FATF

КРИТИЧЕСКАЯ ОЦЕНКА ОБЪЕДИНЕНИЯ ДАННЫХ, СОВМЕСТНОГО АНАЛИЗА И ЗАЩИТЫ ДАННЫХ

ИЮЛЬ 2021

Группа разработки финансовых мер борьбы с отмыванием денег (ФАТФ) — независимая межправительственная организация, разрабатывающая и популяризирующая принципы для защиты всемирной финансовой системы от угроз отмывания денег, финансирования терроризма и финансирования распространения оружия массового уничтожения. Рекомендации ФАТФ являются общепризнанными международными стандартами по противодействию отмыванию денег (ПОД) и финансированию терроризма (ФТ).

Дополнительную информацию о ФАТФ можно найти на сайте http://www.fatf-gafi.org

Данный документ и/или любые прилагаемые схемы не ограничивают статус или суверенитет никаких территорий, не противоречат определению межгосударственных границ и наименований любых территорий, городов или областей.

Неофициальный перевод подготовлен АНО МУМЦФМ

Ссылка для цитирования:

ФАТФ (2021 г.) Критическая оценка объединения данных, совместного анализа и защиты данных, ФАТФ, Париж, Франция,
https://www.fatf-gafi.org/publications/digitaltransformation/documents/data-pooling-collaborative-analytics-data-protection.html

© 2021 ФАТФ/ОЭСР. Все права защищены.
Копирование или перевод данного документа осуществляются только по предварительному письменному разрешению ФАТФ. Заявки на получение такого разрешения для всего документа или его отдельных частей направляются в Секретариат ФАТФ: ул. Андре Паскаля 2, 75775 Париж Седекс 16, Франция (факс: +33 1 44 30 61 37 или e-mail: contact@fatf-gafi.org).

Фотография на обложке: © Gettyimages

Благодарность

ФАТФ хотела бы поблагодарить сотрудников государственных органов и представителей частного сектора, в т.ч. разработчиков технологий, представителей финансовых учреждений и сотрудников органов власти, отвечающих за защиту данных, за предоставление ценной информации, примеров конкретных случаев и обратной связи касательно данного отчета.

Работа над этим отчетом велась под руководством Секретариата ФАТФ (Кристен Альма), важная информация была предоставлена Группой экспертов из следующих делегаций ФАТФ: Канады, Европейской комиссии, Франции, Германии, Израиля, Италии, Японии, Секретариата МАНИВЭЛ, Российской Федерации, Сингапура, Швейцарии, Великобритании, ООН и США.

Содержание

Сокращения **3**

Исполнительное резюме **4**

1. Введение **6**

2. Методология **9**

3. Основная информация **10**

4. Цели и предварительные условия для передачи и анализа информации в сфере ПОД/ФТ в частном секторе **12**

4.1. Зачем передавать данные? 12
4.2. Каковы заявленные цели инициатив по обобщению данных, передаваемых между частными лицами? 14
4.3. Какой тип данных может передаваться? 16
4.4. Инициаторы и предварительные условия использования новых технологий 18

5. Новые технологии обмена и анализа информации в сфере ПОД/ФТ **24**

5.1. Технологии обмена информацией между представителями частного сектора 24

6. Проблемы, связанные с использованием новых технологий при совместном анализе данных **29**

6.1. Обеспечение и повышение эффективности защиты и неприкосновенности данных 30
6.2. Качество данных 36
6.3. Недостаточная четкость законодательного регулирования 36
6.4. Объяснимость и интерпретация 37
6.5. Конфиденциальность СПО и предотвращение утечки данных 38
6.6. Структура рынка и конкуренция 39
6.7. Технологические затраты и ограничения 40
6.8. Упредительные сообщения и снижение рисков 40
6.9. Безопасность 41
6.10. Устранение субъективности в аналитике при использовании искусственного интеллекта 42
6.11. Права человека 42

7. Возможности более широкого применения технологии объединения данных и углубленных методов анализа **43**

7.1. К вопросу о ясности позиции регуляторных органов 43
7.2. Способствование созданию благоприятных условий 44
7.3. Стандартизация данных и управление данными 44
7.4. Принцип непредвзятости при использовании искусственного интеллекта 45

8. Заключительные положения **46**

Приложение A. Глоссарий **47**

Приложение B. Дополнительные примеры в сфере Regtech по новым технологиям анализа и обмена данными (по тематике ПОД/ФТ) между представителями частного сектора экономики данных и углубленных методов анализа **53**

Приложение C. Рекомендации, направленные на поддержку применения технологий **56**

Ссылки и источники информации **59**

© FATF/OECD 2021

Сокращения

ИИ	Искусственный интеллект
ПОД/ФТ	Противодействие отмыванию денег/финансированию терроризма
API	Интерфейс прикладного программирования
НПК	Надлежащая проверка клиента
ГО	Глубокое обучение
ТРР	Технология распределенного реестра
УНФПП	Установленные нефинансовые предприятия и профессии
ЗДК	Защита данных и конфиденциальность
СЗДЕ	Совет по защите данных Европы
ФАТФ	Группа разработки финансовых мер борьбы с отмыванием денег
ФУ	Финансовое учреждение
ОПЗД	Общие правила защиты данных
ОВО	Отчет о взаимной оценке
ОД/ФТ	Отмывание денег/финансирование терроризма
УПДЦ	Услуги перевода денег или ценностей
NLP	Обработка естественного языка
НОР	Национальная оценка риска
ПДЛ	Публичное должностное лицо
КФЧС	Консультативные форумы с частным сектором
ОУС	Орган по установлению стандартов
СПО	Сообщение о подозрительной операции

© FATF/OECD 2021

Исполнительное резюме

1. Успехи, достигнутые недавно в области технологий, помогают финансовым учреждениям более эффективно анализировать большие объемы структурированных и неструктурированных данных, а также более эффективно распознавать шаблоны и тенденции. Объединение данных и их совместный анализ помогает финансовым учреждениям лучше понимать, оценивать и снижать риски ОД/ФТ. Это приводит к более динамичному, действенному и эффективному выявлению деятельности подобного рода и помогает учреждениям частного сектора соблюдать требования в области ПОД/ФТ более оперативно и менее обременительным образом. Кроме того, это не дает возможности злоумышленникам использовать в своих интересах информационные пробелы, поскольку они взаимодействуют с многочисленными национальными и международными финансовыми учреждениями с целью отмывания своих незаконных доходов, каждое из которых имеет ограниченную и частичную информацию об операциях.

2. Однако объединение данных и совместный анализ также способны отрицательно влиять на защиту прав граждан и фундаментальных прав на неприкосновенность частной жизни. Таким образом, необходимо, чтобы при обмене информацией соблюдалось национальное и международное законодательство в области защиты данных и неприкосновенности частной жизни.

3. В данном отчете отмечается, что ПОД/ФТ, а также неприкосновенность и защита данных представляют собой элементы существенного общественного интереса и служат достижению важных целей. Эти цели не противоречат друг другу и по своей сути не являются взаимоисключающими. Целью принципов и правил защиты данных, предусмотренных в национальных и международных юридических актах, является защита прав человека и фундаментальных свобод, особенно прав на защиту частной жизни. В этом отчете отмечается важность того, чтобы системы правового регулирования способствовали достижению обеих этих целей для предотвращения ОД/ФТ/ФРОМУ и других финансовых преступлений таким образом, чтобы фундаментальные права граждан на неприкосновенность частной жизни, а также на защиту данных были полностью соблюдены.

4. Новые и активно разрабатывающиеся технологии повышения конфиденциальности предлагают перспективные способы защиты личных данных в конкретных случаях их применения, а также в соответствии с национальным и международным законодательством в области защиты данных и обеспечения неприкосновенности частной жизни. В технологиях повышения конфиденциальности используется целый ряд различных криптографических инструментов, позволяющих обеспечить защиту персональных данных в различных сферах применения. Эти инструменты позволяют различным сторонам содержательно взаимодействовать между собой для достижения цели применения, не предоставляя основную личную информацию друг другу или третьим сторонам. Этой теме посвящено постоянно увеличивающееся количество исследований и обсуждений, однако технические стандарты до сих пор не выработаны. Для разработки таких стандартов и создания ссылок на открытые источники предстоит осуществить еще много работы, которая позволит прояснить конкретные случаи использования, при которых технологии повышения конфиденциальности могут обеспечить защиту конфиденциальных данных.

© FATF/OECD 2021

5. В этом аналитическом отчете рассматриваются уже имеющиеся на рынке, а также находящиеся на стадии разработки технологии, которые обеспечивают проведение расширенного анализа ПОД/ФТ внутри отдельных подотчетных субъектов, а также совместного анализа между финансовыми учреждениями. В данный отчет также включен анализ намеченных целей и движущих факторов, связанных с использованием этих новых технологий. В нем также высказаны стратегические соображения и содержатся возможные решения, которые могут быть использованы при обсуждении или внедрении таких технологий.

6. ФАТФ продолжит свой диалог с органами, осуществляющими надзор в области ПОД/ФТ, разработчиками технологий, финансовыми учреждениями и с органами власти, обеспечивающими неприкосновенность и защиту личных данных, а также с другими соответствующими экспертами. Это обеспечит использование в полной мере новых технологий, которые могут повысить эффективность ПОД/ФТ, в соответствии с национальным и международным законодательством в области обеспечения неприкосновенности и защиты личных данных.

© FATF/OECD 2021

Введение

7. Под объединением данных и совместным анализом подразумевается процесс анализа (цифровых) данных из различных источников (в т. ч. разными сторонами). Эти данные могут быть сгруппированы централизованным способом (объединение данных) или распределенным образом (совместный анализ)[1]. В этом документе рассматриваются вопросы, связанные с объединением данных и совместным анализом между финансовыми учреждениями (ФИ), в том числе входящими в состав международных финансовых групп и не входящими в них. Они несут в себе определенные преимущества, но вместе с тем характеризуются значительными рисками. Эти способы могут потребовать использования аналитических инструментов, которые способны усилить совместное понимание, оценку и снижение рисков ОД/ФТ, что приведет к более динамичному, эффективному и действенному выявлению деятельности подобного рода. Они могут привести к уменьшению ложноположительных случаев, обеспечивая эффективное соблюдение установленных требований представителями частного сектора наиболее оперативным и наименее обременительным образом. Кроме того, это помогает предотвратить использование информационных пробелов, позволяющих использовать разницу в нормативной базе различных юрисдикций злоумышленниками, которые могут попытаться прибегать к услугам многочисленных национальных и международных финансовых учреждений, каждое из которых имеет ограниченное и частичное представление об операциях. Однако использование таких методов может привести к нарушению прав граждан и фундаментальных прав. Таким образом, очень важно, чтобы при обмене информацией соблюдались требования национального и международного законодательства в области защиты и неприкосновенности данных.

8. Успехи, достигнутые недавно в области технологий, позволяют финансовым учреждениям более эффективно анализировать большие объемы структурированных и неструктурированных данных, а также распознавать шаблоны и тенденции. Использование больших массивов данных и самых современных методов анализа таких, как искусственный интеллект[2] способно усилить соблюдение требований в области ПОД/ФТ учреждениями финансового сектора, но также сопряжено с возникновением рисков для фундаментальных прав и прав граждан в случае обмена личными данными или в тех случаях, когда соответствующим процессам не хватает надлежащей объяснимости, что может привести к неправильным или ошибочным результатам. Например, финансовые учреждения могут использовать современные методы анализа для более тщательного выявления подозрительной деятельности, проверки клиентов и управления рисками. Поскольку точность современных методов анализа в целом соответствует размеру, качеству и релевантности набора данных, эффективность этих инструментов может зависеть от способности финансовых учреждений (входящих в состав финансовых групп и не входящих в них) обмениваться информацией.

9. Технологии, которые позволяют обмениваться данными, объединять или анализировать их, должны защищать личные данные в соответствии с национальным и международным законодательством. Таким образом, потребность в обмене данными требует тщательного анализа его влияния как на ПОД/ФТ, так и на неприкосновенность и защиту данных. На-

[1] При совместном анализе данные не перемещаются в какое-то одно место для их анализа совместно с другими данными. Вместо этого аналитические инструменты «приходят» к данным, а не наоборот. Это облегчает обеспечение секретности данных, а также обеспечивает контроль за тем, кто получает доступ к каким данным и для каких целей..

[2] Список определений основных понятий, связанных с цифровой трансформацией, приведен в Приложении А.

© FATF/OECD 2021

пример, финансовое учреждение должно собирать и обрабатывать личные данные (минимизация данных), необходимые исключительно для достижения конкретной, заранее определенной цели (ограничение цели) и не обрабатывать их дополнительно таким образом, который будет противоречить этим целям. Информацией следует также обмениваться для достижения конкретной цели, которая не может быть достигнута с помощью использования менее инвазивных мер, требующих меньшего доступа к личным идентификационным данным. Кроме этого, собранные данные должны храниться в течение необходимого периода времени и не должны передаваться учреждению, которое не имеет соответствующих правил защиты данных.

10. Новые и активно разрабатывающиеся технологии повышения конфиденциальности предлагают перспективные способы защиты личных данных при их различном использовании, а также в соответствии с национальным и международным законодательством в области защиты данных и обеспечения неприкосновенности частной жизни. В технологиях повышения конфиденциальности используется целый ряд различных криптографических инструментов, позволяющих обеспечить неприкосновенность персональных данных в различных сферах применения[3]. Эти инструменты позволяют различным сторонам содержательно взаимодействовать для достижения цели применения, не предоставляя основную личную информацию друг другу или третьим сторонам. Хотя этой теме посвящено постоянно увеличивающееся количество исследований и обсуждений, технические стандарты до сих пор не выработаны. Для разработки стандартов и создания ссылок на открытые источники предстоит выполнить большой объем работы, которая позволит прояснить, обеспечат ли технологии повышения конфиденциальности защиту личных данных в конкретных случаях применения. Более того, если целью таких технологий является использование данных для выявления конкретных физических или юридических лиц (например, для принятия на обслуживание клиентов), это может отрицательно сказаться на защите неприкосновенности данных. Таким образом, обмен данными в некоторых юрисдикциях в настоящее время может ограничиваться обменом неличных данных (например, корпоративными данными, из которых исключены данные, имеющие отношение к клиентам), на которые не распространяется действие соответствующих правовых требований в области обеспечения неприкосновенности и защиты данных.

11. В июне 2020 г. в соответствии с приоритетами президентства Германии в ФАТФ, связанными с цифровой трансформацией в области ПОД/ФТ, ФАТФ согласилась провести критическую оценку объединения данных, совместного анализа и защиты данных. Целью этого мероприятия является изучение уже имеющихся или находящихся на стадии разработки технологий, которые позволяют осуществлять расширенный анализ в области ПОД/ФТ внутри подотчетных субъектов или совместный анализ между финансовыми учреждениями, а также выявлять проблемы и находить возможные решения для того, чтобы эти технологии можно было использовать в полной мере с целью укрепления соблюдения норм в области ПОД/ФТ в соответствии с национальным или международным законодательством в области обеспечения неприкосновенности и защиты данных.

---

[3] К технологиям повышения конфиденциальности относятся следующие технологии: гомоморфное шифрование, полностью гомоморфное шифрование, доказательство с нулевым разглашением конфиденциальных сведений, протокол конфиденциального вычисления, функциональное шифрование, групповая и кольцевая подписи, получение скрытой информации, пересечение частных наборов, шифрование с возможностью поиска, слепые подписи https://csrc.nist.gov/CSRC/media/Projects/pec/documents/suite-draft1.pdf, шифрование на основе идентификации и т.д. См., например, https://csrc.nist.gov/projects/pec; https://csrc.nist.gov/CSRC/media/Presentations/icmc2020-slides/images-media/20200923-PEC-ICMC-slides.pdf; https://zkproof.org/

© FATF/OECD 2021

12. Этот аналитический отчет организован следующим образом: Раздел 2 содержит описание предыдущей работы ФАТФ, связанной с обменом данными учреждениями частного сектора, в Разделе 3 излагаются намеченные цели и движущие факторы, связанные с использованием новых технологий для обмена данных и их анализа учреждениями частного сектора, в Разделе 4 описываются различные новые технологии, которые разрабатываются или уже используются, в Разделе 5 перечислены проблемы и препятствия, с которыми столкнулись те, кто отвечал на Опросник, при разработке или внедрении этих технологий, в Разделе 6 приведены решения, предлагаемые респондентами, по отношению к более широкому внедрению новых технологий (которое еще не утверждено ФАТФ).

13. Что касается охвата этого мероприятия, в этом документе рассматриваются объединение данных и совместный анализ, осуществляемые учреждениями частного сектора (в т.ч. мероприятия, поддерживаемые или инициируемые государственными органами власти). Использование новых технологий для обмена информацией между государственными органами и учреждениями частного сектора, в частности, между подотчетными субъектами и ПФР/правоохранительными органами рассматривается в отдельном документе под названием «Цифровая трансформация ПОД/ФТ для учреждений, осуществляющих оперативную работу».

© FATF/OECD 2021

2. Методология

14. В ноябре 2020 г. ФАТФ направила через Интернет Опросник, посвященный цифровой трансформации, органам власти различных стран, отвечающим за ПОД/ФТ, и учреждениям частного сектора (в т.ч. ученым, финансовым учреждениям и разработчикам технологий) для получения информации о существующих новых технологиях, позволяющих осуществлять совместный анализ. В общей сложности было получено 188 заполненных Опросника. В этом документе суммируются результаты Опросника, а также камеральных исследований и бесед с сотрудниками государственных органов и представителями учреждений частного сектора, в т.ч представителями финансовых учреждений, разработчиков технологий, органов власти, отвечающих за ПОД/ФТ, а также за обеспечение неприкосновенности и защиты данных.

15. Опросник позволил собрать мнения основных действующих лиц о предполагаемых результатах использования новых технологий с целью осуществления совместного анализа, а также о том, как новые технологии используются для обеспечения безопасности, совместной работы над данными и их анализа. Он также включал в себя вопросы о проблемах и стратегических соображениях, связанных с внедрением таких технологий и взаимодействием с органами, осуществляющими надзор в области ПОД/ФТ и обеспечения неприкосновенности и защиты данных. В Опроснике также содержалась просьба к респондентам привести примеры конкретных случаев, иллюстрирующих полезный опыт (в дальнейшем под «респондентами» будут подразумеваться те, кто направил заполненный Опросник, и эксперты, к которым обратился Секретариат, в т.ч. эксперты, предложенные делегациями стран в ФАТФ).

16. На рисунке ниже приведена разбивка заполненных Опросников по секторам. В секторе государственных органов большую часть респондентов составили надзорные органы, а в частном секторе большая часть информации поступила от финансовых учреждений и разработчиков технологий[4]. Наибольший вклад в Опросник внесли учреждения, классифицируемые как «крупные банки». Большая часть респондентов находится в Европе (53%), за ней следуют Южная и Северная Америки (20%), Азия и Океания (18%) и Африка (9%)[5].

Рисунок 1. Разбивка респондентов по секторам

[4] Из респондентов-представителей частного сектора 54% пришлось на долю финансовых учреждений, а 46% - на долю поставщиков технологий.

[5] Под «Другими» респондентами подразумеваются НКО, аналитические центры и ученые.

© FATF/OECD 2021

3. Основная информация

17. Объединение данных и совместный анализ не являются абсолютно новыми темами для ФАТФ. Некоторые из Рекомендаций ФАТФ содержат элементы, связанные с обменом информацией между учреждениями частного сектора. Например, Рекомендация 18 требует обмениваться информацией в рамках финансовых групп для целей НПК и управления рисками ОД/ФТ. Такой обмен предусматривает обмен информацией и анализом операций или деятельности, которые, по всей видимости, являются необычными (если такой анализ проводился); и может включать в себя СПО, основополагающую информацию или факт направления СПО. Это требование применяется ко всем субъектам (как осуществляющим свою деятельность в пределах одной страны, так и осуществляющим свою деятельность за рубежом), которые подпадают под определение понятия «финансовая группа» в Глоссарии ФАТФ[6]. Помимо этого, Рекомендация 21 требует, чтобы финансовые учреждения, а также их директора, должностные лица и работники по найму могли раскрыть факт направления СПО или связанной с ним информации, если это соответствует требованиям, касающимся управления рисками ОД/ФТ, которые применяются на уровне группы и которые предусмотрены в Рекомендации 18. Наконец, в Рекомендации 2, которая требует от органов власти осуществлять сотрудничество и взаимодействие для обеспечения соответствия требований в области ПОД/ФТ положениям, касающимся неприкосновенности и защите данных, а также другим подобным положениям, подчеркивается важная роль, которую органы власти играют при преодолении препятствий, возникающих при обмене информацией и существующих в действительности или предположительно.

18. Хотя в этих рекомендациях изложены параметры для обмена информацией в рамках финансовой группы, в настоящее время Стандарты ФАТФ не содержат подобных требований к обмену информацией за пределами финансовых групп.

19. В 2017 г. ФАТФ опубликовала свое Руководство относительно обмена информацией между учреждениями частного сектора. В этом Руководстве содержатся инициативы, касающиеся обмена информацией, осуществляемого финансовыми учреждениями, которые выходят за пределы Рекомендаций ФАТФ (с. 22-25). С тех пор в этой области регионы и отдельные страны выдвинули ряд инициатив. Например, в необязательном пункте 46 декларативной части пятой Директивы в области ПОД Европейского союза говорится, что *«злоумышленники перемещают незаконные доходы с помощью многочисленных финансовых посредников для того, чтобы избежать обнаружения. Таким образом, важно дать возможность кредитным и финансовым учреждениям обмениваться информацией не только между членами одной группы, но также с другими кредитными и финансовыми учреждениями, уделяя должное внимание правилам защиты данных, содержащихся в законодательствах отдельных стран».*[7] В декабре 2020 г. Совет по защите данных Европы (СЗДЕ) также выступил с заявлением, в котором говорилось, помимо всего прочего, что ожидаемое внесение из-

[6] В Глоссарии ФАТФ содержится следующее определение понятия «финансовая группа» - группа, которая включает материнскую компанию или юридическое лицо любого другого типа, осуществляющее функции контроля и координации в отношении остальной части группы по осуществлению группового надзора согласно Основным принципам, вместе с филиалами и/или дочерними предприятиями, подлежащими правилам ПОД/ФТ и процедурам на уровне группы.

[7] Пункт 46 декларативной части Директивы (ЕС) 2018/843 Европарламента и Совета Европы от 30 мая 2018 г., вносящий изменения и дополнения в Директиву (ЕС) 2015/849 о предотвращении использования финансовой системы для целей ОД или ФТ, а также вносящий изменения и дополнения в Директивы 2009/138/ЕС и 2013/36/ЕС.

© FATF/OECD 2021

менений в законодательство[8] позволит устранить противоречие между защитой личной жизни/личных данных и мерами в области ПОД/ФТ. СЗДЕ отмечает, что он уверен в том, что более четкое разделение двух наборов правил (в области ПОД/ФТ и в области обеспечения неприкосновенности личной жизни и защиты данных) принесет пользу как защите личных данных, так и эффективности системы ПОД. СЗДЕ подчеркивала необходимость наличия четкого правового основания для обработки личных данных и указания целей и сроков такой обработки в соответствии с пунктом 5(1) Общих положений о защите данных (ОПЗД ЕС), в частности по отношению к обмену информацией и передаче информации на международном уровне (СЗДЕ, 2020, [1]).

20. С внедрением и началом применения различных технологий повышения конфиденциальности[9] учреждения частного сектора начали осуществлять ряд инициатив и пилотных программ, направленных на объединение и совместный анализ данных, в т.ч. данных по НПК, для усиления соблюдения требований в области ПОД/ФТ и более эффективного выявления незаконной деятельности. Эти международные инициативы свидетельствуют о стремлении финансовых учреждений совместно использовать и объединять ресурсы, а также о том, что ФАТФ необходимо разработать новые руководства для решения проблемы, связанной с объединением данных и совместным анализом, учитывая существование новых технологий.

[8] ЕС планирует издать единый свод правил в виде согласованного положения, касающегося ПОД.

[9] Технологии повышения конфиденциальности (зачастую их называют «шифрование, обеспечивающее неприкосновенность личной жизни») представляют собой «особые возможности шифрования, которые позволяют осуществлять обработку данных, служащих основанием для обработки, при этом владелец данных не обязательно разглашает такие данные. Такая технология может обеспечить ситуацию, когда владелец данных не обязательно видит поисковый запрос, при этом запрос и его результаты остаются зашифрованными (или не разглашаются) и являются видимыми только для лица, осуществляющего запрос». (Максвелл, 2020 [16])

© FATF/OECD 2021

4. Цели и предварительные условия для передачи и анализа информации в сфере ПОД/ФТ в частном секторе

21. ФАТФ недавно изучила обмен информацией внутри финансовых учреждений и групп и между такими учреждениями и группами в более узком контексте обмена конкретной информацией в индивидуальном порядке в целях ПОД/ФТ (например, для проверки клиента, который продемонстрировал настораживающие признаки). Настоящий аналитический отчет опирается на эту работу, и в нем рассматривается, как технологические инновации, основанные на крупномасштабном обобщении данных, передаваемых между частными лицами, и на совместной аналитике, могут способствовать достижению целей ПОД/ФТ/ФРОМУ, при этом обеспечивая соблюдение требований в отношении защиты данных и конфиденциальности.

22. Новые технологии, протестированные в других областях, включая шифрование чувствительных личных данных, например, в секторе здравоохранения[10], могут обеспечивать инновационные решения для соблюдения различных национальных и международных законов о защите данных и конфиденциальности, а также для обеспечения передачи и анализа информации в целях ПОД/ФТ. Действительно, согласно результатам анкетирования, 93% респондентов считают, что новые технологии могут помочь преодолеть эти и другие проблемы обмена данными в сфере ПОД/ФТ (например, защита конфиденциальной информации в конкурентных целях).

4.1. Зачем передавать данные?

23. Обмен данными имеет решающее значение для борьбы с ОД, ФТ и финансированием распространения оружия массового уничтожения (ФРОМУ). Многонациональные схемы ОД/ФТ/ФРОМУ не соблюдают национальные границы, и преступники используют не одно учреждение для отмывания своих доходов, полученных преступным путем. Часто незаконная деятельность становится очевидной только тогда, когда учреждения и органы власти могут изучить совокупную деятельность субъекта, осуществляемую через различные границы и платформы. Об этом свидетельствуют различные международные дела об ОД, в которых использовались слабые места финансовых учреждений различных юрисдикций для отмывания значительных сумм доходов от преступной деятельности. Скоординированные оценки совокупной деятельности нескольких учреждений могут повысить общее качество полученных данных финансовой разведки.

24. Чтобы эффективнее предотвращать и выявлять злонамеренное использование международной финансовой системы в целях ОД/ФТ, финансовые учреждения могут рассмотреть возможность сотрудничества, если и когда это соответствует требованиям в отношении защиты данных и конфиденциальности в пределах финансовой группы, а также между финансовыми учреждениями, не являющимися частью одной и той же финансовой группы. В то же время финансовые учреждения должны осознавать ответственность, которую они понесут за нарушение требований в отношении защиты данных и конфиденциальности. Как правило, финансовым учреждениям не рекомендуется передавать личные данные, если параметры такого обмена данными (типы данных, обстоятельства обмена, каналы связи и т. п.) явно не предусмотрены законодательством юрисдикции, в которой осуществляется деятельность.

[10] Например, использование федеративных данных (или федеративного обучения) — усиливающаяся тенденция в секторе здравоохранения, которая облегчает обмен информацией и сотрудничество в исследованиях (Тим Хальсен, 2020 [19]).

© FATF/OECD 2021

25. Такой обмен информацией может поддерживаться властями, но также может происходить на уровне отрасли без обязательного участия правительства, если параметры и цель совместной работы с данными четко определены законодательством и если существует эффективный надзор за защитой данных в частном секторе.

26. Респонденты отметили, что получение доступа к более широкому набору данных может улучшить результаты и позволить принимать решения на основе разведданных за счет уменьшения количества ложноположительных результатов, определения приоритетов, повышения эффективности расследования финансовых преступлений, повышения качества корпоративных данных и повышения эффективности операционной деятельности. Конечно, качество и стандартизация данных являются важными элементами, обеспечивающими точность совместной аналитики в целом, как указано в разделе 6.2.

27. Расширенная аналитика, применяемая к данным, которыми обмениваются несколько финансовых учреждений, может выявить тенденции или потенциально подозрительные виды деятельности, которые в противном случае могли бы остаться незамеченными одним учреждением. Например, респонденты отметили, что такие инструменты и методы, как резолюции учреждений и сетевой анализ, позволяют идентифицировать связи, которые с большей вероятностью останутся незамеченными, когда данные фрагментарны, а технологические решения для следователей ориентированы на проверку отдельных учреждений на соответствие требованиям. Более того, использование аналитики позволяет финансовым учреждениям анализировать риски финансовых преступлений на должном уровне и с гораздо большим упреждением выявлять риски. Соответственно, новые технологии, вероятно, повысят ценность и полезность передаваемой информации. В описанном ниже ситуационном исследовании приводятся примеры преимуществ, достигнутых при проверке концепции передачи данных в 2018–2020 гг. в Великобритании.

Вставка 4.1. Пилотный проект Великобритании Tribank

Пилотный проект TriBank, реализованный в Великобритании в 2019 году, включал в себя три крупных банка и объединял псевдонимизированные данные об операциях (то есть даты, суммы и снабженные метками счета отправителя и получателя) для их комплексного анализа. Банки-участники не раскрывали информацию, позволяющую установить личность (например, имена и адреса). В ходе пилотного проекта было продемонстрировано, что псевдонимизированные данные об операциях могут безопасно и эффективно собираться у нескольких участвующих финансовых учреждений, объединяться и связываться в значимый унифицированный набор данных и централизованно подвергаться анализу. Технологическая платформа продемонстрировала, что без каких-либо знаний о базовых операционных счетах большие и сложные кластеры могут автоматически идентифицироваться, вычленяться из базы данных счетов и становиться кандидатами для дальнейшего анализа, проводимого участвующими учреждениями.

Этот пилотный проект продемонстрировал два взаимодополняющих подхода к совместной аналитике в сфере ПОД/ФТ: 1) участвующие финансовые учреждения предоставили исходную информацию о подозрительных/вызывающих опасения

© FATF/OECD 2021

счетах, а платформа значительно расширила эти основные разведданные, чтобы показать «общую картину»; а также 2) сама платформа автоматически определила важные области, вызывающие озабоченность, без каких-либо основных разведданных, предоставляемых финансовыми учреждениями. Эти два подхода работают совместно и создают эффективную структуру мониторинга межбанковских операций, позволяющую каждому участвующему учреждению вносить свои разведданные и извлекать выгоду из разведданных другого учреждения без необходимости раскрытия какой-либо конфиденциальной информации о клиентах.

28. Кроме того, некоторые респонденты отметили, что в некоторых регионах с появлением ФинТех и других новых участников рынка в банковском секторе клиенты уходят от традиционных банков и используют услуги нескольких учреждений для осуществления банковских операций вместо того, чтобы работать с одним финансовым учреждением, захватившим большую долю рынка. Это означает, что данные об отдельных клиентах становятся все более рассредоточенными среди многочисленных финансовых учреждений, что затрудняет получение информации об ОД и ФТ на основе данных, доступных только одному учреждению. Это дает дополнительный стимул для обмена данными между частными лицами, а также для совместной работы с целью объединения достаточных наборов данных для применения расширенной аналитики с целью более точной оценки клиентских рисков или выявления возможной подозрительной деятельности.

29. Тем не менее, обработка данных должна быть соразмерна преследуемой законной цели их использования. На всех этапах обработки должен обеспечиваться благоприятный баланс между всеми заинтересованными сторонами и правами. Точнее, личные данные должны обрабатываться должным и прозрачным образом и собираться для явных, указанных и законных целей в соответствии с правилами хранения данных. Все аспекты обмена данными и использования технологий, включая эффективность ПОД/ФТ, а также влияние требований в отношении защиты данных, конфиденциальности и конкуренции, должны оцениваться в первую очередь для того, чтобы все аспекты были приняты во внимание до запуска проектов.

4.2. Каковы заявленные цели инициатив по обобщению данных, передаваемых между частными лицами?

30. Несмотря на то, что список не является исчерпывающим, финансовые учреждения могут принимать решения о передаче данных, в том числе за пределы финансовых групп и, возможно, в другие юрисдикции, чтобы облегчить:

- применение ***мер*** надлежащей проверки клиентов, таких как:
  - *оценка институционального риска* — для более точной оценки рисков ОД/ФТ с целью использования более точных показателей для новых продуктов и услуг;
  - *прием клиентов на обслуживание* — для определения того, вызывало ли физическое или юридическое лицо ранее индикаторы опасности или проблемы с другим учреждением в пределах или за пределами финансовой группы; для проверки рейтинга риска клиентов путем выявления возможного аналогичного поведения в других направлениях бизнеса;

© FATF/OECD 2021

- *мониторинг операций* — для обнаружения расслоения средств путем изучения модели операций клиента для оценки финансового профиля; для последующего контроля любой аномальной деятельности учреждений; для более эффективного выявления подозрительной деятельности; для применения пороговых значений сумм операций;

- *управление рисками деловых отношений* — для постоянного обновления информации о клиентах; для определения глобальной подверженности риску в результате приема на обслуживание одного и того же клиента несколькими учреждениями; для динамического управления рисками с целью отражения новой информации или изменений в поведении клиентов;

- *выявление бенефициарного собственника* — для повышения точности идентификации бенефициарных собственников; для определения одного и того же бенефициарного собственника разных учреждений; для более эффективного обнаружения подставных компаний; для разработки более эффективного учета информации о бенефициарных собственниках;

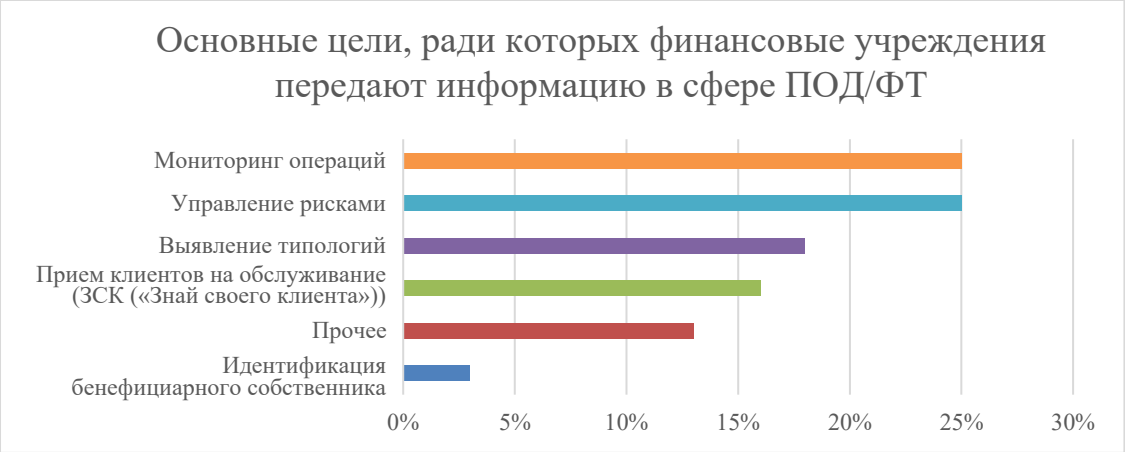
- сквозной ***технический поток***, такой как:

  - *выявление типологий преступлений* — для более быстрого и точного выявления возникающих типологий преступлений и реализации мер защиты, а также для обмена результатами с другими учреждениями и государственным сектором;

  - *расследования на основе разведданных* — для согласования усилий по проведению расследования и получения более определенных следственных заключений.

31. Исходя из результатов анкетирования, основная причина передачи или обобщения данных для целей ПОД/ФТ — это мониторинг операций. Однако некоторые респонденты отметили, что целями таких инициатив могут быть несколько вариантов из приведенного выше списка. В приведенной ниже таблице обобщены ответы на вопросы анкеты, в которых указаны различные цели, ради которых финансовые учреждения могут передавать информацию в сфере ПОД/ФТ.

Рисунок 2. Основные цели, ради которых финансовые учреждения передают информацию в сфере ПОД/ФТ



Примечание к таблице. Каждый респондент мог выбрать только один ответ из приведенного выше списка.

© FATF/OECD 2021

32. Некоторые примеры «прочих» причин для передачи данных в сфере ПОД/ФТ:

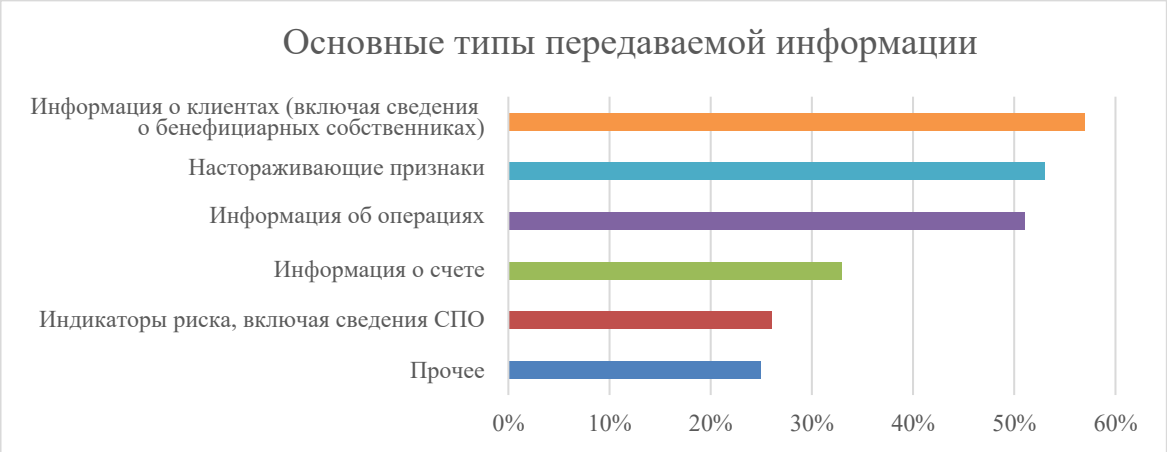
    - снижение риска в целях содействия принятию более эффективных решений при обнаружении, предотвращении и расследовании ОД/ФТ в более общем смысле;
    - упрощение цикла обратной связи в целях разработки и оптимизации параметров обработки данных;
    - проведение расследований на основе разведданных;
    - содействие разработке типологий преступлений на основе данных.

4.3. Какой тип данных может передаваться?

33. Для достижения указанных выше конкретных целей зашифрованные передаваемые данные могут включать: информацию НПК; операции; настораживающие признаки; признаки клиентского риска, например, было ли направлено СПО; обновленную информацию об учреждениях, с которыми установлены корреспондентские банковские отношения, включая информацию о клиентах, если она может облегчить оценку рисков и надлежащую проверку, которую проводят учреждения.

34. Согласно результатам анкетирования, основным *типом* передаваемых данных (которые передаются в настоящее время или передача которых обсуждается) является информация о клиенте (включая сведения о бенефициарных собственниках), информацию, относящуюся к настораживающим признакам, а также данные об операциях. Респонденты отметили, что часто передается комбинация данных разных категорий в зависимости от конкретной цели инициативы. Однако некоторые респонденты также отметили, что информация о клиентах передается только в зашифрованном виде и в ситуациях малого количества доказательств концепции. На приведенной ниже схеме приводится сводка результатов анкетирования, показывающая основные типы информации, которая передается в настоящее время или передача которой обсуждается респондентами анкеты.

Рисунок 3. Основные типы передаваемой информации



Примечание к таблице. Каждый респондент мог выбрать несколько или все ответы из приведенного выше списка.

© FATF/OECD 2021

35. Некоторые примеры «прочих» типов передаваемых данных:

- справочные данные кода идентификации юридического лица[11];
- типологии; а также
- выдача/результаты оповещений (для настройки внутренней модели).

Вставка 4.2. Японский проект доказательства концепции машинного обучения и искусственного интеллекта

Чтобы облегчить передачу данных в соответствии с нормами защиты данных и конфиденциальности в Японии был разработан уникальный проект подтверждения концепции (POC) с участием нескольких японских финансовых учреждений, поддерживаемый Агентством финансовых услуг Японии и спонсируемый Японской организацией по развитию новых энергетических и промышленных технологий (NEDO). В рамках этого проекта объединяются алгоритмы искусственного интеллекта (ИИ) с инструкциями из каждого набора данных операций финансовых учреждений, без передачи или группировки данных, и создается единая модель ИИ.

Проект направлен на создание модели ИИ, помогающей человеку сделать суждение, и включает расчет вероятности истинно положительной оценки для мониторинга операций и проверки по санкционным перечням.

В этом проекте данные об операциях отдельных финансовых учреждений не передаются и не группируются. Используются следующие два подхода: (1) интеграция самих моделей ИИ, уже изучивших наборы данных каждого учреждения; (2) настройка модели ИИ, которая уже изучила набор данных одного учреждения, для изучения другого банка, и продолжение этого процесса для повышения точности данной модели ИИ.

Согласно результатам данного проекта, совместная система мониторинга и проверки операций на базе ИИ обладает достаточным потенциалом для снижения рабочей нагрузки и включает сортировку обнаруженных ложноположительных результатов и работу с ними. С точки зрения точности и интерпретируемости результаты показывают, что некоторые операции, выполняемые человеком при обычной сортировке, можно заменить суждением на базе ИИ. Распространение этой инициативы на более широкий круг участников финансового сектора может повысить эффективность и результативность ПОД/ФТ в целом.

[11] Код идентификации юридического лица (LEI) — это 20-значный буквенно-цифровой код, который позволяет четко и однозначно определить юридических лиц, участвующих в финансовых операциях. Дополнительная информация приводится в документе «Знакомство с кодом идентификации юридического лица (LEI)», Фонд GLEIF, www.gleif.org/en/.

© FATF/OECD 2021

4.4. Инициаторы и предварительные условия использования новых технологий

36. В этом разделе кратко излагаются сложившиеся условия использования новых технологий для обмена данными между частными лицами и совместной аналитики для целей ПОД/ФТ, а также определены благоприятствующие факторы, инициаторы и предварительные условия, которые способствуют развитию и последующему внедрению таких технологий.

37. Согласно результатам анкетирования, 40% респондентов заявили, что финансовые учреждения в их юрисдикции используют новые технологии для передачи или объединения данных с другими финансовыми учреждениями в целях ПОД/ФТ. 72% этих респондентов заявили, что такие инициативы были совместно разработаны государственным и частным секторами.

38. В приведенном ниже ситуационном исследовании представлен пример совместно разработанной модели обмена информацией между частными лицами в сфере ПОД/ФТ.

Вставка 4.3. Тестирование платформы обмена информацией в Китае

Под руководством и контролем Народного банка Китая — Бюро по противодействию отмыванию денег Народного банка Китая — проводится пробный запуск платформы обмена информацией о рисках ОД (далее — «платформа обмена информацией») между несколькими китайскими финансовыми учреждениями, которая объединяет блокчейн, цифровую идентификацию и надежные технологии повышения конфиденциальности. Эта пробная платформа позволяет участвующим финансовым учреждениям шифровать информацию о высокорисковых клиентах, включая цифровой идентификационный номер и метки риска, идентифицированные учреждением, а затем загружать ее на блокчейн-платформу. Когда участвующее учреждение делает запрос о клиенте, выполняется сопоставление посредством блокчейн через защищенную вычислительную платформу. Цифровой идентификационный номер сопоставляется только в том случае, если фамилия/имя и номер национального удостоверения личности искомого человека были загружены другими участвующими финансовыми учреждениями. После сопоставления платформа обмена информацией извлекает информацию о рисках ОД и возвращает ее в закодированном виде для расшифровки; блок обработки также немедленно удаляет любые записи о таких вычислениях. Затем финансовое учреждение, направившее запрос, получает оповещение о том, что физическое лицо также является высокорисковым для другого финансового учреждения, или ему будут адресованы запросы других финансовых учреждений. Следовательно, в этом проекте фактический обмен данными о клиентах между учреждениями не происходит.

39. Кроме того, ответы на вопросы анкеты показывают, что большинство инициатив, использующих новые технологии для облегчения совместной аналитики и объединения данных частных компаний, в настоящее время находятся на начальной стадии разработки и тестирования. Например, большинство респондентов (74%) отметили, что внедрение таких технологий либо все еще обсуждается, либо эти технологии находятся на этапах разработки/тестирования. На приведенной ниже схеме представлены ответы на вопросы анкеты о текущих этапах внедрения этих новых технологий.

© FATF/OECD 2021

Рисунок 4. Стадия внедрения новых технологий передачи данных

40. Как показано в таблице ниже, респонденты отметили, что различные инициативы по тестированию и использованию новых технологий для объединения данных и совместной аналитики инициируются частным сектором, особенно крупными многонациональными финансовыми учреждениями, розничными и коммерческими банками, а также Интернет-компаниями (FinTech-компаниями и другими).

Рисунок 5. Инициаторы развития и внедрения новых технологий

Примечание к таблице. Каждый респондент мог выбрать несколько ответов из списка выше.

41. Другие движущие факторы использования новых технологий обмена данными — появление технологических разработок, которые могут повысить эффективность и действенность систем ПОД/ФТ, а также наличие благоприятных и четких нормативных рамок для внедрения новых технологий обмена данными между частными лицами.

42. В некоторых юрисдикциях органы регулирования и надзора в сфере ПОД/ФТ тесно взаимодействуют с частным сектором для стимулирования разработки новых подходов и технологий для совместной аналитики и объединения данных в области ПОД/ФТ. Некоторые респонденты отметили, в частности, что при разработке новых проектов проводят-

© FATF/OECD 2021

ся консультации с органами надзора в сфере ПОД/ФТ и органами, отвечающими за защиту данных и конфиденциальности. Открытый диалог с надзорными органами и властями отмечался частным сектором как необходимый элемент успешных инициатив с использованием новых технологий и их конечной эффективной реализации.

43. В некоторых случаях законодательные поправки назывались в качестве необходимого условия внедрения технологий совместной аналитики между частными лицами. Поэтому в таких случаях взаимодействие с директивными органами в сфере ПОД/ФТ и органами надзора в сфере ПОД/ФТ является необходимым условием успеха этих инициатив. В приведенном ниже ситуационном исследовании описывается инициатива частного сектора по объединению данных в сфере ПОД/ФТ, для дальнейшей реализации которой требуется внесение поправок в законодательство. Это ситуационное исследование демонстрирует важность открытого диалога между различными компетентными органами и представителями частного сектора.

Блок 4.4. Программа мониторинга транзакций (Нидерланды)

Голландская программа мониторинга транзакций «Transaction Monitoring Netherlands» (TMNL) — общая инициатива пяти банков из Нидерландов по совместному мониторингу платежных операций с целью обнаружения признаков ОД или ФТ. На момент написания данного текста программа TMNL находится на этапе создания.

Первоочередной целью, которой планируется достичь при использовании технологии совместного мониторинга объединенных данных по транзакциям, является повышение эффективности выявления случаев отмывания денег через обнаружение нетипичных операций, которые отдельные банки сами выявить не могут; программа TMNL будет направлять соответствующие уведомления всем банкам-участникам. Они продолжат, в соответствии со своими обязательствами / в рамках законодательства Нидерландов в сфере ПОД, мониторинг своих собственных транзакций в дополнение к использованию этой платформы коллективного мониторинга.

Участвующие в программе голландские банки будут осуществлять объединение только данных по операциям, производящимся в отношении банковских счетов, которые администрируются на территории Нидерландов. Планируется, что со временем к TMNL смогут присоединиться и другие банки. Когда программа начнет работать, при получении сигнала о потенциально нетипичной транзакции или серии переводов с признаками предполагаемого ОД или других незаконных действий, все участники цепочки платежей получат предупредительное уведомление касательно такой транзакции (или ряда). Банки, получившие уведомления системы TMNL, рассматривают их самостоятельно и сами же принимают решение, направлять ли им сообщение о нетипичной транзакции в адрес голландских ПФР (о таком решении TMNL уведомляться не будет). На момент написания данного документа этот проект нацелен на работу с информацией по транзакциям, относящимся к корпоративным клиентам.

© FATF/OECD 2021

Группа TMNL сейчас занимается созданием платформы, необходимой для получения всех данных по транзакциям, объединения их с целью осуществления совместного мониторинга, а также для формирования уведомлений банкам-участникам о предположительно нетипичной активности. Платформа будет использовать облачные технологии и создается на экземпляре так называемой платформы ускорения вычислений одного из банков-участников. Одним из принципов разработки этой специализированной платформы будет модульная настройка, позволяющая и в дальнейшем использовать самые современные инструментальные средства. Конфиденциальные данные по транзакциям, которыми будут обмениваться банки и TMNL, будут псевдонимизированными.

В целях разработки этого проекта участвующие в нем голландские банки тесно сотрудничают с партнерами из госструктур, такими как Служба защиты данных (Data Protection Authority), Министерства финансов, юстиции и безопасности, Служба фискальной информации и расследований (Fiscal Information and Investigation Service), а также с ПФР. Создание TMNL согласуется с Планом действий по ПОД 2019 г., представленным правительством Нидерландов. Планом предусматривается внесение в Закон о ПОД/ФТ изменений, которые позволят осуществлять комплексный совместный мониторинг транзакций[12]. После внесения поправок голландские банки смогут обмениваться большим объемом данных по транзакциям и информацией о предположительно нетипичных операциях, обойдя, таким образом, запрет на аутсорсинг своих процессов мониторинга транзакций и получив возможность использовать в процессе совместного мониторинга номера государственной службы и индивидуальные идентификационные номера физических лиц.

44. Наряду с открытым диалогом между ФУ и государственными органами, занимающимися вопросами ПОД/ФТ и НЗД, респонденты отмечали важность наличия тестовой среды (или инновационных центров) для обкатки взаимодействия новых технологий с национальными (или наднациональными) законами и нормативными актами в сфере ПОД/ФТ и НЗД. Однако, как об этом сказано в недавнем докладе Рабочей группы FinTech офиса Специального советника Генерального секретаря ООН по вопросам инклюзивного финансирования в целях развития (Working Group of the United Nations Secretary-General's Special Advocate for Inclusive Finance for Development, UNSGSA), подобного рода среду может быть сложно создать и затратно поддерживать[13].

45. Респонденты отмечали, что как тестовая среда (регуляторная песочница), так и инновационные центры являлись бы движущей силой создания благоприятного климата для развития и внедрения новых подходов, поскольку формировали бы условия для нахождения участниками новых возможностей, — а также для выявления рисков и уязвимостей, способствовали бы выработке мер по их минимизации. В нижеследующем блоке приведены примеры создания нормативно-правовой тестовой среды и инновационного центра новых технологий для обмена данными в сфере ПОД/ФТ.

[12] На момент написания законодательство, разрешающее деятельность TMNL, все еще находится в стадии разработки (не было представлено парламенту).

[13] Рабочая группа UNSGSA FinTech и Кембриджский центр альтернативного финансирования (Cambridge Centre for Alternative Finance, CCAF) (2019 г.). «Краткий курс по регуляторным инновациям в целях инклюзивного финансирования FinTech: инновационные офисы, регуляторные песочницы и технологии» (Early Lessons on Regulatory Innovations to Enable Inclusive FinTech: Innovation Offices, Regulatory Sandboxes, and RegTech). Офисы UNSGSA и CCAF: г. Нью-Йорк (США) и Кембридж (Великобритания).

© FATF/OECD 2021

Блок 4.5. Создание нормативно-правовой среды

Великобритания

Управлением по финансовому регулированию и надзору (The Financial Conduct Authority, FCA) в 2019 году был проведен конкурс инноваций TechSprint для изучения возможностей технологий шифрования, известных как технологии повышенной конфиденциальности, в отношении обмена информацией в сфере ОД и финансовых преступлений, при условии соответствия при этом законодательству по обеспечению безопасности данных. Участники мероприятия демонстрировали свои проекты, технологии и полученные результаты. Посетили его представители контролирующих органов в сфере ПОД, а также представители Офиса Уполномоченного по вопросам информации (Information Commissioners Office, ICO, Великобритания). Недавно FCA был реализован проект по созданию тематической цифровой тестовой среды Digital Sandbox Pilot, целью которого было предоставление доступа к комплексным наборам данных по банковским операциям инновационным компаниям-разработчикам новых продуктов и решений по противодействию мошенническим операциям и аферам. Некоторые из этих компаний применяют в своих разработках технологии оценки на основании степени устойчивости к изменениям среды (PET, performance evaluation tool). Этот пилотный проект был завершен в феврале 2021г., и его наработки лягут в основу будущих проектов создания цифровой тестовой среды.

Франция

Французским контрольно-разрешительным органом Autorité de Contrôle Prudentiel et de Résolution (ACPR) был создан инновационный центр FinTech, целью которого было формирование инновационной финансовой экосистемы. Там работает специально подобранная небольшая команда, и центр открыт для всех создателей инновационных проектов, выступая для них своего рода бизнес-инкубатором в сфере инноваций. Также там занимаются внедрением в ACPR надзорных технологий (SupTech) — новых технологических решений для исполнения надзорных функций. За последние два года в этом центре функционировали четыре рабочие группы, занимавшиеся тематикой ПОД/ФТ. Проблемы дистанционной идентификации и проверки клиентов (процедура «знай своего клиента», ЗСК), процессов ПОД/ФТ в сфере криптоактивов, взаимоотношений между банками и поставщиками услуг в сфере криптоактивов с подоплекой потенциала по ПОД и др. рассматривались этими рабочими группами с привлечением представителей отрасли и государственных органов (ПФР, органов, занимающихся безопасностью и защитой данных). Кроме того, инновационным центром ACPR был инициирован диалог с научными кругами касательно возможностей и регуляторных вопросов, связанных с новыми технологиями финансового сектора. В контексте этого, в марте 2020 г. ACPR было организовано мероприятие на тему обмена данными и их объединения с акцентом на возможности, которые дают передовые технологические разработки в том, что касается обмена информацией без обязательного обмена данными. Например, гарантии неприкосновенности данных, предоставляемые технологиями дифференцированной приватности, могут использоваться для об-

© FATF/OECD 2021

учения прогнозных моделей (к примеру, применяющихся в системах мониторинга транзакций) в отношении раскрытия сверхконфиденциальных данных тому или иному конкретному финансовому учреждению. При том, что используется и протокол конфиденциального вычисления, стандартный модуль защищенных совместных процессов, таких как определение KPI по мошенническим номерам счетов IBAN, основывается на пользовательских и операционных данных, полученных от ряда ФУ.

46. В завершение следует отметить, что респонденты также подчеркивали необходимость осуществления тщательной оценки результативности процессов защиты данных при разработке новых технологий объединения данных и совместного анализа. В ряде стран проведение подобной оценки перед началом процесса обработки данных является нормативным требованием в целях минимизации выявленных рисков в отношении прав отдельных лиц.

© FATF/OECD 2021

5. Новые технологии обмена и анализа информации в сфере ПОД/ФТ

47. В этом разделе в общих чертах рассматриваются различные разрабатывающиеся или применяющиеся в настоящее время новые технологии обмена данными между ФУ и их анализа в целях ПОД/ФТ. Информация об этих технологиях была получена на основе анализа вторичных источников (кабинетные исследования) и интервью с респондентами.

5.1. Технологии обмена информацией между представителями частного сектора

48. В таблице ниже представлена сводная информация по новым технологиям, которые рассматриваются для применения при совместном анализе и объединении данных представителями частной экономики. Наиболее часто упоминавшимся типом технологии для объединения данных и их совместного анализа является шифрование, а для анализа больших наборов данных — машинное обучение. При этом респонденты часто отмечали, что для обмена и анализа данных требуется применение различных типов технологий — для обеспечения безопасности и анализа больших массивов данных и для гарантии их соответствия национальным и международным требованиям в сфере НЗД — поэтому разные технологии, информация о которых представлена в нижеследующей таблице, часто применяются одновременно в целях обеспечения безопасности и защиты данных.

Таблица 5.1. Технологии совместного анализа информации частного сектора в сфере ПОД/ФТ

Тип технологии	Описание	Примеры потенциальной пользы для обмена данными в сфере ПОД/ФТ
Технологии шифрования/кодирования		
Гомоморфное шифрование	Позволяет учреждениям сопоставлять и вести поиск по данным третьих лиц без раскрытия содержания поисковых запросов либо без нарушения безопасности или дискредитирования права собственности по отношению к используемым данным. Это означает, что различные стороны могут вести совместную работу с конфиденциальными данными при соблюдении их неприкосновенности, конфиденциальности и соответствия регуляторным требованиям. (Майкрософт, 2016 г. [2])	Доступ к большему объему данных с целью улучшения результатов, возможность принятия решений системами искусственного интеллекта благодаря сокращению количества ложноположительных результатов, повышению эффективности расследования финансовых преступлений, повышению качества корпоративных данных, росту эксплуатационной эффективности.
Протоколы доказательств с нулевым разглашением данных	По своей сущности протоколы доказательств с нулевым разглашением данных являются методом шифрования и верификации, применяемым между доказывающей и верифицирующей сторонами. Доказывающая сторона может доказать верифицирующей наличие у себя информации без раскрытия ее базовых данных или самой информации.	Технология позволит Банку А установить, располагает ли Банк В данными в отношении того или иного лица без раскрытия его личности.

© FATF/OECD 2021

Тип технологии	Описание	Примеры потенциальной пользы для обмена данными в сфере ПОД/ФТ
Протокол конфиденциального вычисления (SMPC)	SMPC дает возможность нескольким сторонам производить действия с частными данными из определенных источников без агрегирования или обмена ими. По завершении протокола сторонам становится известно лишь итоговое расчетное значение. (Scheibner, 2020 г. [1])	Технология может применяться в отношении разноплановых источников данных с целью извлечения достоверных подозрений от разных сторон при сохранении собственности на данные владеющей стороной.
Дифференцированная приватность	Протоколы шифрования, позволяющие каждой стороне сохранять анонимность своих собственных данных при совместных с другими сторонами вычислениях на основании объединенных вводных параметров.	Технология может требовать компромисса между точностью данных и их неприкосновенностью, что может подразумевать большую пригодность для анализа более широких трендов, чем для обнаружения аномалий либо конкретных шаблонов.
Углубленный анализ		
Машинное обучение (контролируемое, неконтролируемое, а также обучение с подкреплением)	Тип ИИ, при котором компьютеры могут обучаться (посредством обучающих алгоритмов) на новых данных, без непосредственного программирования на выполнение определенных задач.	Методы контролируемого обучения могут применяться для разработки моделей расчета комплаенс-рисков на основе имеющихся данных прошлых периодов/результатов проверок. Оптимизация этапов принятия решений в бизнес процессах при помощи моделей машинного обучения через понимание текущего положения и прогнозирование оптимальных решений. Для обнаружения подозрительных сетей и т. п. на основе данных финансовых транзакций или других соответствующих данных могут применяться скоринговые (количественные) или классификационные модели.
Федеративное обучение	Федеративное обучение представляет собой технологию машинного обучения, обучающую алгоритм по данным ряда децентрализованных баз с локальными данными. Алгоритм обучается новой информации (трендам) в каждой, не связанной с другими, базе без обмена или перемещения данных. (Shiffman, 2020 г. [2])	Например, перемещающийся алгоритм может получать доступ к и делать запросы по данным других ФУ без перемещения данных. Целью алгоритма является получение обучающей его информации по новым типам преступной деятельности, ее трендам и методам — знаний, которые он бы не получил, если бы оставался в пределах одной организации. Может способствовать формированию более функциональных инструментов оценки рисков, таких как оперативные показатели рисков.
Глубокое обучение	Глубокое обучение является типом машинного, с применением многоуровневых обучающих алгоритмов для получения значения из большого количества данных.	Например, может внедряться ФУ для мониторинга транзакций.
Обработка естественного языка	Технология обработки естественного языка помогает компьютерам общаться с человеком на его языке и дифференцирует другие связанные с языком задачи. Например, позволяет компьютерам читать текст, слышать речь, интерпретировать ее, понимать эмоции и вычленять важное. (SAS, 2020 г. [3])	Например, может внедряться для трансформации произвольного текста СПО в структурированные данные, которые можно использовать в сетевой аналитике. При применении интеллектуального анализа СПО или любые документы могут автоматически аннотироваться для более эффективного поиска по ним в дальнейшем.

© FATF/OECD 2021

Тип технологии	Описание	Примеры потенциальной пользы для обмена данными в сфере ПОД/ФТ
Роботизированная автоматизация процессов	Программное обеспечение для автоматизации процессов. Программа «робот» программируется на основе модели поведения человека и, симулируя соответствующие взаимодействия, выполняет многочисленные повторяющиеся задачи в больших объемах, быстро и точно.	Позволяет повысить эффективность посредством автоматизации повторяющихся задач, прежде выполняемых человеком.
Сетевой анализ	Использование сетевых данных для обнаружения возможно скрытых трендов и шаблонов в больших массивах данных. Позволяет выявить сложные взаимосвязи между участниками выявленных схем, их признаки.	Выводить шаблоны, которые невозможно было бы иначе увидеть в конечной точке. Сетевой анализ может применяться для выявления сетей связанных лиц на основании данных о предметах интереса.
Инфраструктура обработки и передачи данных		
Доверенная среда выполнения (безопасное вычисление)	Защита используемых данных через проведение изолированных вычислений в доверенной выделенной аппаратной среде выполнения. Эта среда защищена путем выделения части мощности процессора и памяти. (Microsoft Azure, без даты [4])	Две стороны договорились об обмене данными (к примеру, транзакционными) и о проведении их анализа в доверенной среде.
Защищенные облачные технологии	Облачные вычисления представляют собой предоставление сервисов ИТ через интернет, что позволяет бизнесу и властям интенсифицировать внедрение инноваций и сотрудничество. Облачная безопасность подразумевает использование процедур и технологий, защищающих облачную среду вычислений как от внешних, так и от внутренних киберугроз. (McAfee, 2020 г. [5])	Прогресс в сфере облачных технологий позволил компаниям собирать, хранить и анализировать значимо крупные массивы данных при очень низких затратах на это. Технология дает возможность хранить и анализировать как структурированные, так и неструктурированные данные, и может применяться для достижения более тесного сотрудничества между имеющими доступ к защищенной облачной среде. Однако независимо от того, находятся ли данные двух ФУ в одной облачной среде, правовые барьеры для обмена данными остаются прежними.
Технологии распределенного реестра	Поддерживаемый участниками сетевой зашифрованный общий реестр транзакций — чрезвычайно надежный и прозрачный способ хранения информации в, по сути, неизменном виде и в хронологическом порядке. Никакой центральный орган не контролирует такой реестр. (ОЭСР, без даты [6])	Например, может использоваться как способ обмена данными между несколькими сторонами, при котором ни одна из них не имеет всех полномочий на удаление данных. При этом все правовые барьеры для обмена данными остаются прежними.
Интерфейсы прикладного программирования (API)	Интерфейс, позволяющий поднадзорным учреждениям предоставлять свои данные. Облегчает коммуникацию между поднадзорными учреждениями и контролирующими органами посредством интегрированного процесса генерирования данных, благодаря которому достигается более высокий уровень автоматизации и сокращаются затраты на предоставление отчетности. (FSB, 2020 г. [7])	Позволяет эффективнее собирать, хранить и анализировать большие объемы данных.

© FATF/OECD 2021

49. Далее приведены примеры уже применяемых или находящихся в разработке новых технологий для осуществления совместного анализа данных ФУ в целях ПОД/ФТ (дополнительные примеры по Regtech см. в Приложении B).

Блок 5.1. Федеративное обучение

Команда поставщиков аппаратных и программных технологий работает над запуском защищенной платформы федеративного обучения, в среде которой модели машинного обучения можно тренировать на множестве комплектов данных в целях выявления и анализа «нормальных» и «аномальных» шаблонов. При этом модели перемещаются по базам данных в разных локациях, а сами данные никогда не перемещаются, что позволяет модели изучать новые тенденции преступного поведения и способы его реализации, используя массивы данных организаций-участниц проекта при сохранении их неприкосновенности и конфиденциальности. Полученные моделью сведения затем могут использоваться участвующими сторонами для постоянного совершенствования и настройки показателей рисков.

Блок 5.2. Протокол конфиденциального вычисления

Компанией из сферы Regtech разработана технология, позволяющая двум или более ФУ совместно вычислять показатели по оценке рисков, обрабатывая зашифрованные данные о клиентах, а также поведенческую информацию в отношении транзакций и учетных данных без их раскрытия. Эта функция задействуется при использовании технологий обеспечения повышенной конфиденциальности и не требует фактического обмена или раскрытия участниками клиентских данных в какой бы то ни было форме. Технология использует протоколы конфиденциального вычисления для обработки данных на стороне каждого из участников, при этом данные вообще не покидают пределы среды соответствующего участника процесса. Учреждения-участники лишь обмениваются полностью случайными последовательностями данных, не содержащими клиентской информации. Принципиальным моментом является то, что ни одна из сторон не раскрывает свои данные другой стороне ни на каком этапе вычислений. Протокол конфиденциального вычисления модифицирует вычислительный процесс таким образом, что не происходит передачи каких бы то ни было данных, но при этом вычисление результата возможно, как если бы данные были переданы в открытом виде. Эта технология может применяться перед фактической отправкой данных о транзакции или на стадиях осуществления мониторинга и анализа из области ПОД/ФТ. Она также фиксирует все произошедшие в системе события на стороне каждого ФУ. При наличии такого криптографического аудиторского следа по всем клиентам, задействованным в транзакции, внешний аудитор может восстановить весь процесс принятия решения.

© FATF/OECD 2021

Блок 5.3. Гомоморфное шифрование

Regtech-компанией была разработана технологичная универсальная адаптивная структура для осуществления безопасного и конфиденциального проведения процессов идентификации и проверки клиентов (ЗСК), а также НПК, ограниченным кругом доверенных ФУ в целях усовершенствования процессов принятия решений системами искусственного интеллекта. При эффективном использовании гомоморфного шифрования с его исключительными возможностями обработки данных в их зашифрованном виде, эта программа дает ФУ возможность безопасного поиска, обмена и совместной обработки данных третьих лиц без раскрытия содержания самих поисковых запросов либо без нарушения безопасности или дискредитирования права собственности по отношению к используемым данным. При использовании этой модели на принципе децентрализации данных участники процессов никогда не перемещают и не объединяют массивы данных, а их владельцы сохраняют контроль над своими данными и управляют доступом к ним.

В этой модели ЗСК-информация поступает к ряду доверенных участников системы или юрисдикций без перемещения или объединения данных при использовании возможностей ее верификации, осуществляемой одной стороной в отношении данных другой посредством зашифрованного поиска. Аналитики получили возможность безопасно и с соблюдением неприкосновенности сопоставлять и вести поиск регулируемых данных в пределах релевантных (из бизнес-соображений) временных рамок при обеспечении в процессе обработки сохранности конфиденциальных файлов в соответствии с нормативными требованиями. Это технологическое решение продемонстрировало возможности инновационных методов шифрования в решении ключевых проблем финансового сектора, позволяя учреждениям делиться конфиденциальной информацией, лучше понимать клиентские риски и быстрее принимать решения при лучшей информированности — в целях разрешения реальных вопросов из сферы ПОД и борьбы с финансовыми преступлениями.

© FATF/OECD 2021

6. Проблемы, связанные с использованием новых технологий при совместном анализе данных

50. Необходимость объединения данных и совместного анализа финансовыми учреждениями, особенно из разных стран и с участием третьих лиц, порождает целый ряд программно-нормативных вопросов. Некоторые из них были изложены в вышеупомянутом документе «Руководство ФАТФ по обмену информацией в частном секторе» (2017 г.) (FATF Guidance on Private Sector Information Sharing). Появляются и новые поводы — если приступить к обработке более объемных групп данных с использованием усовершенствованных технологий повышения конфиденциальности и передовых методов анализа, таких как применение ИИ.

51. Согласно результатам проведенного опроса, при разработке и внедрении новых технологий обмена данными представителями частного сектора (private-private data sharing) требования обеспечения НЗД являются первоочередными. Среди других часто упоминающихся проблем (см. таблицу ниже) – проблемы нормативного характера (включая моменты, связанные с объяснимостью/интерпретируемостью новых технологий, а также недостаточно мотивирующая регуляторная система) и качество данных (недостаток стандартизированности).

Рисунок 6. Основные проблемы при использовании новых технологий для обмена между ФУ информацией, касающейся ПОД/ФТ

Примечание к таблице: Каждый респондент мог выбрать до 4-х вариантов ответа из указанных в списке.

52. В следующем разделе рассматриваются вопросы и проблемы, связанные с объединением и совместным анализом данных, выявленные на основании проведенного анкетирования, опросов и исследовательского анализа.

© FATF/OECD 2021

6.1. Обеспечение и повышение эффективности защиты и неприкосновенности данных

53. Как меры ПОД/ФТ, так и обеспечение НЗД являются важными задачами государственного уровня, решение которых необходимо для достижения важных целей, не противоречащих друг другу и по своей сути не являющихся взаимоисключающими[14]. Целью реализации правил и принципов защиты данных посредством международных и внутригосударственных правовых инструментов является защита прав и основных свобод человека, в частности, права на неприкосновенность личной информации. Принципиально важно, чтобы системы правового регулирования государств способствовали решению обеих этих задач с целью предотвращения ОД, ФТ, ФРОМУ и других финансовых преступлений, с уважением к основополагающим правам отдельных людей на неприкосновенность и защиту данных. В финансовых данных могут содержаться и самые конфиденциальные сведения о людях, говорящие об их материальном положении, взаимоотношениях в семье, образе жизни и привычках, состоянии здоровья и т. д., — поэтому необходимо учитывать важность и ПОД/ФТ, и НЗД, с соблюдением баланса и согласно обязательствам государств-членов в соответствии с международным законодательством (в том числе в сфере прав человека). По этим правовым нормам одним из самых важных требований является наличие веских законных оснований для обработки персональных данных. При этом нужно придерживаться принципа соразмерности в том, что касается использования альтернативных способов достижения поставленной цели. Ниже приведены требования в этом отношении Конвенции о защите физических лиц в отношении автоматической обработки персональных данных (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETs No. 108)), принятой 28 января 1981 г. и являющейся первым международно правовым документом в сфере защиты данных, носящим юридически обязывающий характер.

Блок 6.1. Конвенция о защите физических лиц в отношении автоматической обработки персональных данных (Конвенция 108+)

Согласно Конвенции 108+, обработка персональных данных может осуществляться на основе: 1) свободного, конкретного, информированного и однозначного согласия их субъекта на обработку ее/его персональных данных или 2) обработки (включая получение) данных, базирующейся на ином законном основании (например, исполнение договора, государственные интересы, обеспечение общественной безопасности, законное право контролирующих органов и т. д.). Если в качестве веских законных оснований выступают согласие, государственные интересы или законное право, представители сферы ПОД/ФТ, НЗД и защиты прав человека из других стран должны тщательно изучить и высказать свое мнение о положенных в основу мотивах.

Как указано в Статье 11 Конвенции 108+, все категории данных для совместного использования, а также цель их обработки должны быть четко определены. Это необходимо для того, чтобы установить срок хранения данных, а также

[14]Например, право на неприкосновенность частной жизни является одним из основополагающих согласно Всеобщей декларации прав человека и Международному пакту о гражданских и политических правах (на региональном уровне — Европейской конвенции о правах человека).

© FATF/OECD 2021

убедиться в соразмерности и оправданности вмешательства в частную жизнь. Помимо этого, Статья 6 гласит, что для предотвращения неблагоприятных для субъекта данных последствий обработки конфиденциальных параметров для законных целей обязательны соответствующие дополнительные меры безопасности: например, явно выраженное согласие субъекта; четкое предписание закона, относящееся к данному конкретному случаю; обязательство по сохранению профессиональной тайны, особые меры технической безопасности (такие как шифрование информации).

54. Как уже говорилось выше, при ОД и ФТ часто задействуется множество организаций и юрисдикций. Для более эффективного выявления подозрительных моделей поведения и минимизации злоумышленного использования финансовой системы ФУ обмениваются информацией и аналитикой в отношении своих клиентов, в том числе и в международном масштабе. ФУ могут стремиться обработать и больше данных с тем, чтобы яснее понимать направления движения криминалитета в существующих условиях. При этом ФУ в равной мере по закону обязаны защищать личные данные своих клиентов.

55. Международные и национальные законодательные акты в сфере НЗД со всей своей неоднозначностью толкований могут быть препятствиями ФУ на пути имплементации обязательств по ПОД/ФТ или при разработке инициатив по обмену информацией в отношении представителей частного сектора. Проблема может стать еще глубже при недостатке регламентирующих руководств или рассогласованности подходов к требованиям по ПОД/ФТ и обязательствам в отношении НЗД. Многосложность различных подходов к вопросу НЗД влияет на наличие, доступность, возможность обработки и обмена информацией со стороны частного сектора.

56. В ходе исследования и по результатам опроса респондентов выяснилось, что существенной проблемой при обмене и объединении данных частных пользователей является субъективно воспринимаемое противоречие между стремлением ФУ делиться информацией для повышения эффективности и действенности усилий по ПОД/ФТ и существующими юридическими ограничениями, направленными на защиту приватности клиентов. Во многих юрисдикциях подобный обмен с выходом информации за пределы финансовой группы ограничен в соответствии с требованиями к неприкосновенности личных данных. И наоборот, в одной из юрисдикций (Соединенные Штаты Америки) существуют исключения («безопасные гавани»), позволяющие обмен информацией в сфере ПОД/ФТ между ФУ, не являющимися частью одной финансовой группы (см. блок ниже).

© FATF/OECD 2021

Блок 6.2. Закон США о борьбе с терроризмом (USA PATRIOT Act), Раздел 314(b)

Разделом 314(b) Закона США о борьбе с терроризмом (USA PATRIOT ACT), касающегося обмена информацией между финансовыми учреждениями, предусматривается, что два или более ФУ или любое объединение ФУ могут добровольно делиться друг с другом информацией в отношении физических и юридических лиц, организаций и стран, подозреваемых в возможном осуществлении террористической деятельности или ОД. Финансовое учреждение или объединение, которое передает, получает или делится такой информацией в целях выявления и сообщения о деятельности, которая может иметь связь с терроризмом или ОД, не несет ответственности перед каким бы то ни было лицом или законом либо подзаконным актом США, конституцией, законодательством или нормативными документами любого штата либо его административно-территориального образования, по какому бы то ни было контракту или иному договору, имеющему юридическую силу (включая любые арбитражные соглашения), за таковое разглашение или невозможность о нем уведомить лицо, являющееся субъектом раскрытия, или любое другое лицо, указанное при таковом раскрытии (ФАТФ, 2017 г.[8])

Согласно Разделу 314(b) («безопасной гавани»), финансовому учреждению или их объединению достаточно иметь разумные основания полагать, что информация, которой они делятся, имеет отношение к деятельности, могущей включать отмывание денег или террористическую активность, и что обмен данными производится с целью, подпадающей под действие Раздела 314(b). Таким образом, финансовое учреждение или их объединение могут делиться информацией о деятельности, которая, по их подозрению, может включать отмывание денег или террористическую деятельность, даже если финансовое учреждение или объединение не может идентифицировать конкретные поступления от определенной незаконной деятельности, в отношении которой производится попытка легализации доходов. (FinCEN, 2020 г. [9])

57. Согласно результатам опроса, большая часть респондентов считает, что с помощью новых технологий можно найти решение уже известных проблем с обменом данных представителей частного сектора, соблюдая при этом как фундаментальные, так и права отдельных лиц, связанные с НЗД. Многие респонденты также отдельно акцентировали свои ожидания по разъяснению в национальных и международных нормах того, когда и в каких целях данные (и какие их типы) могут быть предметом обмена или объединения между ФУ в контексте ПОД/ФТ, в особенности если речь идет об обмене с выходом информации за пределы финансовых групп. Кроме того, респонденты отмечали, что применение новых и активно развивающихся технологий не гарантирует сохранение приватности, если целью является использование данных для идентификации конкретного физического или юридического лица, например, при принятии на обслуживание нового клиента.

58. При наличии понимания необходимости существования общемировых стандартов защиты данных для развития сотрудничества в цифровой сфере, в настоящее время нет такой орга-

© FATF/OECD 2021

низации, которая была бы уполномочена координировать их разработку. Напротив, такие стандарты создаются на уровне отдельных государств или на надгосударственном уровне, поскольку страны должны устанавливать в своих юрисдикциях правовые основы в сфере НЗД. В результате — нет очевидности того, чем руководствоваться при обмене данными между ФУ (касательно видов данных и информации, которыми можно обмениваться, даже если это будет совместный анализ), а также позволят ли организациям эти новые и разрабатывающиеся технологии и процессы соответствовать в своей работе национальным и надгосударственным требованиям в отношении неприкосновенности личных данных.

59. Согласно данным Конференции ООН по торговле и развитию (United Nations Conference on Trade and Development), в 132 странах из 194 в той или иной форме введено в действие законодательство в отношении неприкосновенности и защиты данных (UNCTAD, 2020 г. [10]). В то же время, степень защиты и соответствия требованиям по НЗД среди государств существенно разнится. Введение в действие Общего регламента защиты персональных данных (GDPR) ЕС не только гармонизирует нормы по НЗД в странах ЕС и Европейской экономической зоны, но и выступает для многих стран фактором ускорения процессов модернизации норм в отношении неприкосновенности личных данных.

60. В нижеприведенном блоке представлена информация о регламенте ЕС по защите данных.

Блок 6.3. Регламент ЕС по защите данных

Право на неприкосновенность и защиту данных закреплено Хартией Европейского Союза об основных правах (Charter of Fundamental Rights) (Статьи 7 и 8).

Общий регламент защиты персональных данных (GDPR) ЕС, вступивший в силу 25 мая 2018 г., определяет порядок обработки компаниями персональных данных физических лиц. GDPR, помимо всего прочего, требует от компаний минимизировать объем собираемых и обрабатываемых данных, т. е. осуществлять такую деятельность только в отношении информации, необходимой для конкретной указанной цели (принцип целевого ограничения), и не производить дальнейшую обработку тем или иным способом без соответствия указанным целям. Также положениями GDPR предписывается информирование физических лиц, в частности, о том, когда собираются их данные и с какой целью (в каких целях) они будут обработаны, а также установлен перечень законных оснований, позволяющих обрабатывать личные данные, и прав физических лиц, включая права на доступ к данным, их уточнение и удаление, а также право не подвергаться решению, которое основано исключительно на автоматизированной обработке, в том числе на профилировании.

Надзор за соблюдением GDPR в государствах-членах ЕС осуществляют органы по надзору за соблюдением законодательства о защите персональных данных (data protection authorities, DPA). Европейский совет по защите данных (European Data Protection Board, EDPB), в состав которого входят представители всех DPA и Европейская инспекция по защите данных (European Data Protection Supervisor, EDPS), контролирует системное применение положений GDPR во всех странах ЕС.

© FATF/OECD 2021

Передача личных данных третьим странам или международным организациям осуществляется при соблюдении особых условий, гарантирующих соблюдение норм GDPR. Основанием для такой передачи, в частности, может служить «решение о достаточности мер», принимаемое Европейской Комиссией, когда уровень защиты данных в третьих странах в существенной мере соответствует гарантированному в государствах ЕС.

Важно отметить положение GDPR о том, что принципы защиты данных не распространяются на обезличенные данные (а именно, на персональные данные, обезличенные вследствие того, что их субъект не поддается или более не поддается идентификации). Псевдонимизированные же данные (личные данные, которые более не соотносимы с конкретным субъектом без использования дополнительной информации) считаются персональными и подпадают под действие GDPR.

61. При том, что законодательство по НЗД в разных юрисдикциях может различаться, тенденция к сближению есть: например, внедрение концепций защиты данных со сходными ключевыми параметрами (такими как превалирование общего законодательства над секторальными нормами, базовый набор принципов и обязательств в отношении защиты данных, наделение физических лиц юридически закрепленными правами контролировать свои данные (уточнение и удаление), создание независимого надзорного органа с правоприменительными полномочиями). Кроме того, о положительных тенденциях в этом отношении свидетельствуют такие международные стандарты, как, например, Конвенция 108+ (единственный многосторонний юридически обязывающий документ в сфере защиты данных), Руководство ОЭСР по неприкосновенности личных данных (OECD Privacy Guidelines) и др. Организация Объединенных Наций разрабатывает рекомендованные законодательные положения, а также собрание полезных наработок в отношении норм по защите данных с целью содействия международному сотрудничеству в противодействии терроризму («Программа страновой группы ООН по защите данных»).

62. Но как отмечено в Руководстве ФАТФ по обмену информацией в сфере частного сектора (2017 г.), для ФУ в целях обработки данных клиентов (включая их передачу другим сторонам) для противодействия финансовым преступлениям может оказаться сложным или невозможным рассчитывать на согласие или исключения, касающиеся государственных интересов. К тому же необходимо соблюдать условия юридической правомерности такой международной передачи данных. Способствовать обмену информацией может четкое изложение юридических положений с соответствующими защитными мерами или рекомендациями, определяющими обстоятельства, при которых, где это возможно, данные клиентов могут передаваться между юрисдикциями в подобных целях. (ФАТФ, 2017 г. [8])

63. Тем не менее, даже при наличии действующей правовой системы, позволяющей передачу данных представителей частного сектора, предоставляемые ФУ данные могут быть неточными или неполными. Поэтому, хотя применение практики объединения данных и совместного анализа может в некоторых случаях способствовать поддержанию соответствия работы ФУ нормам в отношении ПОД/ФТ (например, по проведению НПК), те ФУ, которые будут такие данные использовать, сами должны обеспечивать их достоверность. Таким образом,

© FATF/OECD 2021

ФУ должны проверять качество полученных от других организаций данных, оценивая актуальность, адекватность и достаточность их компонентов, а также проведенных в отношении таких данных проверок с целью соблюдения своих обязательств по ПОД.

64. В некоторых юрисдикциях ФУ, как распорядители персональных данных, должны предоставлять физическим лицам доступ (по требованию) к информации, которую они собирают, передают и хранят[15]. Это делается для того, чтобы частные лица понимали, какие именно их данные есть в распоряжении ФУ, и могли по своему запросу вносить в них коррективы или удалить неправильную или необязательную информацию (право на исправление или удаление подобных данных при определенных условиях). Проблема может возникнуть, если те, в отношении кого есть подозрение в осуществлении противоправной деятельности или против которых ведется официальное расследование, требуют удаления разоблачительной информации. Однако законом могут быть предусмотрены определенные (надлежаще обоснованные) ограничения, относящиеся к случаям, когда реализация прав отдельного человека может повлиять на исполнение законных обязательств или когда есть риск создания угрозы для текущего расследования.

65. Другие сложности есть в тех юрисдикциях, где разрешается передача обезличенных персональных данных. Некоторые респонденты в своих ответах отмечали наличие двусмысленности в том, что касается возможности обмена между учреждениями обезличенными данными, поскольку требования в отношении обезличенности[16] и псевдоанонимности[17] представляются нечеткими или различаются в зависимости от юрисдикции.

66. Кроме того, на процесс обмена данными представителями частного сектора экономики (с выходом информации за пределы определенной финансовой группы) могут влиять правила их международной передачи. Во многих случаях государственные органы или частные организации не могут передавать данные за пределы своей юрисдикции без равноценной их защиты в юрисдикции получателя или без соответствующих гарантий безопасности. К тому же законы в отношении размещения данных, как правило, могут содержать два основных требования: 1) чтобы личные данные граждан хранились в дата-центрах, расположенных на территории той или иной страны или группы стран; 2) чтобы управление данными и их обработка осуществлялись внутри той же страны. Это также налагает ограничения на передачу информации из-за норм действующих в юрисдикциях правовых систем, в результате чего ФУ может быть запрещено обмениваться определенными данными, связанными с предполагаемыми финансовыми преступлениями, со своими коллегами из ФУ других государств, включая входящих в ту же финансовую группу, либо же они могут быть не защищены от ответственности за это, в противоположность ситуации в их собственной юрисдикции[18].

---

[15] Например, см. Статью 9 Конвенции 108+.

[16] Обезличенные данные представляют собой информацию, не относящуюся к идентифицируемому физическому лицу, или информацию в отношении субъекта, который более не является идентифицируемым (и отсутствует возможность его повторной идентификации). (Управление Комиссара по информации, ICO, «Что такое персональные данные?» (What is Personal Data?), декабрь 2020 г., ico.org.uk.)

[17] Псевдоанонимность представляет собой меру безопасности, в соответствии с которой из блока данных удаляется информация, позволяющая идентифицировать физическое лицо, либо производится замещение такой информации. Такие данные при этом считаются персональными, поскольку их субъект может быть снова идентифицирован (например, при наличии ключа шифрования). (Там же.).

[18] Для получения дополнительной информации см. IIF (Институт международных финансов, ИМФ), 2019 г. [17]

© FATF/OECD 2021

67. И в завершение, в качестве препятствия более широкому распространению новых технологий для целей объединения данных и их совместного анализа респонденты отмечали недостаточное взаимодействие между внутригосударственными и международными институциями, занимающимися ПОД/ФТ и НЗД. Такой недостаток согласованности действий и сотрудничества может препятствовать исполнению Рекомендации 2 ФАТФ в отношении сотрудничества и (где это целесообразно) согласованности между соответствующими органами, осуществляющими деятельность по ПОД/ФТ, в целях обеспечения совместимости требований системы ПОД/ФТ и норм НЗД.

6.2. Качество данных

68. Стандарты и форматы данных существенно разнятся в зависимости от институции, юрисдикции, инфраструктуры и сетей передачи сообщений. Вследствие подобных различий может понадобиться проведение анализа данных, ими могут быть обусловлены задержки банковских процессов и рост затрат на поддержание соответствия стандартам. Низкое качество данных (в т. ч. недостоверность или неактуальность) может свести на нет все преимущества процессов их объединения и совместного анализа, поскольку может привести к получению ошибочных аналитических результатов. Применение автоматизированных и передовых аналитических инструментов, в частности, зависит от того, насколько стандартизированы входные данные.

69. Согласно результатам опроса, качество данных представляет основную проблему для более широкого применения методов углубленного анализа в отношении централизованных и децентрализованных блоков данных. Респонденты особо отмечали низкое качество данных отдельных ФУ, наблюдаются и несовместимость стандартов данных между различными учреждениями. Качество данных остается главным препятствием в том, что касается создания нужных массивов данных корректного и совместимого формата с целью предотвращения необъективных выводов, что может в худшем случае привести к финансовым потерям. Все это еще более усложняется при применении шифрования, т. к. становится труднее выявлять ошибки в данных, что может в свою очередь привести к ошибкам в результатах.

6.3. Недостаточная четкость законодательного регулирования

70. Рядом респондентов отмечалось, что недостаток четко сформулированных регуляторных требований и соответствующих руководств по применению новых технологий представляет проблему для процессов объединения данных представителей частного сектора и применения совместного анализа. Рядом юрисдикций осуществляются попытки прояснить эти моменты или адаптировать свои правила, чтобы ФУ могли обмениваться данными и производить их совместный анализ, а в некоторых действуют партнерские отношения между подразделениями финансовой разведки. Некоторые респонденты отмечали, что отсутствие методологических ориентиров и определенности со стороны регулятора не способствует скорейшему инвестированию в дорогостоящие новые технологии и их применению — что могло бы содействовать в проведении совместного анализа данных.

71. Один респондент также отметил, что существующая правовая система при ее создании не подразумевала возможности использования новых технологий повышения конфиденциальности, и поэтому в ней нет четкого описания границ применения таких технологий.

© FATF/OECD 2021

72. И наконец многие отметили, что существующие национальные нормативы полностью исключают обмен частными данными (кроме случаев такого обмена внутри финансовой группы).

6.4. Объяснимость и интерпретация

73. В январе 2020 г. Европейской службой банковского надзора (European Banking Authority, EBA) был выпущен документ, регламентирующий использование в европейской банковской системе больших массивов данных и углубленных методов анализа. В нем говорится, что европейские ФУ находятся на начальной стадии использования углубленного анализа, при котором применяются простые модели машинного обучения и приоритизируется принцип объяснимости и интерпретации. Одной из проблем, связанных с применением более сложных аналитических моделей, является их объяснимость и интерпретация для регулятора, а также возможность получения необъективных и непредусмотренных результатов. Согласно EBA, модель является объяснимой, когда ее внутреннее поведение может быть полностью понятно для человека (объяснимость) или когда в отношении основных факторов, приведших к получению результата, могут быть предоставлены объяснения (обоснования). (EBA, 2020 г. [11]) При отсутствии подобного понимания технология может восприниматься регулятором как «черный ящик», что может повлиять на ее применение, т. к. регулятор не может должным образом осуществлять проверки, оценку рисков, адекватно управлять и минимизировать все выявленные риски, связанные с применением такой технологии. Это особенно касается случаев, когда решение принимается при высоком уровне автоматизации и непосредственно влияет на клиентов. Для решения таких проблем регуляторы могут работать с соответствующими техническими специалистами и др., как частного, так и госсектора, для оценки и содействия внедрению соответствующих практик в том, что касается объяснения, документирования и управления методами углубленного анализа в контексте ПОД/ФТ[19]. Подобная работа может вестись в направлении выявления необходимости и способов применения требований к объяснимости согласно риск-ориентированному подходу — например, применение более жестких требований к объяснимости при возрастании потенциального воздействия модели на бесперебойность функционирования бизнеса и (или) вреда для клиентов.

74. Некоторые респонденты отмечали, что во внедрении новых технологий обмена данных и анализа в сфере ПОД/ФТ ФУ останавливает то, что регулятор ожидает полной ясности в отношении моделей шифрования и машинного обучения. Это особенно сложнодостижимо, если технологии разрабатывались третьей стороной, которой и принадлежат права собственности на технические спецификации, или для ФУ, испытывающих дефицит технически грамотных в области новейших систем шифрования и аналитики кадров. Один из респондентов обозначил видение регулятором алгоритмических моделей в том ключе, что они должны разрабатываться с возможностью воспроизводства того же результата при условии введения тех же первоначальных данных, что не всегда возможно для систем машинного обучения.

[19] См. запрос федеральных банковских агентств США в отношении информации и рекомендаций по использованию финучреждениями искусственного интеллекта, включая системы машинного обучения (Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning) www.federalregister.gov/documents/2021/03/31/2021-06607/request-for-information- and-comment-on-financial-institutions-use-of-artificial-intelligence. Также см. документ на эту тему центра FinReglabs и Стэнфордского университета (после запроса информации федеральными банковскими агентствами США), целью которого было дать оценку новым практикам по объяснению, документированию и управлению моделями машинного обучения для целей предоставления кредитования: https://finreglab.org/ai-machine-learning/explainability-and-fairness-of-machine-learning-in-credit-underwriting/

© FATF/OECD 2021

75. Респондентами был отмечен важный момент: необходимость проверки результатов углубленного анализа (ИИ, машинное обучение) человеком в целях обеспечения их достоверности и постоянного совершенствования алгоритмов. Хорошим выходом был назван смешанный подход, при котором человек проверяет более сложную аналитику, а базовые рутинные задачи могут выполняться простыми моделями. Однако были также высказаны опасения, что иногда углубленные системы анализа могут применяться ФУ без глубокого понимания принципов функционирования и целей применения конкретной технологии, что может привести к получению непроверенных и ненадежных результатов. Также руководители работ по ПОД/ФТ должны сами понимать или работать с командой тех, кто понимает работу моделей углубленного анализа с тем, чтобы проверять, как ФУ разрабатывали и оценивали правильность работы своих моделей.

76. Наконец, респонденты отмечали важность понимания поднадзорной организацией (и это должно быть очевидно как их вышестоящему органу, так и им самим) того, что любая новая технология дает лучшие результаты, чем прежняя система, особенно в тех областях, где может быть неочевидно, повышает ли данная технология эффективность работы по ПОД/ФТ.

6.5. Конфиденциальность СПО и предотвращение утечки данных

77. Правила в отношении конфиденциальности СПО могут препятствовать обмену ими (или уведомлению о самом факте подачи СПО либо предоставлению содержащейся в СПО информации). Конфиденциальность СПО очень важна для эффективного функционирования системы отчетности, а также для гарантий нераспространения информации о субъекте СПО и третьих лицах, поскольку это может отрицательно повлиять на сбор информации и на сам ход расследования, а также может дать возможность скрыться вместе с активами либо же избавиться от них. Соблюдение конфиденциальности дает защиту репутации субъекта СПО и защищает человека, формирующего это СПО, а ее нарушение может подорвать работу всей системы СПО. Несанкционированное раскрытие данных СПО может привести во многих юрисдикциях к уголовной ответственности для ФУ. Все это лежит в основе установления необходимых ограничений в отношении обмена данными СПО. (ФАТФ, 2017 г. [8])

78. Вопрос конфиденциальности СПО становится еще сложнее, когда дело касается обмена информацией с другими государствами, где правовые системы отличны. Сложности, например, могут состоять в наличии в национальном законодательстве положений в отношении открытости и фиксации доступных данных при судебных разбирательствах. В некоторых странах приняты нормы, по которым требуется уведомление регулятора о судебных запросах и повестках, касающихся внутригосударственных СПО, — и регулятор может действовать в направлении обеспечения конфиденциальности СПО в ходе судопроизводства, — однако эти нормы не могут быть защитой в случае подачи СПО из иностранного государства в иностранное ПФР.

79. При том, что вопрос конфиденциальности СПО может создавать определенные трудности при обмене данными между представителями частного сектора, важно не допускать утечек информации. Защитить данные без потерь для эффективности работы по ПОД/ФТ можно при помощи альтернативных правовых и технологических механизмов, обеспечивающих анонимность или шифрование персональных данных.

© FATF/OECD 2021

6.6. Структура рынка и конкуренция

80. Широкое применение методов сбора и анализа данных не является новшеством, но сегодня технологические инновации позволяют хранить существенные объемы информации и мгновенно ее анализировать. Чем больше, например, объем данных, тем выше вероятность более высокой точности результатов ее анализа. Сейчас только крупные ФУ располагают столь обширными массивами данных, чтобы эффективно применять методы углубленного анализа, поэтому нужно распространять сведения о межинституциональной обработке данных, чтобы небольшие и средние ФУ тоже могли применять новые технологии. Это также дает возможность всем пользоваться экономическими выгодами, возникающими в результате такого применения.

81. Как отметили многие респонденты, циркулирование больших блоков обрабатываемой клиентской информации между ФУ потенциально может вызвать проблемы, связанные с конкуренцией. Результатом может стать выборочный обмен данными лишь с участниками небольших групп «доверенных лиц» и, как следствие, — неравномерный обмен информации по системе. Таким образом, может наблюдаться переход рисков ОД/ФТ от ФУ, располагающих механизмами обмена информацией, к тем, кто их не имеет. Ненадежные участники, исключенные из своей группы первого типа, могут затем тяготеть ко вторым, чтобы уменьшить вероятность выявления, поэтому ФУ или секторы, не располагающие механизмами обмена информацией, могут столкнуться с дополнительными рисками ОД/ФТ, и в связи с этим может понадобиться рассмотрение дополнительных способов снижения этих рисков.

82. ФУ также могут быть не расположены делиться коммерчески важной информацией, которая может исказить конкуренцию на рынке. Разные возможности ФУ в том, что касается сферы ИТ, тоже могут быть препятствием для эффективного обмена информацией, поскольку различные или несовершенные системы ИТ, а также разные форматы данных исключают возможность объединения и совместного анализа. Подобным образом, в неблагоприятном положении могут оказаться организации, пользующиеся инфраструктурой и системами ИТ прежних поколений, что, получается, приведет к их исключению из системы обмена данными.

83. Доступ к данным (и обмен ими) со стороны ограниченного числа ФУ не должен приводить к тому, чтобы они имели несправедливые преимущества, ведь конкурентоспособность на рынке финансовых услуг все более обуславливается возможностью доступа к большим массивам актуальных (в режиме реального времени) данных. Поэтому при оценке возможностей обмена данными в сфере ПОД/ФТ могут возникать соображения, направленные в сторону законодательства о защите конкуренции, обеспечивая одинаковые условия для всех участников рынка и исключая возможности для вытеснения потенциальных конкурентов. Так, при гарантированном доступе к данным он должен предоставляться на справедливых, разумных и равных для всех условиях, а также способом, исключающим тайные договоренности и не способствующим их формированию. Также обмен данными должен быть ограничен лишь критически необходимым их объемом.

© FATF/OECD 2021

6.7. Технологические затраты и ограничения

84. Рядом респондентов было отмечено, что на возможность более широкого применения технологий повышения конфиденциальности, а также методов углубленного анализа, в частности, влияют существенные затраты на первоначальном этапе. И если крупные ФУ могут располагать ресурсами для их вложения в подобные технологии или приобретения лицензий для доступа к продуктам сторонних разработчиков, многие небольшие и средние компании все еще откладывают обновление используемых ими технологий прежних поколений. Результатом этого может стать сокращение банка данных, т. к. туда будут попадать только данные тех организаций, которые могут себе позволить первоначальные затраты на запуск таких технологий.

85. В качестве дорогостоящих для внедрения и поддержания их работы респондентами также были названы методы углубленного анализа, такие как машинное обучение. Еще более осложняет ситуацию необходимость интегрирования новой аналитики в существующие системы, что влечет за собой дополнительные затраты на модернизацию. Барьером с точки зрения чрезмерной стоимости было названо и пробное использование новых углубленных методов анализа одновременно с эксплуатацией имеющихся систем. Дополнительные расходы в этом контексте связаны и с необходимостью содержать технических специалистов, имеющих достаточный профессиональный опыт в этих технологиях, для разработки комплексных моделей и усовершенствования их со временем.

86. Еще одной технологической проблемой с точки зрения объединения и анализа больших объемов данных является необходимость располагать существенными вычислительными мощностями для работы алгоритмов. Величина массивов данных может значительно влиять на стоимость вычислительных процессов.

87. Объединение и обмен данными в сфере ПОД/ФТ может подразумевать, например, передачу больших их массивов, включая информацию о транзакциях и клиентах. Такие крупные блоки данных много «весят» и их сложно передавать (это еще называют «гравитацией данных»). Поэтому при разработке вариантов объединения данных важно учитывать этот момент, а также потенциальные возможности роста показателя гравитации данных при их централизации.

88. И еще одной сложностью в плане внедрения углубленного анализа (машинного обучения) в контексте ПОД/ФТ является необходимость проверки корректности данных или подтверждения того, что поведение того или иного лица действительно носит признаки преступного. Валидация модели может быть особо затруднена, когда речь идет об ОД/ФТ, ведь расследование может вестись годами. Во многих случаях ФУ не получают информацию о конечных результатах по направленным ими в ПФР СПО, как и о том, выносились ли обвинения в ОД или ФТ в отношении действий, по которым формировались СПО.

6.8. Упредительные сообщения и снижение рисков

89. Как правило, совместный анализ данных в деятельности по ПОД/ФТ применяется для идентификации преступного поведения в рамках группы ФУ. При эффективном использовании технологий повышения конфиденциальности, например, можно обойти требования в отно-

© FATF/OECD 2021

шении размещения данных и конфиденциальности СПО и узнать, не направляли ли другие организации СПО в отношении их клиента, — но без получения связанных с этим сведений закрытого характера. Однако тут кроется вероятность искажения ситуации путем направления избыточных упредительных СПО. Если слишком полагаться на систему обмена подозрительной информацией, можно столкнуться с ситуацией, когда ФУ сочтет клиента сомнительным только лишь на основании информации третьей стороны, а она может быть неточной или же мотивы возникновения подозрений могут быть полностью опровергнуты подразделением финансовой разведки. Это может повлечь отказ (непредвиденный и неэтичный в данном случае) добросовестному клиенту в доступе к финансовой системе, или же в отношении операций клиента могут производиться дальнейшие выяснения их характера и целей, с задержками в исполнении банковских операций.

90. Кроме того, само по себе наличие подозрения не значит, что другие организации, получив такую информацию, обязательно будут направлять свои соответствующие СПО. Это может служить важным элементом анализа рисков и привести к расширенным мерам НПК. Таким образом, широкое внедрение практики совместного анализа и объединения данных может привести к росту количества подозрений (особенно при наличии упредительных сообщений) и может привести к существенному росту применения расширенных мер НПК, а как следствие этого — к росту затрат на соблюдение нормативов. Все это может препятствовать применению подобных технологий или стать причиной принятия мер по снижению рисков.

6.9. Безопасность

91. С внедрением новых технологий для объединения и обработки данных проявляются новые существенные уязвимости, а также новые возможности для киберпреступников, связанные с обнаружением и использованием недостатков системы безопасности. Например, при применении технологий, формирующих централизованный массив данных, возникают серьезные уязвимости в системе кибербезопасности, а также проблемные моменты с безопасностью на государственном уровне. Появляются и важные процедурные соображения касательно того, кто в конечном итоге должен следить за безопасностью данных в таких хранилищах, и кто будет ответственен за нарушения работы системы или в случаях кибератак. Объединение больших объемов данных создает также возможности катастрофически крупных утечек всего лишь из одного источника. Соответственно, с ростом масштабов объединения данных и обмена ими возрастает и важность защиты от внутрисистемных угроз.

92. Определенная защита есть благодаря прогрессу в применении методов совместного анализа с использованием технологий псевдонимизирования, при условии отдельного хранения персонифицирующих сведений и соблюдения технических и организационных мер по недопущению связывания личных данных и какого-либо конкретного или идентифицируемого физического лица. Тем не менее, несмотря на успехи псевдонимизирующих технологий, законодательство по защите данных действует, и следует все еще учитывать риск повторной идентификации (отслеживания данных). В этих целях нужно оценить необходимый объем работ, время, ресурсы в соответствии с характером данных, сферой их использования, существующими технологиями повторной идентификации и связанными с этим издержками. При внедрении методов совместного анализа с использованием псевдонимизирующих технологий также необходим строгий надзор со стороны органов, занимающихся вопросами НЗД.

© FATF/OECD 2021

6.10. Устранение субъективности в аналитике при использовании искусственного интеллекта

93. В отношении применения аналитической обработки данных (ИИ) для объединения информации, важнейшим соображением является то, что использование любого углубленного метода анализа исключает субъективность и роль человеческого фактора, и, таким образом, предотвращает дискриминацию (религиозную, расовую, гендерную, по возрасту, сексуальной ориентации, национальности и т. д.). Смещение объективности может быть привнесенным в систему фактором посредством введения или исключения определенных данных либо при программировании алгоритмической модели[20]. Обязательным при разработке и обучении этим методам является использование непредвзятых данных и создание алгоритмов, не поддерживающих свойственную человеку пристрастность и дискриминационные мотивы.

6.11. Права человека

94. В целях получения коммерческой выгоды частные предприятия могут осуществлять профилирование частных лиц. В конечном итоге это может привести к дискриминации (расовой, гендерной политической, религиозной). Поэтому со стороны надзорных и контролирующих вопросы НЗД органов необходимы требования полной прозрачности, строгого мониторинга и (или) контроля в отношении всех инструментов, применяемых для объединения данных и их совместного анализа. Это касается и инструментов с использованием технологий псевдонимизирования, поскольку при их применении есть возможность отслеживания данных из массивов и выведения персональных данных с идентификацией личности.

[20] Для более подробной информации по этическим вопросам, связанным с ИИ, см. (FSB, 2017 г. [15]), Приложение B.

© FATF/OECD 2021

7. Возможности более широкого применения технологии объединения данных и углубленных методов анализа

95. Среди ответов респондентов в качестве варианта достижения более широкого применения новых технологий объединения данных и совместного анализа, а также решения некоторых из вышеупомянутых проблем, наиболее часто называлось повышение уровня регуляторной стабильности в отношении их применения. В приведенном ниже разделе обобщены различные решения, определенные респондентами и участниками частного сектора, которые могут способствовать более широкому использованию новых технологий для обмена и анализа данных между частными лицами. Эти решения дают старт диалогу между ФАТФ, частным сектором и органами, обеспечивающими НЗД, а также перспективным проектам ФАТФ. Эти факторы создания соответствующей среды более широкого применения систем объединения данных и их совместного анализа по состоянию на настоящее время не подтверждены ФАТФ.

7.1. К вопросу о ясности позиции регуляторных органов

96. Респонденты отмечали растущую необходимость разработки системы данных, включающей все сферы, связанные с обменом или объединением данных частным сектором, включая данные по ПОД/ФТ. Достичь этого респонденты предлагали путем более интенсивного сотрудничества между органами ПОД/ФТ (включая регуляторов) и НЗД. Это может способствовать появлению среды, благоприятствующей сокращению уровня нерасположенности к риску со стороны субъектов экономики вследствие наблюдающегося в настоящий момент недостатка четких руководств. Большая часть отвечавших также акцентировала внимание на необходимости адекватных разъяснений со стороны национальных финансовых регуляторов относительно видов данных, которыми могут обмениваться ФУ, а также относительно того, обеспечивают ли организациям те или иные технологии (например, гомоморфное шифрование и др.) и процессы их дальнейшее соответствие требованиям в отношении неприкосновенности данных (на национальном и наднациональном уровне) и более узким нормативам для предприятий финансового сектора. Это может дать финучреждениям уверенность, необходимую для того, чтобы инвестировать в технологии, обучение, кадровый потенциал и производственное развертывание решений в области обмена данными. Аналогично, ряд респондентов высказались за обобщение и опубликование содержательных материалов с вариантами использования новых технологий (из практики применения) с конкретикой в разрезе отдельных новых технологий по разрешению вопросов, связанных с неприкосновенностью данных при их обмене субъектами частного сектора экономики.

97. Отмечали респонденты и необходимость правовых положений на национальном уровне в отношении «безопасных гаваней», позволяющих добровольный обмен данными между ФУ для определенных целей по ПОД/ФТ на основе принципов необходимости и соразмерности.

98. В отношении требований по недопущению утечек информации по СПО рядом респондентов отмечалась необходимость внесения изменений в регуляторных требованиях в отношении СПО, позволяющих ФУ более свободно обмениваться сведениями о том, направлялось ли СПО по конкретному лицу или по данным [по факту].

© FATF/OECD 2021

7.2. Способствование созданию благоприятных условий

99. Многие участники опроса также ожидали бы от контролирующих органов в сфере ПОД/ФТ создания дополнительных экспериментальных программ, правовых режимов, центров инноваций для тестирования новых технологий анализа и обмена данными в условиях отсутствия карательных или излишне жестких мер принуждения со стороны надзорных органов на стадии внедрения ФУ той или иной технологии. Это способствовало бы росту инноваций в этой сфере, поскольку ФУ не сталкивались бы с негативом даже в случаях неудачного, в конечном итоге, запуска экспериментальной программы. Успех подобных инициатив также зависит от уровня вовлеченности и взаимодействия национальных органов, контролирующих соблюдение требований по НЗД. Достаточная степень их участия может способствовать согласованности работы, совместному обучению и лучшему пониманию сложных моментов, связанных с управлением моделями, технологиями моделирования, способами воздействия через анализ данных на конкретные риски ОД/ФТ и вариантами интенсификации обмена данными при соблюдении требований по НЗД.

100. ФАТФ также были разработаны *«Рекомендации, направленные на поддержку применения технологий в сфере ПОД/ФТ» (Suggested Actions to Support the Use of Technology in AML/CFT)* (см. Приложение С), продвигающие сформулированный на форуме в Сан-Хосе (2017 г.) принцип *развития позитивных и ответственных инноваций.* В этом документе говорится, что новые технологии в сфере ПОД/ФТ должны разрабатываться и внедряться с учетом как существующих угроз, так и возможностей, а также при обеспечении того, что их применение не противоречит международным стандартам в отношении неприкосновенности и защиты данных, а также правилам кибербезопасности.

7.3. Стандартизация данных и управление данными

101. С целью улучшения качества данных некоторые респонденты выступали за стандартизирование форматов их сбора, а также за стимулирование использования открытых API, чтобы можно было обмениваться данными между ФУ. На местах, в юрисдикциях, можно было бы, используя регуляторные механизмы в качестве инструментов обратной связи, информировать ФУ о требованиях к качеству данных, а также вводить в действие соответствующие меры по его повышению до приемлемого уровня.

102. Что касается управления данными, респонденты особо отмечали необходимость введения в действие ФУ соответствующих принципов, структур и систем контроля в целях обеспечения:

    a. качества данных, включая их полноту, указание на то, насколько недавно они были собраны или обновлены, структурированы ли в подходящей для компьютерной обработки форме, возможно ли влияние источника данных на их интерпретирование или надежность; сюда же входят средства оценки достоверности данных; и

    b. фиксации источника их происхождения, включая ведение контрольного журнала («аудиторского следа») в отношении данных.

103. Применение методов цифровой идентификации личности также указывалось среди возможных вариантов решения проблем с качеством данных. Это могло бы стать и стандартным инструментом, позволяющим третьей стороне полагаться на результаты иден-

© FATF/OECD 2021

тификации, способствуя тем самым более активному обмену данными. Аналогично, правоохранительные органы могли бы служить источником документации для НПК в отношении юридических лиц. Участие правоохранительных органов гарантировало бы соответствие каждому юридическому лицу своего уникального идентификатора и избавило бы от необходимости проверки соответствия названий.

104. И наконец, в качестве образца назывался в ходе опроса «Единый стандарт по обмену информацией» (Common Reporting Standard, CRS). Документ предписывает юрисдикциям получать от своих ФУ определенную информацию и автоматически делиться ею с другими юрисдикциями (на ежегодной основе) в целях противодействия уклонению от уплаты налогов. (ОЭСР, без даты [12]) Ответившие таким образом респонденты считают, что применение такой модели может стимулировать обсуждение вопроса качества данных для обмена ими в целях ПОД/ФТ, поскольку содержит особые требования по стандартизации данных (специфицирование информации, подлежащей сбору и обмену).

7.4. Принцип непредвзятости при использовании искусственного интеллекта

105. В том, что касается предотвращения влияния человеческого фактора и дискриминации при использовании ИИ, респонденты подчеркивали важность систематических проверок законности и надежности источников данных, расширенного тестирования моделей и постоянного их мониторинга. Например, в отношении блока данных по тем или иным лицам может понадобиться внесение дополнительного тренировочного их набора для повышения точности и объективности результатов.

106. Кроме того, в «Основных положениях ОЭСР в отношении ИИ» (Principles on AI), принятых членами этой организации в мае 2019 г., говорится, что системы ИИ должны создаваться таким образом, чтобы соблюдался принцип верховенства права, права человека, с уважением к демократическим ценностям и этнокультурному многообразию, и что они должны содержать соответствующие предохранительные возможности (например, позволяющие вмешательство человека при необходимости) в целях обеспечения существования достойного и справедливого общества. Системы ИИ также должны полноценно, безопасно и надежно функционировать в течение всего срока своего существования, при этом должна производиться постоянная оценка рисков и управление ими. Поэтому первоочередной необходимостью является полное понимание принципов использования прогнозных моделей в регуляторном контексте уже на начальных стадиях работ в этом направлении, поскольку ответственность за надлежащее функционирование систем ИИ будет лежать на учреждениях и лицах, осуществлявших их разработку, внедрение и эксплуатацию. (ОЭСР, 2019 г. [13])

© FATF/OECD 2021

8. Заключительные положения

107. Высказанные соображения по ситуации с обменом частными данными в сфере ПОД/ФТ для ФАТФ не новы. Но имеющиеся и активно разрабатывающиеся технологические новшества могут предоставить новые возможности обмена и анализа данных для более успешного и эффективного обнаружения потенциально подозрительной активности и исполнения обязательств по ПОД/ФТ. Новые технологии также могут предоставить решения по улучшению защиты персональных данных с целью обеспечения соблюдения национальных и международных правовых норм по НЗД при обмене и обработке информации. Тем не менее, перед внедрением необходимо должным образом оценить соответствие указанных разработок требованиям в отношении защиты данных в той или иной юрисдикции — с тем, чтобы не осложнять защиту фундаментальных прав и свобод. В некоторых юрисдикциях, к примеру, подобные инициативы в настоящее время могут не быть законодательно допустимыми.

108. В настоящем документе определены существующие и находящиеся в активной разработке технологии, облегчающие объединение данных и их совместный анализ ФУ, а также рассмотрены политические соображения, правовые проблемы и возможные решения, по которым высказались респонденты. Действительно, работа в направлении использования методов объединения и совместного анализа данных дает почву для целого ряда соображений по вопросам процедурного характера. Важно, например, чтобы при реализации методов объединения данных и совместного анализа в равной степени оценивались и минимизировались любые риски, связанные с несклонностью к рискам, а также с отказом добросовестному клиенту в доступе к финансовой системе до исполнения подобных мер. ФАТФ будет учитывать изложенное в данном документе при ведении дальнейшего диалога с контролирующими исполнение требований по ПОД/ФТ и НЗД органами, с разработчиками технологий, с ФУ, а также с другими профильными экспертами для обеспечения возможности полноценного применения и соответствия национальным и международным правовым нормам в сфере НЗД новых технологий, которые могут способствовать повышению эффективности деятельности по ПОД/ФТ.

© FATF/OECD 2021

Приложение A. Глоссарий

- **Advanced Analytics — Углубленные методы анализа.** Под углубленными методами анализа понимается изучение данных или содержимого автоматическими или полуавтоматическими системами с использованием развитых технологий и цифровых средств, возможности которых, как правило, превышают таковые традиционных систем бизнес-аналитики, с целью получения глубоких выводов, прогнозирования, формулирования рекомендаций. Технологии углубленного анализа включают интеллектуальный анализ данных/текстов, средства машинного обучения, сопоставление с шаблоном, прогнозирование, визуализацию, семантический анализ, анализ эмоциональной окраски, сетевой и кластерный анализ, многомерную статистику, анализ графов, моделирование, способы обработки сложных событий, нейронные сети. При применении углубленных методов анализа обычно используются большие массивы данных (big data).

- **Application — Приложение.** Компьютерное программное обеспечение, разработанное под конкретные задачи пользователя.

- **Application Programming Interface (API) — Интерфейс прикладного программирования.** API представляет собой набор определений и протоколов для создания и интегрирования программных приложений. API позволяет одним цифровым продуктам и сервисам взаимодействовать с другими.

- **Algorithm — Алгоритм.** Компьютерный алгоритм представляет собой набор пошаговых инструкций для выполнения определенной задачи.

- **Artificial intelligence (AI) — Искусственный интеллект (ИИ).** ИИ является автоматической системой, способной в определенных заданных человеком целях давать прогнозы и рекомендации, принимать решения, влияющие на реальную или виртуальную среду (действуя с разной степенью автономности). (ОЭСР, 2020 г. [14]) Цель ИИ состоит в компьютерной автоматизации некоторых аспектов анализа, потенциально высвобождая при этом усилия человека для выполнения более тонких задач, а также в получении выводов, к которым человек мог и не прийти. В основе ИИ лежат многокомпонентные технологии с многочисленными приложениями. Не существует единого мнения по поводу того, в чем состоит «мышление» и «интеллект», или что есть «полностью автоматически». Есть ряд категорий ИИ, но в целом, в различной степени, системы ИИ создают «умные машины», сочетающие преднамеренность, интеллектуальность и адаптивность. В настоящее время системы машинного обучения являются наиболее известной и развитой формой ИИ.

- **Big data — Большие массивы данных («большие данные»).** Советом по финансовой стабильности (Financial Stability Board) дано такое определение понятия «больших данных»: «огромные объемы данных, генерируемые вследствие все возрастающего использования цифровых инструментов и информационных систем», таких как данные о финансовых транзакциях, информация социальных сетей, машинные данные (например, вычислительная сеть «интернет вещей» (Internet of Things), данные компьютеров и мобильных телефонов). (FSB, 2017 г. [15])

- **Black Box — «Черный ящик».** Понятие «черный ящик» относится к технологиям ИИ/машинного обучения и др., которые не являются прозрачными и интуитивно понятными че-

© FATF/OECD 2021

ловеку, не предоставляют надлежащую информацию в отношении принятия ими решений и получения расчетных данных/результатов, т. е. в отношении технологий «черного ящика» есть недостаток объяснимости.

- **Benchmarking — Сопоставительный анализ.** Сопоставительный анализ — это подход к определению реальных и относительных возможностей процессов, продуктов или сервисов, основанных на определенных технологиях, а также к выявлению проблем, связанных с эффективностью работы, путем тестирования в сравнении с наилучшими достигнутыми показателями в отношении определенной функции, задачи или цели (внутри той или иной организации, по отрасли в целом или в другой отрасли), с применением предельных рабочих характеристик, рассчитанных по специфическим сравнительным критериям. Метод сопоставительного анализа может применяться для измерения (сравнения) показателей функционирования новой технологии в сравнении с показателями системы, применявшейся до того, либо с показателями других новых технологий.

- **Collaborative Analytics — Совместный анализ.** Для осуществления совместного анализа данные не перемещаются и не централизуются, чтобы проанализировать их вместе с другими данными. Наоборот, аналитический инструментарий «приходит» к данным для их анализа. Это облегчает обеспечение безопасности данных и контроль над получением доступа к ним (кто, с какой целью и к каким данным имеет доступ).

- **Cybersecurity — Кибербезопасность.** Кибербезопасность является более широким термином, чем «безопасность данных», и относится к комплексному процессу защиты данных и систем перемещения, хранения и аутентификации указанных данных.

- **Data pool/pooling — Объединение данных.** Это процесс объединения цифровых данных из разных источников с получением более полного и полезного набора данных для анализа (в т. ч. любым количеством обращающихся). Такие комплекты данных централизуются.

- **Data security — Безопасность данных.** Это определение относится к процессу защиты данных от несанкционированного доступа и от искажения информации в течение всего времени ее существования. Включает методы защиты данных во всех приложениях и платформах: шифрование данных, хеширование, токенизация, управление ключами. Безопасность данных — более узкое понятие, чем «кибербезопасность».

- **Data standardization — Стандартизация данных.** Стандартизация данных представляет собой приведение к единому формату для того, чтобы пользователи могли их обрабатывать и анализировать. Этот процесс очень важен для возможности обработки больших массивов данных, применения методов углубленного анализа, разработки и применения других новейших цифровых инструментов и методик. Например, в разных организациях формат представления финансовых данных может разниться. При помощи процесса стандартизации данных они приводятся в общую форму, что позволяет применять передовые методы крупномасштабного анализа.

- **Digital Identity (ID) Systems/solutions — Системы/решения цифровой идентификации (ЦИ).** Системы/решения ЦИ — это системы (продукты/сервисы) идентификации, осуществляющие процесс идентификации/верифицирования лиц (физических или юридических), связывая подтвержденную личность с цифровыми данными и используя цифровое подтверждение и потенциально другие факторы аутентификации для установления

© FATF/OECD 2021

(подтверждения) личности того или иного лица (т. е., что лицо, заявляющее о себе как таковое, именно этим лицом и является).

- **Distributed Ledger Technology (DLT) (a.k.a. blockchain) — Технология распределенного реестра («блокчейн»).** Понятие DLT технологий относится к типу технологического протокола, позволяющего одновременный доступ, валидацию и обновление неизменяемого цифрового реестра, распределенного на множество компьютеров (и, как правило, на множество организаций или локаций), т. е. создает распределенную цифровую базу данных.

- **Deep Learning (DL) — Глубокое обучение.** Технологии глубокого обучения — это передовой тип машинного обучения, при котором искусственные нейронные сети (алгоритмы, в основу работы которых положены принципы функционирования мозга человека) с множественными (глубинными) слоями обучаются на большом объеме данных в условиях высокой степени автономности. Алгоритмы DL многократно выполняют задание, раз за разом дорабатывая результат, что позволяет машинам решать сложные задачи без вмешательства человека.

- **Digitalisation — Цифровизация.** Распространение цифровых технологий. Цифровизация представляет собой применение цифровых технологий и данных для изменения бизнес-модели, воздействия на методы выполнения работ, изменение принципов взаимодействия компании и ее клиентов и создания новых возможностей получения дохода и генерирования дополнительной стоимости.

- **Digitisation — Оцифровка, перевод в цифровой формат.** Оцифровка — это перевод данных, информации, текста, изображений, звука или других форм аналогового представления данных в цифровой формат (бинарный код), который может обрабатываться компьютером.

- **Dynamic data — Динамические данные.** Понятие динамических данных относится к непрерывному, постоянно изменяющемуся цифровому потоку данных в режиме реального времени (в отличие от статических или постоянных данных, с течением времени остающихся большей частью неизменными).

- **Explainability — Объяснимость.** В контексте новых технологий понятие объяснимости означает, что технологические процессы, решения или системы могут быть объяснимыми (истолкованными), понятными, и по их действиям и решениям можно получить отчет. При соблюдении принципа объяснимости есть надлежащее понимание того, как система работает и как производит результат. Объяснимость является базовым условием доверительного и ответственного использования [технологий]. При использовании технологий объяснимого ИИ результат получается на основе прозрачных данных, переменных и точек принятия решений.

- **FinTech — Финтех, финансово-технологические решения.** Понятие «Финтех» в широком смысле применяется в отношении использования новых и находящихся на стадии разработки цифровых технологий в финансовом секторе для широкого спектра целей. Первоначально термин в основном применялся к технологическим инновациям в новых финансовых продуктах и услугах для клиентов (мобильные платежи, предоставление онлайн платформ, предлагающих более быстрое кредитование физических и юридических лиц, алгоритмические инструменты сбережений и инвестиций, платежи в виртуальной валюте, привлечение ресурсов (краудфандинг) и депозитов (дистанционный прием чеков,

© FATF/OECD 2021

мобильный банкинг). Сейчас Финтех также включает в себя использование новых и находящихся на стадии разработки технологий для автоматизированного выполнения функций промежуточных и служебных систем предприятий, таких как использование алгоритмов и больших массивов данных, ИИ и машинного обучения, а также связывает аналитику крупных расчетов в отношении, например, ценных бумаг, деривативов, крупномасштабного финансирования и платежей с действиями, направленными на соблюдение нормативных требований (см. определение «RegTech» ниже). Ожидается разработка и других способов применения.

- **Fuzzy logic — Нечеткая логика.** Одна из разновидностей ИИ, использующая открытый неопределенный спектр данных и обрабатывающая несколько значений с получением ряда промежуточных результатов между «ДА» и «НЕТ» (например, «определенно, да», «возможно, да», «неопределенно», «возможно, нет», «определенно, нет»). Системы на принципах нечеткой логики дают определенный результат при неопределенных, двусмысленных, искаженных, неточных (нечетких) вводных, имитируя процесс принятия решений человеком точнее, чем традиционная логика «да/нет». Применяется в аппаратных средствах, программных продуктах или комбинированно.

- **Internet of Things (IoT) — «Интернет вещей».** Это глобальная сеть всех подключенных к интернету приборов и машин, собирающих, отсылающих, обменивающихся данными и производящих над ними действия, используя встроенные датчики, процессоры и коммуникационное оборудование без вмешательства человека. IoT генерирует огромное количество данных в реальном времени, которые можно анализировать и использовать целевым образом, в т. ч. для получения бизнес-результатов (см. «big data»).

- **Interoperability — Операционная совместимость.** Под операционной совместимостью подразумевается способность различных информационно-технологических систем и программного обеспечения коммуницировать, обмениваться данными и беспрепятственно использовать информацию в реальном времени, при этом все участники имеют возможность работать во всех системах.

- **Machine Learning — Машинное обучение.** Одна из разновидностей ИИ, «обучающая» компьютерные системы учиться на данных, идентифицировать шаблоны и принимать решения при минимальном участии человека. Технологии машинного обучения включают формирование последовательности действий для решения задачи в автоматическом режиме посредством учета предыдущего опыта и с применением алгоритмов распознавания шаблонов при ограниченном участии человека или без него, т. е. это метод анализа данных, автоматизирующий построение аналитической модели.

- **Machine Readable Regulation — Машиночитаемое регулирование.** Замещает естественно-языковые юридические правила программным кодом, позволяя использовать искусственный интеллект для предоставления регуляторной отчетности.

- **Natural language processing (NLP) — Обработка естественного языка.** Ветвь ИИ, позволяющая компьютерам понимать, интерпретировать и оперировать естественным языком. NLP дает возможность людям говорить с машинами.

- **Privacy Enhancing Technologies — Технологии повышения конфиденциальности.** «Специализированные возможности шифрования, позволяющие производить расчеты по

© FATF/OECD 2021

базовым данным без обязательного их раскрытия владельцем данных. Эта же технология обеспечивает отсутствие доступа владельца данных к содержанию поисковых запросов, при этом запросы и их результаты остаются зашифрованными (либо не раскрываются) и доступны только формирователю запроса». (Maxwell, 2020 г. [16]) Таким образом, это понятие включает ряд технологий, использующих шифрование, применение которых целесообразно прежде всего для защиты неприкосновенности данных при их использовании.

- **Real-time analytics — Анализ в режиме реального времени.** Представляет собой процесс машинного обучения, при котором система обрабатывает и анализирует только что загруженные данные и сразу (практически в режиме реального времени) генерирует значимый результат (информацию, прогноз, решение).

- **Real-time data (RTD) — Данные в реальном времени.** Под RTD понимается информация, предоставляемая сразу после сбора, с обеспечением ее актуальности. Такие данные позволяют осуществлять анализ в режиме реального времени и могут быть динамическими или статическими (например, новый ввод, указывающий на конкретное месторасположение в конкретное время).

- **Regulatory Technology (RegTech) — Регулятивные технологии.** RegTech представляют собой подтип FinTech. Используют новые технологии для обеспечения более полного и эффективного (по сравнению с применяющимися) соответствия регуляторным требованиям.

- **Responsible Innovation — Ответственная инновация.** Инновации являются ответственными, если они подходят для целей и соответствуют нормативным требованиям, в т. ч. в сфере ПОД/ФТ, защиты интересов потребителей, кибербезопасности, защиты неприкосновенности личных данных.

- **Smart machines — «Умные машины».** Компьютерные аппаратно программные системы, использующие алгоритмы ИИ. «Умные машины» разрабатываются для принятия решений, часто при использовании данных в реальном времени. В отличие от пассивных машин, которые способны только на механические или предопределённые реакции, умные машины используют датчики, цифровые данные и возможности дистанционного ввода, комбинируют информацию из этих разных источников, мгновенно анализируют введенные данные и действуют на основании такого анализа. Умные машины имитируют работу человеческого интеллекта, используя передовые вычислительные процессы, для получения выводов на основе мгновенного анализа данных.

- **Static data — Статические данные.** Фиксированный набор данных, которые после их сбора остаются неизменными.

- **Supervised learning — Контролируемое обучение.** Процесс машинного обучения, обучающий алгоритмы при помощи прогнозных моделей с введением в алгоритм заданных результатов, т. е. происходит обучение алгоритмов на примерах. Пара входных и выходных данных (размеченные данные) дает алгоритму обратную связь, на основании которой (тренировочного набора данных) тот корректирует модель для минимизации ошибок. Например, набор данных для обучения может состоять из изображений различных животных с соответствующей маркировкой, позволяющей алгоритму сравнивать прогнозируемый вариант маркировки с верным. При контролируемом обучении используется контрольный набор данных для оценки прогресса алгоритма в изучении модели, а также

© FATF/OECD 2021

проверочный набор для оценки работы модели на ранее неизвестных ей данных с тем, чтобы определить эффективность усвоения моделью тренировочных данных и понять, может ли она их обобщать для получения новых.

- **Supervisory technology (SupTech) — Надзорные технологии.** Использование надзорными органами новейших технологий для осуществления надзора и проверок.

- **Unsupervised learning (a.k.a. unsupervised machine learning) — Неконтролируемое обучение (неконтролируемое машинное обучение).** Процесс машинного обучения, позволяющий алгоритмам анализировать и объединять *неразмеченные* наборы данных для выявления скрытых шаблонов, группирования данных или отклонений без вмешательства человека. Алгоритм анализирует имеющиеся данные, находит корреляции и взаимосвязи без ключей путем получения информации и группирования подобных объектов, основываясь на ничем не ограниченном наблюдении и интуиции. С увеличением количества используемых алгоритмом данных возрастает тщательность и точность моделирования.

© FATF/OECD 2021

Приложение B. Дополнительные примеры в сфере Regtech по новым технологиям анализа и обмена данными (по тематике ПОД/ФТ) между представителями частного сектора экономики

Зашифрованные запросы: экспериментальная программа с использованием гомоморфного шифрования

Компания сферы Regtech в партнерстве с ФУ внедряет межбанковскую систему обмена информацией повышенной конфиденциальности. Эта технология с применением гомоморфного шифрования позволяет внедрять зашифрованные запросы по финансовым преступлениям, а также по соответствию комплаенс требованиям при обеспечении соблюдения регуляторных норм. В настоящее время Regtech-компания и ФУ работают в направлении привлечения в программу и других банков, определяют новые варианты применения (в т. ч. внутрибанковские трансграничные варианты применения, связанные с рейтингами рисков клиентов и модельными порогами) и двигаются в направлении производственного развертывания. Гомоморфное шифрование в данном случае специально применяется для защиты конфиденциальной информации от раскрытия, но при этом участники системы могут использовать данные в том числе и других учреждений для их анализа и сопоставления. Преимущества сохраняющих приватность аналитических инструментов состоит в возможности поисковых запросов участниками без раскрытия друг другу их условий. Это предоставляет потенциальным участникам возможность вести аналитическую работу при отсутствии рисков раскрытия, утечки информации и нарушения регуляторных норм. Основным препятствием для данного проекта является недостаточная четкость прояснения со стороны регулятора в отношении того, какого типа данными можно обмениваться, при каких условиях и как.

Совместная аналитическая платформа (Германия)

Компания из сферы FinTech в партнерстве с консорциумом ведущих банков, поставщиками программного обеспечения и научными работниками занимаются разработкой новой объединенной аналитической платформы для борьбы с финансовыми преступлениями. Такая платформа будет содержать инструментарий для объединения и анализа данных с целью обмена между ФУ финансовыми данными и данными о транзакциях. Это позволит получить новые сведения в отношении модели поведения преступников и об их сетях, как будет понятно по результатам анализа по системе в целом, а не только по каждому ФУ в отдельности. Имея такую аналитику, финучреждения Германии и всей Европы смогут видеть общую картину активности своих клиентов в рамках более широкой финансовой системы, тем самым затягивая узел вокруг отмывания денег через выявление прежде скрытых взаимоотношений и моделей операционного поведения.

Платформа для идентификации клиентов (на примере внедрения в странах Северного региона)

Компания из сферы Regtech была основана в 2019 г. шестью ведущими банками стран Севера в качестве совместной инициативы для решения вопросов, возникающих в связи с нормативными требованиями в сфере ПОД для рынка этого региона. Банки-

© FATF/OECD 2021

основатели разработали общий стандарт данных в отношении информации для идентификации клиентов (ЗСК), которая доступна посредством соответствующих сервисов идентификации компании и цифровой платформы, содержащей портал конечного потребителя/пользователя. Платформа полностью автономна и доступна для использования участвующими в проекте финансовыми учреждениями, нуждающимися в надежной и согласующейся с нормативными требованиями информации о клиентах. Она обеспечивает доступ и использование финансовыми учреждениями этой информации о клиентах в качестве базы для проведения собственной оценки рисков. Это идет на пользу и их клиентам, поскольку чем выше клиентоориентированность ФУ, тем легче выстраивать финансовые взаимоотношения. Контроль над взаимоотношениями с клиентами осуществляет само финучреждение. Компания обеспечивает неприкосновенность персональных данных в программе посредством применения безопасной гибридной облачной архитектуры, в принцип работы которой заложены моменты безопасности и неприкосновенности данных.

Использование индекса финансовой преступности

Чтобы лучше рассчитывать риски финансовых преступлений Банк А начал использовать индекс финансовой преступности (Financial Crime Index) Regtech. Индекс позволяет использовать собственные данные банка плюс информацию из общедоступных источников в комбинации с закрытой базой данных Regtech для ежемесячного формирования общего показателя риска финансовых преступлений, в дополнение к показателям и отчетам по девяти тематикам в сфере рисков финансовых преступлений.

Защищенная платформа сквозного шифрования

Компанией из сферы Regtech была создана платформа обмена информацией и данными, позволяющая банкам и другим ФУ обмениваться информацией, относящейся к сфере ПОД. Информация, обмен которой производится посредством этой платформы, может использоваться для индивидуальных сообщений (запросы информации) или для объединения данных по типу «один ко многим» (one-to-many), что позволяет ФУ: 1) решать задачи как по более простым запросам (например, уведомления о санкциях, согласно которым требуется дополнительная информация от ФУ контрагентов), так и 2) проводить более сложные совместные расследования (например, расследование по уведомлениям мониторинга транзакций 2-го уровня, касающиеся ряда учреждений), а также 3) расширить данные, используемые для надлежащей проверки высокорисковых клиентов (например, обмен данными в отношении ПДЛ, сотрудников регионального таможенного управления, конечных бенефициарных собственников, источников финансовых средств и т. д.).

Платформа создана с применением сквозного шифрования. Все данные, подлежащие обмену, защищены ключами шифрования и парольной защитой. Для объединения данных применяется одностороннее шифрование и хеширование, поэтому ФУ может делиться информацией со множеством реципиентов (верификация аутентичности данных или файлов для обмена производится при помощи хеширования). Владелец платформы не имеет доступа к каким бы то ни было незашифрованным данным, и платформа обеспечивает полную контролируемость посредством фиксации всех критических операций.

© FATF/OECD 2021

Подбор вслепую с использованием гомоморфного шифрования

Компания-разработчик программного обеспечения работала с государственным органом над экспериментальным проектом, позволяющим осуществлять подбор данных вслепую с использованием гомоморфного шифрования. Госоргану требовалось собирать и привязывать данные, полученные из нескольких частных и государственных источников, включая несколько ФУ, для статистических целей формирования общественной политики. Разработчик применил комбинацию технических и структурных мер контроля, чтобы можно было вносить зашифрованные данные таким образом, что:

1. только зашифрованная информация поступает из программной среды вносящего данные;

2. до того, как данные поступят реципиенту, осуществить их привязку невозможно: для конвертирования зашифрованных данных в компонуемый, размеченный массив реципиенту требуется посредник, третья сторона;

3. реципиент не может обратить процесс обработки и получить исходные данные, но может делать привязку массивов.

Проект успешно продемонстрировал возможность привязки данных к общему признаку так, чтобы он не был виден какой-либо стороне после того, как данные покинули среду реципиента. Это дает защиту приватности физических лиц, но в то же время позволяет осуществлять демографический анализ для целей выработки соответствующей политики. Технология в настоящее время производится в Великобритании и используется подразделением государственной системы здравоохранения (National Health Service Digital).

© FATF/OECD 2021

Приложение C. Рекомендации, направленные на поддержку применения технологий в сфере ПОД/ФТ

Ответственное применение новых технологий, включая технологии цифровой идентификации и передовые решения в области мониторинга и анализа операций (в т. ч. совместный анализ) может содействовать эффективному, с учетом рисков, внедрению Стандартов ФАТФ в государственном и частном секторе, а также расширению доступа к финансовым услугам.

Нижеприведенные положения продвигают сформулированный на форуме в Сан-Хосе *принцип развития позитивных и ответственных инноваций*, утвержденный ФАТФ в 2017 г. Новые технологии в сфере ПОД/ФТ должны разрабатываться и внедряться с учетом как существующих угроз, так и возможностей, обеспечивая, чтобы их применение не противоречило международным стандартам в отношении неприкосновенности и защиты данных, а также правилам кибербезопасности.

1. Создание как государственным, так и частным сектором благоприятной среды для ответственных инноваций с целью повышения эффективности ПОД/ФТ:

    i. *Инновационные решения, облегчающие имплементацию мер ПОД/ФТ, включая оценку рисков, НПК и другие требования; усиление проверок и контроля.*

    ii. *Положительные примеры модернизации внутренних систем прежних поколений или замена их новыми технологиями.*

    iii. *Соответствующие меры контроля и функции для новых решений в области ПОД/ФТ, включая: объяснимость и прозрачность процессов и результатов; контроль со стороны человека; соблюдение принципов неприкосновенности и защиты данных; строгая кибербезопасность; соответствие лучшим примерам применения и стандартам на общемировом и национальном уровне, а также техническим стандартам.*

2. Обеспечение неприкосновенности и защиты данных при внедрении новых технологий:

    i. *Обеспечение действующей правовой основы для обработки персональных данных при внедрении новых технологий.*

    ii. *Защита личной информации в соответствии с национальными и международными правовыми нормами.*

    iii. *Обработка данных в явных, конкретных и законных целях, в соответствии с национальными и международными правилами.*

    iv. *Поддержка ответственного развития и внедрения инновационных технологий, обеспечивающих сохранение конфиденциальности, в целях полноценного анализа и обмена информацией по ПОД/ФТ (при сохранении неприкосновенности данных).*

© FATF/OECD 2021

3. Продвижение инноваций в сфере ПОД/ФТ, в основных принципах которых заложено расширение доступа к финансовым услугам:

    i. *Минимизировать препятствия для более широкого доступа к финансовым услугам посредством разработки и внедрения инновационных решений.*

    ii. *Обеспечить ответственный подход к инновациям в соответствии с целями ФАТФ по способствованию расширению доступа к финансовым услугам.*

4. Разрабатывать и распространять гибкие, непредвзятые по отношению к той или иной технологии, основанные на результатах, а также соответствующие риск ориентированному подходу политику и принципы регулирования в сфере инноваций.

    i. *Рассмотреть вопрос влияния новых технологий комплексно, в контексте сопутствующих им организационно-структурных изменений, их возможные непреднамеренные последствия и общее влияние на эффективность ПОД/ФТ, а также на расширение доступа к финансовым услугам.*

    ii. *Создать и (или) обновить четкие программно-политические принципы и руководства, использовать примеры и лучшие варианты применения, нормативы (при необходимости) в целях инициирования и стимулирования ответственного применения новых технологий в сфере ПОД/ФТ.*

    iii. *Проводить консультации с коллегами и поднадзорными организациями для разработки содержания соответствующих программно-политических процессов и процессов принятия решений.*

5. Осуществлять информированный контроль

    i. *Получать опыт и знания в сфере новых технологий для обеспечения возможности информированного регулирования и надзора за их применением, в т. ч. для конкретных целей соответствия требованиям по ПОД/ФТ.*

    ii. *Находить варианты однозначно положительного, четко очерченного применения новых технологий для осуществления проверок и контроля в сфере ПОД/ФТ.*

    iii. *Осознавать риски и пользу новых технологий, понимать содержание соответствующих мер по минимизации рисков в целях сохранения их положительного воздействия.*

    iv. *Использовать технологии для усовершенствования контроля над исполнением мер по ПОД/ФТ.*

6. Продвигать и способствовать сотрудничеству

    i. *Сотрудничать, координировать усилия с соответствующими органами (в том числе занимающимися вопросами НЗД) для содействия выработке всеобъемлющего, согласованного подхода к пониманию рисков и пользы применения новых технологий в целях ПОД/ФТ, а также к решению связанных с этим проблем.*

© FATF/OECD 2021

ii. *Рассмотреть возможность создания среды сотрудничества для стимулирования межправительственных и (или) межсекторальных (государственный/частный сектор) исследований, а также разработки новых технологий и инновационных решений.*

iii. *Участвовать в международных программах по развитию глобальных принципов, регулирующих использование новых технологий для целей ПОД/ФТ, с тем, чтобы способствовать их соответствию принципам соблюдения прав человека, мерам по более полной имплементации принципов ПОД/ФТ в общемировом масштабе, обеспечению кибербезопасности, неприкосновенности и защиты данных, а также соответствующим техническим и отраслевым стандартам.*

© FATF/OECD 2021

Ссылки и источники информации

EBA (2020 г.), *Большие Данные и расширенный анализ данных.* [13]

EDPB (2020 г.), *Заявление о защите персональных данных, обрабатываемых в связи с предотвращением отмывания денег и финансирования терроризма*, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_20201215_aml_actionplan_en.pdf. [1]

ФАТФ (2017 г.), *Руководство по обмену информацией в частном секторе,* https://www.fatf- gafi.org/publications/fatfgeneral/documents/guidance-information-sharing.html. [10]

FinCEN (2020 г.), *Раздел 314(b) Информационного Бюллетеня*, http://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf. [11]

FSB (2020 г.), *Использование надзорных и регулирующих технологий властями и регулируемыми учреждениями*, стр. 32, http://www.fsb.org/2020/10/the-use-of-supervisory-and-regulatory- technology-by-authorities-and-regulated-institutions-market-developments-and-financial- stability-implications/. [9]

FSB (2017 г.), *Искусственный интеллект и машинное обучение в сфере финансовых услуг,* https://www.fsb.org/wp-content/uploads/P011117.pdf [17]

GLEIF (без даты), *Знакомство с кодом идентификации юридического лица (LEI),* http://www.gleif.org/en/. [21]

IIF (2019 г.), *Трансграничные потоки данных - преодоление ограничений, связанных с локализацией данных,* http://www.iif.com/Portals/0/Files/32370132_iif_data_flows_across_borders_march2019.pdf [19]

Maxwell, N. (2020 г.), *Инновации и дискуссионный документ: Примеры использования анализа данных с сохранением конфиденциальности для борьбы с финансовыми преступлениями,* http://www.future- fis.com/uploads/3/7/9/4/3794525/ffis_innovation_and_discussion_paper_-_case_studies_of_the_use_of_privacy_preserving_analysis_-_v.1.3.pdf. [18]

McAfee (2020 г.), *Что такое Cloud Security?* http://www.mcafee.com/enterprise/en-us/security- awareness/cloud.html. [7]

Microsoft (2016) г., *Гомоморфное шифрование* http://www.microsoft.com/en- us/research/project/homomorphic-encryption. [2]

© FATF/OECD 2021

Microsoft Azure (без даты), *Конфиденциальные вычисления* https://azure.microsoft.com/en-us/solutions/confidential-compute. (по состоянию на декабрь 2020 г.). [6]

ОЭСР (2020 г.), *Принципы искусственного интеллекта* https://www.oecd.ai/ai-principles. [16]

ОЭСР (2019 г.), *Принципы искусственного интеллекта* http://www.oecd.org/going- digital/ai/principles/. [15]

ОЭСР (без даты), *Blockchain Primer*, http://www.oecd.org/finance/OECD-Blockchain-Primer.pdf (по состоянию на декабрь 2020 г.). [8]

ОЭСР (без даты), *Что такое общий стандарт обмена информацией (CRS)?* http://www.oecd.org/tax/automatic-exchange/common-reporting-standard/ (по состоянию на декабрь 2020 г.). [14]

SAS (2020 г.), *Обработка естественного языка* http://www.sas.com/en_us/insights/analytics/what- is-natural-language-processing-nlp.html. [5]

Scheibner, J. (2020 г.), *Требования к защите данных и этике в рамках мультисайтовых исследований с использованием медицинских данных: сравнительный анализ законодательной структуры управления и роли технологий защиты данных* http://www.ncbi.nlm.nih.gov/pmc/articles/PMC7381977/pdf/lsaa010.pdf. [3]

Shiffman, G. (2020 г.), *«Федеративное обучение с помощью революционных технологий (Белая книга) ».* [4]

Tim Hulsen, T. (2020 г.), *Делиться – значит заботиться - инициативы по обмену данными в сфере здравоохранения,* http://www.mdpi.com/1660-4601/17/9/3046/pdf. [20]

ЮНКТАД (2020 г.), *Законодательство о защите данных и конфиденциальности во всем мире* https://unctad.org/page/data-protection-and-privacy-legislation-worldwide. [12]

© FATF/OECD 2021

КРИТИЧЕСКАЯ ОЦЕНКА ОБЪЕДИНЕНИЯ ДАННЫХ, СОВМЕСТНОГО АНАЛИЗА И ЗАЩИТЫ ДАННЫХ

Достигнутый за последние годы технологический прогресс позволяет финансовым организациям более грамотно анализировать большие объемы данных и эффективнее распознавать шаблоны и тенденции. Объединение данных и их совместный анализ может содействовать сотрудничеству между финансовыми учреждениями в целях лучшего понимания, оценивания и снижения рисков отмывания денег и финансирования терроризма. В ФАТФ изучают новейшие технологии, позволяющие проще и качественнее выявлять преступные действия, сократив при этом количество ложноположительных результатов и ограничивая криминалитет в использовании информационных пробелов, существующих во взаимодействии между финансовыми организациями.

Также в настоящем документе говорится о необходимости протекционизма в отношении защиты информации и личных данных: ПОД/ФТ, конфиденциальность и защита данных представляют собой элементы существенного общественного интереса и служат достижению важных целей. Новые и активно разрабатывающиеся технологии повышения конфиденциальности сулят большие возможности по защите личных данных в конкретных случаях их использования и в соответствии с национальными и международными нормами по обеспечению неприкосновенности и защиты данных.

www.fatf-gafi.org | ИЮЛЬ 2021 Г.