеррористической деятельности, «Обеспечение соблюдения прав человека при принятии мер по противодействию финансированию терроризма», Глобальный контртеррористический договор ООН (ноябрь 2025 года), раздел C, доступно по адресу: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/hr_cft_guidance_november_2025.pdf

90. Полномочия и роль органов по защите данных значительно различаются между юрисдикциями и непосредственно влияют на проектирование и управление ГЧП; положительные изменения отмечены выше. В юрисдикциях с комплексными механизмами защиты данных, такими как GDPR, до создания любого механизма обмена персональными данными обычно требуется официальная консультация с органами по защите данных. В Европейском союзе это прямо предусмотрено статьей 75 Регламента о ПОД, которая требует от надзорных органов до начала деятельности партнерства по обмену информацией проверить в консультации с органами по защите данных наличие надлежащих механизмов соблюдения требований и завершение оценки воздействия на защиту данных. В таких системах любой обмен персональными данными должен оцениваться с точки зрения ограничения цели, соразмерности, минимизации данных и наличия правовой основы.
91. Другие юрисдикции, например, Сингапур, обеспечивают надежное управление конфиденциальностью на основе национального законодательства и структурированно взаимодействуют с органами по защите данных. Однако во многих юрисдикциях взаимодействие между органами ПОД/ФТ и органами по защите данных остается ограниченным, из-за чего механизмы ГЧП могут не иметь надлежащих гарантий защиты данных и конфиденциальности. В отдельных случаях это частично объяснялось тем, что соответствующие юрисдикции не сообщали о препятствиях для обмена информацией и имеют весьма открытое или благоприятствующее законодательство, например, более широкий доступ и полномочия, ограниченные целями ПОД/ФТ.
92. Одна из центральных тем документа — необходимость обеспечить совместимость обмена информацией в рамках ГЧП с механизмами защиты данных и конфиденциальности. Чтобы стороны не применяли чрезмерно осторожное или консервативное толкование законодательства о защите данных, необходимы четкие регуляторные ожидания и руководства. Заинтересованные стороны могут занимать осторожную позицию, особенно когда существуют основания высокого уровня, например, законный интерес, но они не подкреплены достаточно подробными разъяснениями органов по защите данных. Ответы на опрос показывают, что даже при наличии правовых оснований неверное толкование или отсутствие четких указаний препятствует своевременным действиям.
93. Поэтому некоторые юрисдикции приняли меры для уточнения правовых оснований и укрепления уверенности в обмене, в том числе используя предусмотренные законодательством исключения для передачи информации в определенных обстоятельствах. Сингапур создал COSMIC в соответствии с Законом о финансовых услугах и рынках, обеспечив четкую законодательную защиту информации, передаваемой через платформу. Гибралтар разработал формальные соглашения об обмене информацией, аналогичные меморандумам о взаимопонимании, и провел широкую коммуникацию с отраслью, что помогло организациям понять свое правовое положение и стимулировало участие. Эти примеры показывают, что правовые препятствия можно смягчить четкими законодательными актами для операционного обмена либо специальными механизмами для стратегической информации в сочетании с активным взаимодействием заинтересованных сторон и достаточно подробными руководствами.
94. Еще один значимый вывод касается ограниченного применения технологий повышения конфиденциальности (РЕТ). Хотя небольшое число юрисдикций экспериментирует с псевдонимизацией или гомоморфным шифрованием, большинство пока не использует РЕТ в операционных ГЧП. Указываются следующие причины: высокая стоимость, нехватка технических возможностей, ограниченное предложение поставщиков, регуляторная неопределенность и сомнения в способности РЕТ обеспечить требуемые скорость и точность. Следует также отметить, что РЕТ являются одним из инструментов более широкой системы защиты данных и конфиденциальности и не заменяют необходимость четкой правовой основы, ограничения цели и соблюдения иных применимых требований. Тем не менее для некоторых стран они оказались полезными, особенно в контексте обмена между субъектами частного сектора.

95. Технологии повышения конфиденциальности, федеративное обучение²³, безопасные многосторонние вычисления (SMPC)²⁴ и гомоморфное шифрование²⁵ все чаще используются для облегчения сотрудничества без ущерба конфиденциальности.
96. РЕТ способствуют защищенному и соответствующему требованиям конфиденциальности обмену между субъектами частного сектора²⁶ и деятельности ГЧП в целом, особенно при противодействии ОД и ФТ. Эти инструменты обеспечивают инновационные механизмы совместного анализа и формирования оперативной информации без раскрытия конфиденциальных данных или информации, позволяющей установить личность.
97. Некоторые страны сообщили, что применение РЕТ или шифрования в их ГЧП имеет важнейшее значение для защиты обмена конфиденциальной информацией, тогда как другие их не используют. Австралия, Канада, Нидерланды, Соединенное Королевство и Соединенные Штаты выделяются применением защищенных аналитических сред, зашифрованных каналов связи и механизмов псевдонимизации для защиты персональных данных при совместной работе органов власти и финансовых учреждений. Мексика сообщила о положительном опыте использования РЕТ (см. блок 16 ниже).

²³ Федеративное обучение использует общую модель искусственного интеллекта для обучения на децентрализованных наборах данных.

²⁴ Безопасные многосторонние вычисления распределяют вычислительную функцию между разными наборами данных, которые затем объединяются для получения конечного результата.

²⁵ Гомоморфное шифрование позволяет анализировать зашифрованные данные без их предварительной расшифровки.

²⁶ Консолидированные Стандарты ФАТФ по обмену информацией. См. инновационный и дискуссионный документ FFIS «Практические примеры использования анализа с сохранением конфиденциальности для борьбы с финансовой преступностью» (июнь 2020 года): <https://www.future-fis.com/the-pet-project.html>

Блок 16. Использование технологий повышения конфиденциальности (PEP) при обмене информацией между субъектами частного сектора

В Мексике обмен информацией между субъектами частного сектора облегчается с помощью технологии повышения конфиденциальности, действующей как децентрализованная межбанковская платформа обмена оперативной информацией. Она предназначена для того, чтобы финансовые учреждения могли в режиме реального времени и автоматически обмениваться сведениями об отмеченных клиентах и результатами проверки сотрудников с целью предупреждения ОД и финансовой преступности в более широком смысле. Архитектура платформы, основанная на принципе встроенной конфиденциальности, обеспечивает обмен без раскрытия исходных персональных данных и устраняет ограничения конфиденциальности, которые исторически препятствовали обмену информацией между конкурирующими организациями. Платформа работает на полностью децентрализованной инфраструктуре: все данные хранятся, обрабатываются и шифруются в пределах защищенного контура каждой организации. «Слепой» центральный узел координирует информационные потоки между участниками, но ни на одном этапе не получает доступа к данным, не обрабатывает и не хранит их.

Это обеспечивается архитектурой, при которой через центральный узел передаются только итоговые хеш-значения информации о клиентах или сотрудниках, позволяющей установить личность, вместе со значениями из согласованного организациями справочника, характеризующими природу подозрений. Имена, реквизиты счетов и исходные данные никогда не покидают организацию-источник. Организация может запросить, был ли потенциальный клиент отмечен другой организацией, либо получить предупреждение, если один из ее клиентов отмечен другим участником, при этом исходные данные обеих сторон остаются внутри их защищенных контуров. Платформа также поддерживает прямую связь между организациями по протоколу асимметричного шифрования, при котором ключ расшифровки имеется только у сторон конкретного обмена. В результате техническая архитектура структурно устраняет барьер доверия, препятствовавший эффективному межбанковскому сотрудничеству в сфере ПОД, и позволяет организациям, работающим на одних рынках, совместно предупреждать финансовую преступность без ущерба суверенитету данных или конфиденциальности клиентов.

Источник: Мексика

Конфиденциальность и целостность уголовных расследований

98. Оценки ИДКТК ООН показывают, что страны сталкиваются с трудностями при институционализации партнерств с частным сектором по обмену финансовой информацией, особенно в контексте ПФТ, где значительная часть информации государственного сектора имеет гриф секретности, а органы власти иногда ограничены законом в передаче таких сведений частным организациям.
99. Эффективным положительным примером является Оперативная группа Нидерландов по финансированию терроризма (NL-TFTF). В 2017 году Нидерланды запустили проект государственно-частного партнерства Центра финансовой экспертизы по финансированию терроризма (TF PPS FEC), более известный как Оперативная группа FEC по ФТ. В группу входят четыре государственных партнера — Полиция Нидерландов, Прокуратура (ОМ), ПФР Нидерландов и Служба фискальной разведки и расследований (FIOD) — и шесть частных партнеров: ABN Amro, ING, Rabobank, ASN Bank, KNAB и Triodos Bank. С 2019 года сотрудничество действует на постоянной основе. Партнеры группы обмениваются сигналами и связанными персональными данными лиц, имеющих отношение к терроризму. Такой обмен сигналами и направление сообщений о необычных операциях осуществляются при соблюдении строгих правовых условий. Предоставление информации о соответствующих лицах основано на положении Закона Нидерландов о полицейских данных.

Операционные и институциональные проблемы

100. ГЧП сталкиваются с широким кругом операционных проблем. Зрелые партнерства, например, в Австралии и Соединенном Королевстве, испытывают трудности, связанные с масштабом и сложностью. Опыт Австралии, британского JMLIT+ и аналогичных инициатив других юрисдикций показывает возможные проблемы управления масштабом с точки зрения участника: выбор надлежащих операционных партнеров из сотен лицензированных банков и провайдеров платежных услуг, поддержание активного участия и предотвращение непреднамеренных последствий, таких как отказ частных участников от обслуживания определенных категорий клиентов.
101. Относительно новые ГЧП по мере совершенствования процессов сталкиваются с иными операционными проблемами, например, нехваткой персонала, ограниченной технической экспертизой и фрагментированной межведомственной координацией. Гана и Эсватини отмечают, что некоторые запросы требуют подтверждения несколькими ведомствами, что увеличивает сроки обработки. Маршалловы Острова и ряд небольших юрисдикций сообщили, что они всё ещё находятся на ранних этапах развития ГЧП и поэтому сталкиваются прежде всего с базовыми проблемами управления и подключения участников, а не со сложными вопросами интеграции.
102. Во многих странах также наблюдается неодинаковая зрелость разных секторов. ОАЭ и Индонезия описали ситуации, когда банки и крупные финансовые учреждения хорошо подготовлены к представлению информации в рамках ГЧП, тогда как УНФПП, ПУВА и небольшие компании могут иметь недостаточные или более ограниченные возможности. Эта асимметрия отрицательно влияет на качество и последовательность загружаемой оперативной информации и создает пробелы в охвате выявления. Подход Китайского Тайбэя, предусматривающий стимулирование первой загрузки или представления высококачественных материалов, является примером операционной меры, направленной на изменение поведения, а не только на правовые или технические решения (см. блок 17 ниже).

Блок 17. Стимулы платформы обмена информацией ПОД/ФТ/ФРОМУ для повышения результативности

Для увеличения вклада организации и сотрудники, впервые загружающие материалы или представляющие высококачественный контент в ГЧП, получают официальное признание. Надзорному органу и подотчётному субъекту направляется письмо, которое может служить основанием для поощрения организации и ее сотрудников. В ответе также отмечается необходимость более широкой стратегии и стимулов как в государственном, так и в частном секторе.

Источник: Китайский Тайбэй

103. Некоторые юрисдикции укрепили рабочие процессы путем создания четких процедур и устойчивых моделей взаимодействия. Как отмечалось выше, британское JMLIT+ использует структурированные группы для эффективного управления информацией, а Гонконг, Китай применяет стандартные операционные процедуры, поддерживаемые периодическими брифингами для участвующих организаций.

Технологические и инфраструктурные ограничения

104. Технологические ограничения также могут препятствовать эффективной коммуникации и обмену информацией. Около 28% юрисдикций упомянули ограничения систем, требования безопасности или различия платформ как факторы, влияющие на скорость обмена. Австралия отмечает, что защищенные платформы позволяют передавать секретную информацию, однако

доступ также ограничен способностью участников соответствовать стандартам ИТ и безопасности. Швеция пояснила, что различия форматов данных и отсутствие общих ИТ-платформ ограничивают возможности агрегирования и анализа. Лаосская НДР назвала ограниченную ИТ-инфраструктуру одной из основных проблем создания эффективных платформ ГЧП, тогда как Мьянма и Нигерия совершенствуют платформы защищенного обмена. Когда ведомства и частные компании используют разные, иногда несовместимые форматы и системы, возникают проблемы совместимости, требующие ручных обходных решений и увеличивающие задержки.

105. Эти ограничения могут снижать объем обмена в режиме реального времени и качество аналитических результатов, а также повышать вероятность роста затрат на обслуживание платформ. В юрисдикциях с более развитыми технологическими возможностями, таких как Сингапур и Австралия, внимание смещается от базового доступа к более сложным вопросам: масштабируемости систем данных, управлению сложными и крупными массивами, обеспечению защищенной многосторонней аналитики и снижению рисков непреднамеренного раскрытия. В опросе также отмечается растущий спрос на аналитику больших данных и возникающая нагрузка на инфраструктуру и модели управления, не рассчитанные на такой масштаб. Вместе с тем британская модель JMLIT+ Data Fusion преодолела часть этих проблем, успешно обеспечивая обмен и анализ крупных массивов данных совместной аналитической группой с ресурсами государственного и частного секторов.
106. Применение технологий повышения конфиденциальности различается между ГЧП. В одних партнерствах они почти или совсем не используются, в других применяются выборочно или экспериментально. Однако даже при их использовании признается, что одни только РЕТ не способны устранить правовые проблемы или дефицит доверия: они должны действовать в четких механизмах управления и технически соответствовать возможностям участников.
107. Отдельно несколько стран инвестируют в защищенные технические платформы, поддерживающие ГЧП. Австралия применяет модель многоуровневого доступа, позволяющую широкое участие при сохранении надлежащих уровней безопасности. Южная Африка модернизировала системы для улучшения взаимодействия регуляторов и подотчетных субъектов, стимулируя более структурированные информационные потоки.

Проблемы культуры и доверия

108. Иногда препятствия для ГЧП обусловлены простым отсутствием доверия и приверженности. В странах, где участие остается добровольным и не стимулируется, взаимодействие часто носит эпизодический характер и различается по качеству. Банки и другие частные участники могут опасаться регуляторных или репутационных последствий передачи конфиденциальной информации, особенно при правовой неопределенности. Опасения, высказанные от имени Гибралтара до запуска FLINT, показывают, что доверие можно формировать посредством раннего взаимодействия, открытого управления и прозрачных соглашений об обмене информацией. При отсутствии таких мер частные участники воздерживаются от передачи сведений из-за риска раскрытия или ответственности.
109. Доверие также формируется за счет взаимности и обратной связи. В юрисдикциях, где обратная связь ограничена или предоставляется с задержкой, стимулы частного сектора к обмену ослабевают. Формальные структуры — четкое распределение ответственности, регулярные брифинги и ясность правового положения — институционализируют доверие в крупных и сложных сетях ГЧП, как в Соединенном Королевстве и Австралии. Нигерия также усилила меры обеспечения доверия посредством назначенных контактных лиц и более четкой коммуникации.
110. Углубленное сотрудничество выходит за рамки обмена информацией: оно предполагает формирование общего языка и подлинного партнерства государственного и частного секторов.

Обеспечение соблюдения основных прав (справедливое судебное разбирательство и презумпция невиновности, конфиденциальность) и предупреждение непреднамеренных последствий (например, прекращения деловых отношений и финансовой изоляции)

Надлежащая правовая процедура и основные права

111. ГЧП должны проектироваться и действовать с соблюдением фундаментальных принципов внутреннего законодательства и, когда это применимо, принципа надлежащей правовой процедуры, включая право на справедливое судебное разбирательство и презумпцию невиновности. Важны также надлежащие механизмы оценки надежности и точности данных, полученных в рамках ГЧП и используемых в судебных или административных производствах.
112. Следует отметить, что ГЧП не предназначены для обхода процессуальных гарантий, включая пороговые требования к доказательствам для получения судебного разрешения на принудительные меры. При оценке соблюдения этих принципов необходимо учитывать, в частности:
 - 1) вид ГЧП — стратегический, операционный или гибридный, — характер осуществляемой деятельности и участвующие органы, включая правоохранительные, прокурорские и/или судебные органы;
 - 2) охват и условия запросов данных, включая соответствующие пороговые критерии, вид передаваемой информации, основные права, в том числе при использовании полученной в рамках ГЧП информации в уголовном процессе, а также соблюдение применимых требований защиты данных, включая четкую правовую основу, ограничение цели и соразмерность обработки персональных данных.
113. Надежная регуляторная система должна обеспечивать строгое соблюдение принципов необходимости, соразмерности, ограничения цели и прозрачности при любом обмене данными в рамках ГЧП (см. раздел о правовых и регуляторных вопросах). Эти принципы служат этическим и правовым ориентиром для обеспечения баланса между операционной эффективностью и соблюдением прав человека.
114. В 2025 году Глобальный договор ООН по координации контртеррористической деятельности выпустил «Руководство по обеспечению соблюдения прав человека при принятии мер по противодействию финансированию терроризма», содержащее конкретные рекомендации, в частности по использованию соответствующей финансовой информации частного сектора, обмену информацией и созданию партнерств с частным сектором. Руководство подчеркивает принципы, применимые не только к ГЧП в сфере ФТ: партнерства должны проектироваться и реализовываться в полном соответствии с международным законодательством о правах человека, включая принципы законности, необходимости, соразмерности и недискриминации, а также сопровождаться надежными гарантиями защиты данных, ограничения цели, хранения, доступа и надзора. Оно также подчеркивает необходимость четкого управления, подотчетности и средств правовой защиты для предупреждения необоснованного дерискинга, финансовой изоляции или неблагоприятного воздействия на законную гуманитарную деятельность и деятельность гражданского общества²⁷.
115. При проектировании ГЧП следует учитывать, что в результате дерискинга и отказа в обслуживании подозреваемые лица и сети могут перейти на менее доступные платформы, что приведет к упущенным возможностям сбора информации о незаконной деятельности.

²⁷ https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/hr-cft_guidance_november_2025.pdf (раздел J).

116. Частный сектор, на который распространяются законы о защите данных, также обязан соблюдать права человека²⁸. При отсутствии надлежащих гарантий обмен информацией между государственным и частным секторами может приводить к предвзятости и профилированию по расовому, политическому или религиозному признаку, как прямо отмечается в аналитической записке ИДКТК ООН; соответствующие принципы применимы независимо от угрозы, для противодействия которой создано ГЧП.
117. ГЧП должны тщательно оценивать баланс между эффективным обменом информацией и гарантиями от возможного вреда и рассмотреть возможность прямо включать регуляторную ясность и конкретные рекомендации частному сектору по практике дерискинга.
118. ГЧП также должны создавать возможности для содержательного участия гражданского общества, чтобы партнерства не наносили ущерба финансовой доступности и гражданскому пространству, в том числе не оказывали сдерживающего воздействия на законную деятельность некоммерческих организаций и исключительно гуманитарную деятельность.
119. Наконец, ГЧП должны обеспечивать, чтобы разработанные в их рамках типологии и превентивные меры или передаваемая тактическая информация не оказывали несоразмерного воздействия на представителей какого-либо пола, в том числе посредством ограничения доступа к финансовым услугам.

Управление данными, хранение и удаление

120. С учетом взаимодополняющего характера целей защиты данных и конфиденциальности, а также ПОД/ФТ механизмы ГЧП должны обеспечивать, чтобы передаваемые данные регулировались четкими политиками и процедурами, предусмотренными применимым законодательством. Они могут включать ограничение цели, сроки хранения, контроль доступа и процедуры удаления в соответствии с национальным законодательством и соответствующими стандартами защиты данных и конфиденциальности. Несколько юрисдикций подтвердили, что данные ГЧП хранятся в течение установленных сроков и удаляются после прекращения цели, для которой были собраны.
121. Несколько юрисдикций подтвердили наличие требования об удалении персональных данных. В таких случаях обязанность удаления главным образом возникает при следующих обстоятельствах:
 - после прекращения цели, для которой данные собирались и обрабатывались;
 - по завершении расследования, если установлено, что лицо не совершало преступление;
 - после прекращения первоначальной цели хранения данных; и/или
 - при выходе участника ГЧП из меморандума о взаимопонимании.
122. Юрисдикции должны обеспечивать документальное закрепление обязанностей по удалению, когда они применимы, в механизмах управления ГЧП. Если национальное законодательство предоставляет физическим лицам права в отношении их персональных данных, партнерства должны четко устанавливать, как эти права — прежде всего право на удаление и право на доступ — взаимодействуют с требованиями хранения в сфере ПОД/ФТ и как ГЧП должно обрабатывать соответствующие запросы. Юрисдикции также указывали, что отсутствие специальных руководств по такому взаимодействию является известным источником затруднений.

²⁸ «Руководящие принципы предпринимательской деятельности в аспекте прав человека: осуществление рамок Организации Объединенных Наций в отношении защиты, соблюдения и средств правовой защиты», 2011 год, доступно по адресу: https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf

123. Разнообразие практик юрисдикций указывает на необходимость общей базовой основы: определенных сроков хранения, связанных с целями обработки, журналов аудита, ролевого контроля доступа и документированных процедур удаления, последовательно применяемых ко всем участникам ГЧП. Несколько юрисдикций демонстрируют возможные передовые практики в этой области. Австралия, Южная Африка и Соединенное Королевство применяют четкие графики хранения и процедуры удаления. Южная Африка и Соединенное Королевство ведут установленные журналы аудита и применяют контроль доступа, обеспечивая ясность для партнеров. Австралия публикует руководство по обращению с данными в соответствии с законодательством о конфиденциальности, что способствует прозрачности и предсказуемому управлению. Грузия и Молдова укрепляют свои механизмы, формируя более четкие ожидания для подотчётных субъектов. Вместе с тем в некоторых юрисдикциях по-прежнему отсутствуют определенные или последовательные практики, что вызывает вопросы о соблюдении требований конфиденциальности и возможности аудита. Юрисдикциям рекомендуется формализовать эти элементы в механизмах управления ГЧП и в максимально возможной степени привлекать национальные органы по защите данных и конфиденциальности к проектированию механизмов управления данными ГЧП.

Дерискинг и непреднамеренные последствия

124. Информация ГЧП может влиять на подход организаций к секторам повышенного риска, при этом потенциально вредным побочным результатом обмена информации является дерискинг. Партнерства типа JMLIT+ приводили примеры, когда после получения предупреждения или оперативной информации частные участники предпочитали прекратить отношения, а не совместно снижать риск. В отношении COSMIC Сингапур выразил обеспокоенность возможным переносом риска на банки, не участвующие в механизме; другие юрисдикции отмечали этапы, когда частные партнеры прекращали отношения с организациями, отмеченными механизмами ГЧП. Эти модели показывают, что, если материалы ГЧП не сопровождаются указаниями по соразмерному управлению рисками и разъяснением регуляторных ожиданий, частные организации могут выбирать прекращение отношений, что способно вытеснять незаконную деятельность в менее регулируемые каналы.
125. Сингапур предоставляет четкие рекомендации по соразмерному снижению рисков и создал рабочую группу по вопросам дерискинга для обсуждения соответствующих проблем и практик управления клиентами повышенного риска без необоснованного прекращения отношений. Соединенное Королевство взаимодействует с отраслью по применению сбалансированных подходов к проверке счетов, поддерживая единообразное толкование. Нигерия и Гамбия указали, что продолжают надзорный диалог, чтобы организации управляли риском сбалансированно. Южная Африка рекомендует банкам консультироваться с государственными следственными органами до принятия мер по вопросам, рассматриваемым в рамках ГЧП. Такая практика помогла поддерживать уровень доверия, критически важный для деятельности партнерства.

Вопросы, относящиеся к трансграничным государственно-частным партнерствам

Правовые и регуляторные вопросы

126. Трансграничные ГЧП сталкиваются с проблемами, аналогичными внутреннему обмену информацией, но иногда в более крупном масштабе и с большей сложностью. ЕС подчеркивает необходимость правовых оснований, соответствующих GDPR, особенно в контексте реализации статьи 75, в связи с которой ожидается рост числа ГЧП в европейских юрисдикциях. При трансграничном обмене особенно отмечаются операционные затруднения и сроки. Если ГЧП не встроены в формальные многосторонние площадки или меморандумы о взаимопонимании, запросы могут направляться через традиционные каналы ПФР, например, сеть «Эгмонт», что иногда добавляет формальные этапы и увеличивает сроки. Успешные трансграничные ГЧП

объединяют заранее определенные контактные лица, порядок эскалации и установленные сроки ответа; результаты опроса показывают, что при наличии таких механизмов, например, в EFIPPP или устойчивых связях JMLIT+, сроки обработки и операционные результаты заметно лучше.

127. В вопросах защиты, хранения и удаления данных и допустимости доказательств, влияющих на виды передаваемой информации, трансграничный обмен должен соответствовать режимам защиты данных как государства-источника, так и государства-получателя. Ответы показывают различия в сроках хранения данных ГЧП: в одних юрисдикциях действуют строгие сроки удаления и журналы аудита, в других политики менее определены. Эти различия осложняют обмен, поскольку принимающая юрисдикция может быть не в состоянии выполнить обязательства государства-источника по хранению и удалению, либо правоохранительные органы могут опасаться, что собранные доказательства не будут соответствовать требованиям допустимости или непрерывности цепочки хранения в другой юрисдикции. Отсутствие четкой правовой основы трансграничной передачи данных может стать серьезным препятствием и должно учитываться при создании трансграничных ГЧП. Соединенные Штаты и некоторые европейские респонденты подчеркнули, что правовые ограничения на обращение с доказательствами и их раскрытие существенно ограничивают объем передачи без судебных постановлений или взаимной правовой помощи. Практический вывод опроса состоит в том, что согласованные шаблоны хранения, ограничения цели, ролевого доступа и контролируемого уничтожения помогают преодолеть трансграничные правовые разрывы, если включены в меморандумы о взаимопонимании или соглашения об обмене информацией.
128. Использование технологий повышения конфиденциальности в трансграничных ГЧП все еще развивается. Юрисдикции называют четыре ограничения их трансграничного внедрения, требующие внимательного учета: 1) различия правовых позиций относительно того, могут ли обезличенные данные по-прежнему считаться персональными; 2) сомнения в технической зрелости и совместимости внедренных РЕТ; 3) аналитические ограничения; 4) стоимостные и ресурсные барьеры для небольших партнеров. В трансграничных пилотных проектах РЕТ поддерживают обмен информацией повышенного риска, позволяя совместно анализировать маскированные наборы данных, однако не устраняют необходимость правовых оснований и механизмов доверия.

Технические вопросы

129. Технические возможности влияют на эффективность обмена информацией между юрисдикциями. Австралия отмечает, что развитые внутренние системы не всегда легко применимы к трансграничному обмену ГЧП, поскольку партнеры могут использовать различные стандарты шифрования или классификации. Европейские юрисдикции используют общие платформы, включая SIENA, которые содействуют согласованию на трансграничном уровне.
130. Техническая несовместимость проявляется в двух формах: несоответствии платформ и стандартов данных и различиях классификации безопасности. AUSTRAC отмечает, что защищенные платформы позволяют осуществлять более содержательный обмен, однако партнеры различаются по способности выполнять требования сертификации или шифрования. Опыт австралийского Fintel Alliance показывает необходимость многоуровневого защищенного доступа: не всем партнерам требуется максимальный допуск, но различия требуют надежной логики управления доступом и стандартов маркировки данных. Швеция и Лаосская НДР сообщили об устаревших системах и ограниченных ИТ-возможностях, вынуждающих использовать ручные обходные процессы и повышающих риск ошибок при переносе данных. Отсутствие общих форматов сообщений, классификации типологий и согласованных правил метаданных затрудняет автоматизированную трансграничную аналитику. Ответы показывают, что юрисдикции с заранее согласованными схемами данных, общей классификацией и совместимыми платформами проводят более быстрый и качественный трансграничный анализ.

Доверие, взаимность и циклы обратной связи

131. Доверие и взаимность столь же необходимы в трансграничных ГЧП, как и во внутренних партнерствах. Страны, участвующие в сложившихся региональных механизмах, например, Гибралтар через JMLIT+ и EFIPPP, пользуются встроенными структурами доверия. Австралия и Сингапур поддерживают активную связь с зарубежными партнерами для обеспечения прозрачности и общего понимания.

Дерискинг и непреднамеренные последствия

132. Что касается возможного дерискинга и побочных эффектов, трансграничные ГЧП иногда приводят к непреднамеренному прекращению отношений. Соединенное Королевство сообщило о случаях, когда обмен оперативной информацией побуждал некоторые частные организации прекращать отношения с отмеченными клиентами вместо применения соразмерных мер снижения риска. Поэтому трансграничные предупреждения могут не пресекать, а перемещать незаконные потоки, если получающие организации используют защитную стратегию выхода. Результаты опроса указывают на необходимость трансграничных рекомендаций по соразмерному реагированию, надзорного контроля, препятствующего массовому закрытию счетов, и механизмов совместных планов снижения рисков между юрисдикциями. Без таких гарантий результаты ГЧП могут усиливать именно те уязвимости, которые призваны устранить.

Почему эти проблемы сохраняются и чем различаются юрисдикции?

133. Ответы многих юрисдикций показывают три структурные причины устойчивости проблем ГЧП. Во-первых, правовые системы сформировались до появления современных потребностей обмена данными, что создает несоответствия, если законодательство не обновляется. Во-вторых, технологии меняются быстро, и многие организации не успевают проводить требуемую модернизацию. В-третьих, доверие и поведенческие стимулы являются социальными проблемами, которые технические или правовые решения способны устранить лишь частично.
134. Преобладающие ограничения различаются по юрисдикциям. Государства с высоким потенциалом сталкиваются главным образом с проблемами масштаба, управления и предупреждения непреднамеренного вреда, такого как дерискинг. Государства со средним потенциалом сосредоточены на правовой определенности и создании защищенных платформ. Государства с низким потенциалом испытывают базовые трудности с персоналом, техническими ресурсами и последовательностью политики. Там, где правовая реформа возможна и сопровождается практическим управлением, например, в Соединенном Королевстве, Сингапуре и Гибралтаре, ГЧП способны обеспечивать операционные результаты. В юрисдикциях, где реформы оспариваются или непрозрачны, партнерства вынуждены действовать в ограниченном обезличенном стратегическом режиме.

Достижения и добавленная стоимость государственно-частных партнерств

135. Надлежащий обмен информацией позволяет всем соответствующим заинтересованным сторонам эффективнее использовать доступные ресурсы и инновационные методы противодействия финансовой преступности. ГЧП стимулируют частный сектор укреплять возможности снижения рисков деятельности высокого риска и тем самым эффективнее поддерживать органы власти в сфере ПОД/ФТ/ПРОМУ. Это особенно важно с учетом быстрого развития финансовых технологий и характера угроз, которые могут включать операции небольшой стоимости ниже порогов мониторинга или отчетности либо совершаться с применением способов сокрытия. ГЧП позволяют сочетать данные, аналитические инструменты и технологии с общими экспертными знаниями государственного и частного секторов по противодействию угрозам.
136. ГЧП могут позволять частным организациям, которые часто не вправе обмениваться необходимой информацией непосредственно друг с другом, предупреждать отрасль или сектор о способах использования продуктов и услуг лицами, отмывающими деньги и финансирующими терроризм. Они могут создавать возможности для проактивной передачи соответствующих сведений и раннего выявления угроз, а также обеспечивать обмен информации, требующий незамедлительных и срочных действий.
137. Особенно важно, что во многих юрисдикциях операционные ГЧП являются наиболее эффективным способом преодоления широко распространенной проблемы изолированности практически применимой информации и оперативных данных в отдельных организациях частного или государственного сектора, прежде всего, но не исключительно, в сфере ФТ. При обмене в режиме реального времени многосторонние ГЧП позволяют разрабатывать более эффективные и комплексные стратегии расследования, поскольку государственные органы могут совместно с частным сектором проактивнее отслеживать, картировать и выявлять террористические сети²⁹. Более тесное взаимодействие и координация разных секторов имеют ключевое значение, поскольку они часто участвуют в одних процессах и каждый располагает частью общей картины. Например, краудфандинговая платформа нередко имеет богатые данные о поведении, тогда как финансовое учреждение, обеспечивающее платежи, располагает платежной информацией. Критически важно понимать, как использовать эти возможности.
138. Эксперты частного сектора в области блокчейн-разведки, инновационных комплаенс-инструментов на основе ИИ, краудфандинговых платформ и торговли цифровыми активами могут предоставлять специализированные знания и передовые технологии, помогая органам выявлять и пресекать финансирование терроризма и защищать свои секторы от использования в целях ФТ. Например, компании блокчейн-аналитики предоставляют инструменты мониторинга операций, которые помогают добросовестным организациям цифровых активов защищаться от злоумышленников. Это важно, поскольку частный сектор объясняет принципы работы таких продуктов и услуг, а государственный сектор определяет способы их использования для ОД/ФТ.

Доказательства повышения эффективности выявления ОД/ФТ и возврата преступных активов

139. Юрисдикции, внедрившие государственно-частные партнерства, сообщают о значительных преимуществах для укрепления мер по предупреждению и выявлению в сфере ПОД/ФТ. При обмене стратегической информацией он способствует раннему выявлению возникающих угроз, индикаторов риска и типологий.

²⁹ https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/cted_analytical_brief_on_ppps_cft_2023.pdf. См. также материалы экспертных обсуждений при запуске документа: <https://www.un.org/securitycouncil/ctc/news/cted-holds-multi-stakeholder-discussion-establishing-effective-public-private-partnerships>

140. ПФР с более зрелыми ГЧП обмениваются индикаторами, связанными с СПО, данными НПК/ЗСК и финансовыми метаданными, укрепляя возможности выявления во всем финансовом секторе и среди УНФПП. Кроме того, партнерства обеспечивают структурированные механизмы обратной связи, совершенствующие механизмы соблюдения требований ПОД/ФТ у подотчётных субъектов. Основные преимущества операционной информации проявляются в пресечении преступных сетей, ускорении расследований и предоставлении более практически применимых сведений. См., например, блок 2 о раннем выявлении ФТ в Индонезии.
141. Несмотря на преимущества, о которых сообщают некоторые ГЧП, разработка показателей результативности и оценка достижения стратегических целей остаются сложной задачей. Критически важны количественный и качественный мониторинг и оценка вклада ГЧП, поскольку они укрепляют доверие заинтересованных сторон, поддерживают подотчетность и обеспечивают долгосрочную устойчивость. Пример Австрии ниже показывает улучшение результатов возврата активов благодаря специальной рабочей группе в рамках ГЧП.

Блок 18. Улучшение результатов возврата активов благодаря специальной подгруппе Австрийской сети финансовой разведки (FINA)

Подставные компании представляют один из наиболее значимых рисков отмывания денег в Австрии. FINA рассмотрела этот вопрос в приоритетном порядке, создав в начале 2026 года специальную подгруппу. Сотрудничество органов власти и подотчетных субъектов обеспечило операционный успех:

- До создания подгруппы в 2025 году финансовая полиция вынесла 117 постановлений о замораживании и постановления о конфискации на сумму 186 млн евро.
- Однако всего за шесть месяцев результаты почти удвоились: к июню 2026 года было вынесено уже 181 постановление о замораживании и постановления о конфискации на сумму 18,2 млн евро.

Источник: Австрия

Повышение качества СПО

142. Совместный характер ГЧП обеспечивает систематический обмен типологиями, индикаторами и стратегическим анализом, повышая точность и обоснованность СПО посредством их согласования с возникающими рисками и национальными или международными приоритетами. Структурированное сотрудничество через защищенный электронный обмен и специализированные площадки сокращает информационную асимметрию между компетентными органами и подотчётными субъектами и ускоряет направление своевременных СПО с более высокой операционной ценностью.
143. Регуляторная обратная связь и публикация агрегированного анализа рисков способствуют последовательности и стандартизации, сокращают дублирование и улучшают прослеживаемость. Доступ к данным НПК/ЗСК, отраслевым тенденциям рисков и риск-ориентированным рекомендациям позволяет превратить СПО из общих предупреждений в содержательные отчеты с аналитикой, поддерживающей определение приоритетов и сегментацию расследований. В совокупности эти практики, основанные на Стандартах ФАТФ и принципах Группы «Эгмонт» о защищенном обмене информацией, не только повышают полезность СПО для финансовой разведки, но и укрепляют способность системы выявлять сложные модели и снижать системные риски.

144. Данные о влиянии ГЧП на качество СПО ограничены из-за отсутствия формальных механизмов и показателей оценки. Вместе с тем установлено, что ГЧП как дискуссионная площадка, обмен типологиями, тенденциями рисков, риск-индикаторами («красными флагами») и показателями, а также доступ к стратегической информации и другим элементам — данным НПК/ЗСК, финансовым метаданным и индикаторам СПО — способствуют представлению подотчётными субъектами более полных, значимых и соответствующих рискам СПО.
145. Италия, Малайзия, Сингапур, Соединенное Королевство и Соединенные Штаты отметили некоторые положительные изменения: риск-ориентированные рекомендации, регуляторная обратная связь и конкретные данные помогают улучшать структуру, обоснование и направленность СПО, переводя их от базовых сообщений к более точным материалам, соответствующим реальным моделям. См. также блок 7 о гибком и оперативном подходе Латвии, который обеспечил целевые СПО и более эффективные результаты.

Пресечение преступных сетей

146. ГЧП пресекают преступные сети посредством улучшения обмена оперативной информацией и данными, обеспечивая проактивное выявление, более быстрые расследования и лучшие результаты, а также оптимизацию ресурсов и экспертизы. Респонденты подчеркнули, что сотрудничество государственного и частного секторов формирует общую информацию, которая может использоваться при расследовании тяжких преступлений и создавать основу для действий против сетей и схем ОД/ФТ. Взаимодействие ГЧП также углубляет совместное понимание моделей и помогает органам выявлять подозрительные группы операций в разных организациях, создавая более надежную основу для расследований, ориентированных на сети, и повышая способность понимать модели и принимать меры.
147. Важно отметить, что сочетание операционных данных и индикаторов риска считается полезным для создания более надежной и крепкой основы расследований и последующих действий в отношении групп подозрительной деятельности. Установленный законом режим сообщений о подозрительной деятельности и условия обращения с информацией ГЧП поддерживают использование правоохрнительными органами оперативной информации, основанной на таких сообщениях.
148. Очевидно, что ГЧП все чаще рассматриваются как эффективный механизм более раннего снижения рисков преступной деятельности, обеспечивающий переход от реактивной модели формального соблюдения требований к проактивной совместной модели, поскольку позволяют объединять ресурсы, технологии и специализированные знания, которые могут отсутствовать у отдельного государственного органа. См. примеры пресечения в блоках 19 и 20 ниже. Также применим блок 12 об обмене между субъектами частного сектора, поддерживаемом более широким законодательством о государственно-частном партнерстве.

Блок 19. Практический пример Fintel Alliance: развитие сотрудничества для пресечения отмывания денег с использованием наличных в Австралии

Этот пример Fintel Alliance охватывает ряд принципов ГЧП, рассматриваемых в отчете, и показывает, как устойчивое партнерство, доверенный обмен информацией и сотрудничество с сохранением конфиденциальности обеспечивают переход от реактивного выявления к проактивному системному пресечению отмывания денег с использованием наличных.

Стратегическое выявление рисков под руководством ПФР с учетом НОР и первых обсуждений государственного и частного секторов в рамках ГЧП определило типологии отмывания денег с использованием наличных как каналы высокого риска, которые ни одно ФУ не могло видеть полностью. В ответ партнерство запустило целевые операционные проекты, объединив отраслевую экспертизу и финансовые данные для углубления понимания и проверки возникающих типологий.

Первая совместная работа непосредственно поддержала правоохранные операции, что привело к обвинительным приговорам за преступления, связанные с доходами от преступной деятельности, и конфискации миллионов долларов незаконных наличных средств и активов, а также огнестрельного оружия, наркотиков и зашифрованных устройств. Деятельность также обеспечила более четкое понимание типологий отмывания наличных, включая групповые внесения, метод отмывания денег, при котором преступники используют банковские счета ничего не подозревающих клиентов сервисов денежных переводов («кукушкин смурфинг») и использование счетов третьих лиц; признание деятельности ОД ниже порогов отчетности; выявление уязвимостей существующих мер контроля финансовой системы, которые впоследствии были усилены одновременно с прекращением предоставления услуг по внесению наличных высокого риска.

Извлеченные уроки были преобразованы в общедоступное руководство по финансовой преступности и улучшили выявление и отчетность во всем финансовом секторе. Кроме того, эта деятельность стала катализатором создания Центра совместной аналитики (САН) ГЧП как подтверждения концепции. Последующая интенсификация его текущей деятельности объединила аналитиков ПФР, правоохранных органов и прикомандированных специалистов отрасли для сбора и анализа десятков миллионов точек данных. Это привело к выявлению около 4 млн австралийских долларов в рамках предполагаемой деятельности «кукушкиного смурфинга», новых лиц, представляющих интерес, следственных зацепок, а также к усиленным внутренним проверкам и отчетностям банков.

Источник: Австралия

Блок 20. Пример ликвидации финансовой пирамиды с использованием государственно-частного партнерства (Южная Африка)

Южноафриканское ГЧП располагает операционной платформой — тактической операционной группой (TOG), которая может рассматривать конкретные преступные угрозы и определенных субъектов, представляющих интерес.

В одном случае банк выявил подозрительную операционную деятельность по банковским счетам ряда клиентов. Анализ указал на предполагаемую финансовую пирамиду. Предполагалось, что организаторы пирамиды «работа из дома» имитировали известный интернет-магазин и предлагали гражданам перечислять средства для получения комиссионных от продаж.

Для ускоренного анализа подозрительных операций была сформирована TOG. Установлено, что в трех банках имелись действующие счета, связанные с участниками этой финансовой схемы. Государственные органы по вопросам конфискации активов и финансовый регулятор, отвечающий за защиту потребителей и расследование незаконных финансовых пирамид, были приглашены к сотрудничеству и присоединились к TOG вместе с банками. Через TOG банки ускоренно проанализировали счета и направили регуляторные сообщения. Это помогло государственным органам получить доказательственную информацию о деятельности пирамиды. Были проанализированы многочисленные счета восьми наиболее активных участников. Финансовый анализ выявил множество зачислений от граждан. Владельцы счетов переводили средства между собственными счетами и счетами друг друга. Назначения и модели операций указывали на внесение наличных и зачисления с определенными уникальными обозначениями. По итогам работы TOG Центр финансовой разведки распорядился остановить операции по выявленным счетам, а Подразделение по конфискации активов получило судебное постановление о замораживании средств на шестидесяти (60) банковских счетах на сумму около 458 000 долларов США. Благодаря ГЧП банки и государственные органы углубленно взаимодействовали для выявления и пресечения серьезного финансового преступления.

Источник: Южная Африка

Блок 21. Сотрудничество в рамках государственно-частного партнерства, которое привело к выявлению многомиллионной схемы торгового финансирования

Положение Сингапура как международного торгового центра делает его уязвимым для угрозы отмыкания денег через торговые операции. В 2018 году в рамках ACIP был опубликован отраслевой документ о передовых практиках, освещающий распространенные риск-индикаторы («красные флаги») и типологии ОД через торговые операции, а также передовые практики выявления и снижения соответствующих рисков. ACIP постоянно контролирует риски и типологии ОД через торговлю, а банки регулярно обмениваются наблюдениями и принятыми мерами снижения рисков.

Эти усилия обеспечили ощутимые и значительные результаты. В 2019 году один из банков ACIP сообщил CAD о занижении счетов-фактур компанией А, фиктивных поставках и предполагаемом использовании подставных компаний. CAD взаимодействовал с банками для обмена информацией и оперативными данными через механизм ACIP по обмену информацией о делах; банки направили СПО в отношении компании А. Управление по сообщениям о подозрительных операциях, являющееся ПФР Сингапура, затем проанализировало СПО и передало соответствующую информацию CAD, позволив принять быстрые и эффективные правоприменительные меры. На основе финансовой информации и многочисленных сообщений банков и финансовых компаний, предоставивших компании А кредитные линии для торгового финансирования, CAD в январе 2020 года начало расследование в отношении бывшего финансового директора компании А. В январе 2023 года она была признана виновной по 11 эпизодам мошенничества в соответствии со статьей 420 Уголовного кодекса 1871 года и одному эпизоду фальсификации отчетности в соответствии со статьей 477А Кодекса. За обман 16 финансовых учреждений на сумму более 469 млн долларов США ей было назначено 20 лет лишения свободы.

Источник: Сингапур

Повышение возможностей финансовых учреждений и УНФПП по соблюдению требований

149. ГЧП могут значительно укреплять возможности ФУ и УНФПП по соблюдению требований ПОД/ФТ/ФРОМУ, облегчая обмен финансовой информацией для предупреждения и выявления незаконной финансовой деятельности. Такие партнерства позволяют государственному сектору, включая ПФР и правоохранительные органы, и частному сектору — ФУ и УНФПП — теснее обмениваться информацией о новых угрозах, преступных методах и уязвимостях, в том числе через рассмотренные центры по противодействию мошенничеству. Центры реагирования показывают, как ФУ могут обмениваться информацией о типологиях мошенничества и подозрительной деятельности, совершенствуя выявление и реагирование по всем платежным потокам.
150. Некоторые страны отмечают, что участие в ГЧП помогает организациям совершенствовать внутренние политики и практики мониторинга, обновлять их с учетом информации о рисках и укреплять общее соблюдение требований ПОД/ФТ. Они также подчеркивают, что наличие правовой основы, оценок воздействия на конфиденциальность и структурированных каналов взаимодействия с частным сектором повышает осведомленность и укрепляет внутренний контроль, управление и управление рисками.
151. Обмен стратегической информацией и индикаторами риска по всей финансовой системе считается ключевым для совершенствования риск-ориентированных подходов, установления надлежащих мер снижения, более точной настройки сценариев мониторинга и согласования программ ПОД организаций с национальными приоритетами угроз. Платформы ГЧП используются для предоставления рекомендаций по рискам и обратной связи, что укрепляет институциональную оценку рисков, тематический мониторинг, управление и общую культуру соблю-

дения ПОД/ФТ среди банков, ПУВА и УНФПП, а также позволяет включать общую оперативную информацию в оценки рисков, внутренний контроль, модели мониторинга и управление соблюдением требований, укрепляя потенциал ПОД/ФТ банков, страховщиков, компаний, предоставляющих денежные услуги и других подотчётных субъектов.

152. При этом показатели для оценки улучшения возможностей ФУ и УНФПП по соблюдению требований не упоминаются; их можно рекомендовать как меру воздействия ГЧП.

Обмен оперативной информацией и укрепление доверия

153. Доверие является наиболее часто упоминаемым фактором успеха в глобальном массиве данных. Эффективные ГЧП формируют его посредством структурированного взаимодействия, сбалансированных информационных потоков и конструктивной обратной связи.

- Стратегия «сначала стратегическая информация». Почти все юрисдикции обмениваются стратегической информацией — типологиями (76,9%), риск-индикаторами («красными флагами») (75,6%) и тенденциями рисков (76,9%), — что делает ее естественной основой сотрудничества с меньшим числом правовых ограничений.
- Контролируемые операционные потоки. Обмен операционной информацией — данными по делам, сведениями НПК/ЗСК и индикаторами СПО — осуществляется в 55–65% юрисдикций, но при наличии четкой правовой основы и надежных гарантий защиты данных и конфиденциальности. Защищенные системы и определенные мандаты значительно повышают готовность частного сектора к обмену.
- Надежные циклы обратной связи. Около 64% юрисдикций предоставляют обратную связь по СПО/СПД, повышая качество отчетности, сокращая защитное направление сообщений и укрепляя общее понимание рисков.
- Инкубаторы доверия. Регулярные стратегические, операционные или разовые встречи создают пространство для открытого диалога о возникающих угрозах и пробелах в оперативной информации, уменьшая неопределенность и обосновывая будущие правовые или технические реформы.

154. Эффективные ГЧП сочетают структурированные процессы с формированием отношений, создавая экосистему, в которой оперативная информация передается свободнее и увереннее.

Операционные структуры, технологии и ресурсы

155. Операционно зрелые ГЧП опираются на защищенные технологии, специализированные группы и многоотраслевое участие для поддержки стратегических и операционных направлений работы.

- **Защищенные технологические платформы.** Ведущие юрисдикции используют специализированные зашифрованные платформы, такие как COSMIC в Сингапуре, защищенный обмен на основе goAML и платформа Fintel Alliance в Австралии. Эти системы обеспечивают обмен в режиме реального времени с высокой контролируемостью и надежным управлением доступом.
- **Многоотраслевое участие.** Хотя банки остаются основой большинства ГЧП, развитые модели включают УНФПП, ПУВА, провайдеров профессиональных услуг, операторов связи и цифровые платформы — секторы, часто становящиеся целями преступлений с использованием цифровых технологий.

- **Специализированные ресурсы и совместное размещение.** Такие юрисдикции, как Сингапур, Соединенное Королевство и Австралия, используют совместное размещение, при котором аналитики частного сектора работают вместе с сотрудниками ПФР и правоохранительных органов. Это углубляет доверие и ускоряет тактические решения благодаря повышению точности обмена при одновременном соблюдении всеми участниками требований конфиденциальности и защиты данных.
- **Гибкие форматы обмена.** Передовые ГЧП сочетают ежеквартальные стратегические совещания, ежемесячные операционные рабочие группы и предупреждения в режиме реального времени или по мере необходимости при возникновении угроз.

156. Такие операционные механизмы позволяют ГЧП масштабироваться, быстро реагировать на угрозы и поддерживать непрерывность аналитической работы.

Государственно-частные партнерства как связующее звено между стратегическим и операционным сотрудничеством

157. Многие ГЧП являются стратегическими, а не операционными. Стратегическая информация — типологии, тенденции и риск-индикаторы («красные флаги») — широко доступна для обмена, тогда как операционная часто сталкивается с правовыми, культурными ограничениями и требованиями защиты данных.

158. Модель «сначала стратегическая информация, операционная — по возможности» распространена во всем мире и отражает:

- правила конфиденциальности и банковской тайны;
- ограничения мандата;
- институциональную склонность к избеганию рисков;
- отсутствие прямо предусмотренных законом оснований обмена информацией.

159. Таким образом, ГЧП выполняют функцию связующих механизмов, создавая безопасную среду для диалога, укрепления доверия и обмена ранними предупреждениями, которая по мере развития гарантий может перерасти в полноценные структуры с операционной точки зрения.

Выводы

160. Среди широкого разнообразия механизмов обмена информацией ГЧП выделяются как постоянные эффективные инструменты противодействия ОД/ФТ/ФРОМУ при наличии надежной правовой основы, четкого управления и технологических инноваций. ГЧП внедрены во всех регионах мира.
161. В рамках Глобальной сети ФАТФ ГЧП устраняют критические пробелы в оперативной информации, повышают скорость и качество финансовых расследований и формируют культуру общей ответственности государств и частного сектора. Особенно важно, что они позволяют взаимодействовать с секторами, которые могут не относиться к подотчётным субъектам и поэтому не охватываются другими механизмами обмена, например, социальными сетями и платформами обмена сообщениями.
162. ГЧП необходимо создавать не только с учётом требований органов по защите данных и соответствующих правил и принципов, но и в сотрудничестве с этими органами. Для достижения целей ПОД/ФТ крайне важно, чтобы требования защиты данных необоснованно не препятствовали законным усилиям по борьбе с финансовыми преступлениями, которые соответствуют действующим нормативным актам. Странам необходимо устанавливать общие цели и четкие правовые и регуляторные ожидания и исключения, в том числе посредством взаимодействия высокого уровня и совместных руководств органов ПОД/ФТ и защиты данных и конфиденциальности. ФАТФ может изучить возможности поддержки более тесного взаимодействия между этими органами.
163. Некоторые юрисдикции по-прежнему сталкиваются с ограниченным доверием между заинтересованными сторонами, строгими режимами защиты данных и недостаточными техническими возможностями для поддержания защищенных и эффективных каналов обмена.
164. Эти проблемы подчеркивают необходимость гармонизированного подхода, поддерживающего ГЧП и сочетающего правовую ясность, институциональную координацию и передовые технологии для достижения операционной эффективности и соблюдения международных стандартов. ФАТФ может сыграть соответствующую роль в этой сфере.
165. Экспоненциальный рост мошенничества в мире также выявляет фрагментированность внутренних органов и необходимость более тесного сотрудничества с ФУ/ПУВА и нетрадиционными заинтересованными сторонами. Противостоять угрозе можно только обеспечив доступ всех соответствующих участников к надлежащей информации, а ГЧП являются скоростным каналом ее обмена.
166. Юрисдикции следует поощрять к внедрению или укреплению механизмов ГЧП, полностью соответствующих Рекомендациям ФАТФ и принципам защиты данных. Следует продвигать пилотные проекты с применением РЕТ, чтобы показать, как инновации позволяют сочетать эффективность, конфиденциальность и соблюдение законодательства.
167. На первом этапе ГЧП могут создаваться в форме пилотных инициатив или неформальных механизмов, например, обмена типологиями и дискуссионных групп, чтобы сформировать основу доверия между государственным и частным секторами, определить общие приоритеты и оценить правовые, регуляторные и институциональные препятствия сотрудничеству. По мере зрелости партнерства соответствующим заинтересованным сторонам следует использовать итерационный процесс для постепенного расширения состава участников, операционного охвата и ресурсной базы одновременно с разработкой стандартизированного защищенного механизма сотрудничества. Этот процесс должен поддерживать все более сложные формы обмена информацией, включая передачу закрытых/операционных данных, в соответствии с применимыми правовыми, регуляторными требованиями и требованиями защиты данных.



Июль, 2026

www.fatf-gafi.org