



EAG



МЕЖДУНАРОДНЫЙ СЕМИНАР

«Государственно-частное партнерство
как инструмент повышения
эффективности системы ПОД/ФТ»

Консультации с частным сектором

СБОРНИК ПРЕЗЕНТАЦИЙ

26 - 27/09.2019

КАЗАНЬ/РОССИЙСКАЯ ФЕДЕРАЦИЯ



Council of Europe
Conseil de l'Europe

НР.3 и НР.4 *Существующие методики оценки* *ОБЗОР*

Котрина Филипавичюте (Kotryna Filipaviciute)
Администратор Секретариата МАНИВЭЛ

Council of Europe
Conseil de l'Europe

Непосредственный результат 4: предупредительные меры, принимаемые частным сектором

Оценка применения предупредительных мер и подтверждение выводов по Основным вопросам:

- уровень соответствия требованиям Рекомендаций 9-23 и 1, 6 и 29;
- повышенное внимание к конкретным секторам (в соответствии с рисками и факторами, определяемыми ситуацией);
- выбор подотчетных субъектов на основе анализа институциональных данных и информации, предоставленной надзорными органами;
- **достижение НР.4 оценивается на основании выездных интервью.**
- **Выводы должны подтверждаться данными других источников информации**, такими как:
 1. внутренние политики в сфере ПОД/ФТ;
 2. данные надзорных органов: а) данные выездных проверок: оценки отраслевого/институционального риска; б) данные удаленных проверок (всесторонние данные надзорных органов, статистика, серьезность нарушений и т.п.);
 3. результаты НОР;
 4. тенденции и методики направления СПО и т.д.

Основной вопрос 4.1

Насколько хорошо подотчетные субъекты понимают риски ОД/ФТ и обязательства в сфере ПОД/ФТ? (I)

В какой мере учитывались результаты НОР?

НОР

- Подверженность страны риску - Национальная оценка рисков (НОР);



ОПР

- Оценка предпринимательских рисков (ОПР)

Основной вопрос 4.1

Насколько хорошо подотчетные субъекты понимают риски и обязательства в сфере ПОД/ФТ? (II)

1. Подверженность страны риску - Национальная оценка рисков (НОР)

- Результаты НОР (включая НКО, юридических лиц и юридические образования, виртуальные активы, риски, связанные с ФТ и т.п.)
- В какой мере результаты НОР используются для углубления понимания рисков, угроз и уязвимостей?

2. Оценка отраслевых рисков, наднациональная оценка рисков (при наличии)

3. Подверженность фирмы риску - Оценка предпринимательских рисков (ОПР)

- основные риски, угрозы и уязвимости;
- план снижения рисков;
- распределение ресурсов/обязанностей и мониторинг (в том числе привлечение высшего руководства);
- обновление ОПР (частота, охват, побудительные причины).

Соразмерны ли меры контроля рискам?

Примеры:

Коррупция

- Акцент на ПДЛ;
- более жесткие меры контроля в отношении ПДЛ (иностранцы ПДЛ и национальные ПДЛ);
- особый акцент на приближенных лиц и бенефициарных собственников;
- специальные сценарии контроля и т.п.

Преобладающее использование наличных

- Акцент на наличных операциях и клиентах, занимающихся бизнесом, связанным с большим объемом наличных расчетов;
- сниженные пороговые значения;
- более жесткие сценарии контроля денежных депозитов / снятия наличных и обмена наличной валюты и т.д.

Уклонение от налогов и уклонение от санкций

- Акцент на юридических лицах и юридических образованиях и т.п. (например, большая доля юридических лиц со сложной структурой собственности в базе данных всех клиентов), их сделках / деловых партнерах;
- более жесткие меры контроля в отношении бенефициарных собственников (включая расширенные данные о собственниках);
- сценарии контроля, соответствующие бизнесу и профилю риска клиента;
- специальное обучение сотрудников и т.д.

Основной вопрос 4.3 НПК и хранение данных и документов

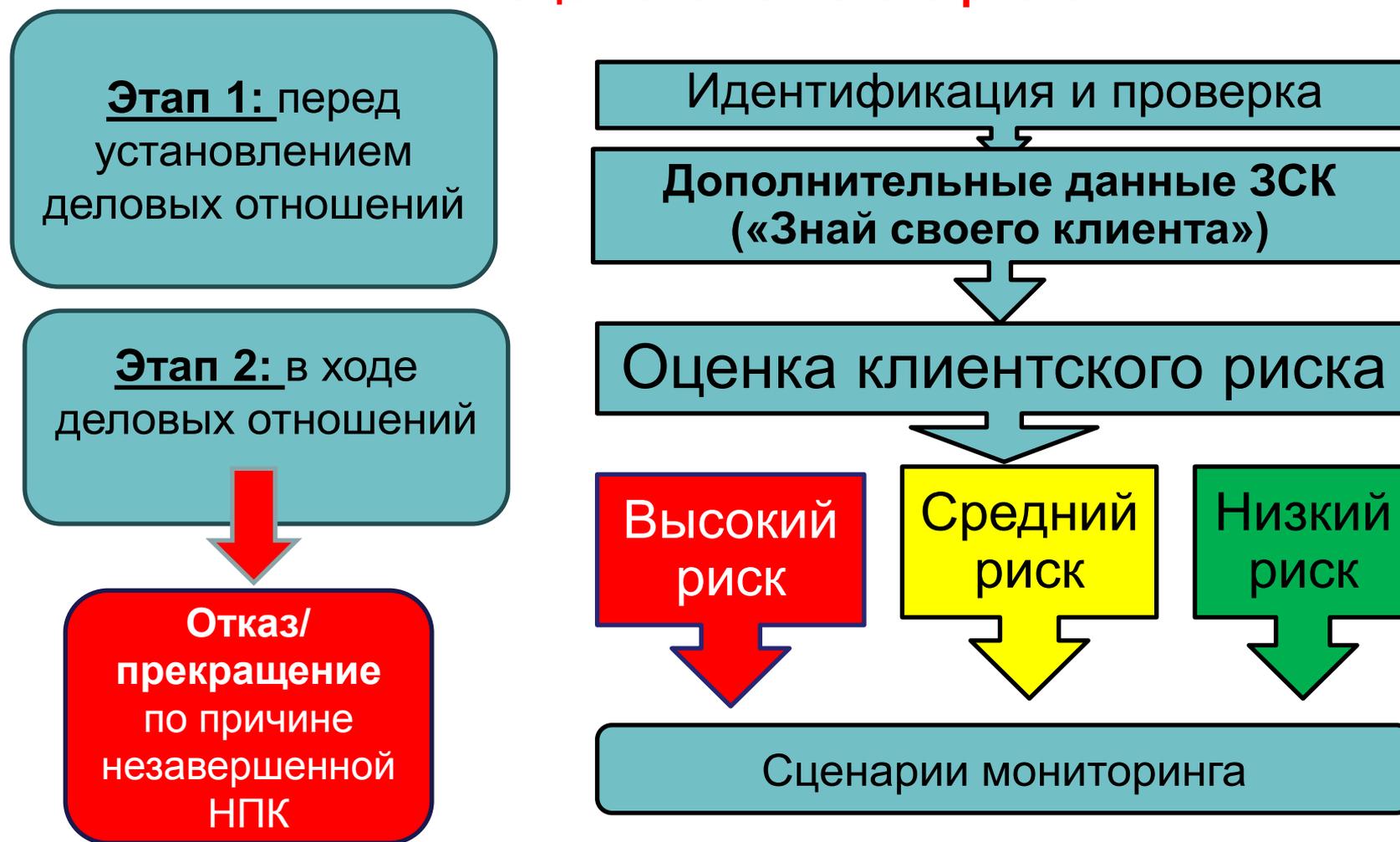
Области оценки (Р.10,11,17, Р.22-23):

1. Идентификация и проверка клиента и бенефициального собственника;
2. цель и характер деловых взаимоотношений;
3. оценка клиентского риска - профиль риска;
4. отказ в установлении деловых отношений по причине незавершенной НПК; отказы, на основании которых были направлены СПО (критерий 10.19);
5. мониторинг;
6. хранение данных и документов;
7. прекращение деловых отношений по причине незавершенной НПК; прекращения, на основании которых были направлены СПО (критерий 10.19);
8. возобновление НПК (частота, охват, побудительные причины).

Основной вопрос 4.3

НПК и хранение данных и документов:

Оценка клиентского риска



Основной вопрос 4.3 НПК и хранение данных и документов:

Слабые стороны:

- Проблемы идентификации бенефициарного собственника (сложные правовые структуры и механизмы, номинальные акционеры, акции на предъявителя и т.д.);
- Нечеткая и необоснованная цель и характер деловых отношений (например, клиенты-нерезиденты);
- Оценка клиентского риска не в полной мере учитывает все соответствующие факторы (риск, связанный с географическими факторами, каналы доставки, продукты, услуги, операции, предпринимательская деятельность клиента и т.д.);
- Уделяется мало внимания оценке клиентского риска в ходе деловых отношений (например, нет конкретных критериев для переоценки риска, не применяются никакие особые или усиленные меры, когда уровень клиентского риска меняется с низкого/среднего на высокий и с высокого на более низкий уровень);
- Сценарии мониторинга не разрабатываются в соответствии с уровнем клиентского риска, т. е. не существует конкретных/расширенных сценариев мониторинга для клиентов с высоким уровнем риска; нет различия между мониторингом клиентов с низким и средним уровнем риска и т. д.;
- Отказ в установлении деловых отношений или их прекращение ввиду присутствия серьезных подозрений о вовлеченности клиента в ПОД/ФТ не приводит к представлению СПО;
- Нет расширенного мониторинга деловых отношений после представления СПО;
- НПК для существующих клиентов не выполняется в соответствии с подходом, основанным на оценке риска (например, частота обновлений НПК и охват информации по ЗСК/НПК не определяются на основании клиентского риска).

Основной вопрос 4.3

Неспособность в полном объеме провести мероприятия по НПК

Дополнительные пояснения по просьбе участников семинара

Рекомендация 10, критерий 10.19:

Если финансовое учреждение не в состоянии применить соответствующие меры НПК должным образом, то:

(a) оно должно быть обязано:

- 1) не открывать счет;
- 2) не вступать в деловые отношения;
- 3) не осуществлять операцию

или должно прекратить деловые отношения;

(b) Необходимо рассмотреть возможность предоставления сообщения о подозрительных операциях (СПО) относительно клиента.

*УНФПП должны соответствовать требованиям рекомендации 10; см. Рекомендацию 22: «УНФПП: надлежащая проверка клиентов»

Основной вопрос 4.4 Усиленные и специальные меры НПК

Области оценки:

1. меры контроля в отношении ПДЛ (Р.12, Р.22);
2. корреспондентские банковские и аналогичные отношения (Р.13);
3. новые технологии (Р.15, Р.22);
4. правила в отношении электронных денежных переводов (Р.16, Р.14, в особенности критерий 14.4-14.15);
5. целевые финансовые санкции за ФТ (ЦФС за ФТ) (Р.6, критерий 16.18);
6. страны повышенного риска, указанные ФАТФ (Р.19, Р.23).

*УНФПП: Р.22-23

Основной вопрос 4.4

Усиленные и специальные меры НПК

Публичные должностные лица (ПДЛ)

- Р.12 (технические недостатки);
- сфера применения мер НПК (национальные и иностранные ПДЛ); цель установления деловых отношений с иностранными ПДЛ;
- проверки статуса ПДЛ (заявление клиента о себе + проверка с использованием надежных источников):
 - на этапе установления отношений с клиентом;
 - в ходе деловых отношений;
 - частота и объем проверок (клиент, бенефициарный собственник, цепочка собственников, ключевые сотрудники);
- идентификация членов семьи и приближенных лиц ПДЛ;
- Усиленный мониторинг (конкретные сценарии)
- Другие усиленные меры НПК (одобрение высшего руководства, источник денежных средств, источник благосостояния и т.д.) ;
- Разграничение между:
 - источником благосостояния;
 - источником денежных средств.

Основной вопрос 4.4

Усиленные и специальные меры НПК

Публичные должностные лица (ПДЛ)

Слабые стороны:

- Нечеткая цель вступления в деловые отношения с иностранными ПДЛ;
- Отсутствуют процессы/процедуры для идентификации членов семьи и ближайшего окружения ПДЛ (например, нет заявления клиента о себе, чрезмерная зависимость от коммерческих баз данных, нет проверок в отношении ближайшего окружения ПДЛ в ходе постоянного мониторинга, т.е. не хватает более внимательного и тщательного подхода к сторонам сделки, деловым партнерам и т. д.);
- Отсутствие процедур, которые определяют, стал ли существующий клиент ПДЛ (в ходе деловых отношений);
- Небольшой объем проверок для подтверждения статуса ПДЛ (например, отсутствие проверок бенефициарного собственника, включая директоров);
- Не применяется расширенный мониторинг в отношении ПДЛ (или выработанные конкретные сценарии мониторинга);
- Сценарии мониторинга, разработанные для иностранных и местных ПДЛ, не отличаются друг от друга (уместно, когда цель деловых отношений с иностранными ПДЛ четко не определена или не обоснована);
- Нет различия между источником благосостояния и источником денежных средств (плохое понимание).

Основной вопрос 4.4

Усиленные и специальные меры НПК

Корреспондентские банковские отношения

Риск и существенные факторы:

- статистика (корреспондентские банковские отношения и объем переведенных средств);
- страны учреждения банков-респондентов;
- другие типы корреспондентских банковских отношений.

Меры НПК:

- уровень соответствия требованиям Р.13 (влияние на практическое применение);
- специальные меры НПК.

Основной вопрос 4.4

Усиленные и специальные меры НПК

Новые технологии

- Уровень соответствия требованиям Р.15
- Проводится ли оценка до запуска новых продуктов / услуг / технологий / механизмов доставки?
- Проводится ли оценка на постоянной основе?
- Каковы основные риски и меры по снижению рисков?

•! ПРИМЕРЫ

Возможные общие недостатки:

- УНФПП менее осведомлены о требовании / не проводят такую оценку риска (однако оценка должна учитывать характер услуг, которые предоставляют подотчетные учреждения, и технологии, которые они используют (если это имеет место));
- оценки рисков финансовых учреждений (ФУ) в отношении новых технологий обычно связаны с оценками операционных рисков, при этом рискам ОД/ФТ уделяется очень мало внимания, если вообще уделяется.

Основной вопрос 4.4

Усиленные и специальные меры НПК

Электронные переводы денежных средств

Риск и существенные факторы:

• статистика (основные страны, участвующие в переводе средств (источник / место назначения); объем переведенных средств).

Применение правил в отношении электронных денежных переводов:

- уровень соответствия требованиям Р.16;
- объем информации, сопровождающей перевод средств;
- процедуры обнаружения недостающей информации;
- меры, принятые в соответствии с РОП (ограничение/прекращение деловых отношений с платежной системой плательщика, платежной системой посредника; направленные СПО);
- Внутренний контроль по отношению к агентам провайдера УПДЦ;
- ЦФС и страны повышенного риска.

Основной вопрос 4.4

Усиленные и специальные меры НПК

Целевые финансовые санкции за ФТ (ЦФС за ФТ)

- **Процедуры тщательной проверки: характер, объем и периодичность проверок:**
 - в момент установления деловых отношений с клиентом;
 - в ходе деловых отношений;
- **совпадения с санкционными списками и процедуры отчетности;**
- **обработка ложных совпадений.**

Возможные общие недостатки:

- тщательная проверка проводится эпизодически (частота проверок определяется в зависимости от уровня риска клиента);
- объем проверок не является достаточным (например, в случае сложных правовых структур и механизмов);
- отсутствие процедур для обнаружения ближайшего окружения санкционированных организаций / лиц и / или лиц, имеющих прямые и косвенные связи с санкционированными лицами / организациями; не уделяется должного внимания тщательной проверке каждой из сторон сделки.

Основной вопрос 4.4

Усиленные и специальные меры НПК

Страны повышенного риска, указанные ФАТФ

Риск и существенные факторы:

- объем средств, поступающих из стран повышенного риска; объем средств, переведенных в страны высокого риска;
- количество клиентов и бенефициарных собственников из стран высокого риска (место жительства, гражданство, национальность);
- масштаб деятельности, связанной со странами высокого риска.

Применение усиленных или специальных мер:

- специальные меры НПК, применяемые в отношении клиентов, имеющих связи с высокорисковыми юрисдикциями (примеры);
- специальные меры НПК, применяемые в отношении операций, инициированных в странах повышенного риска / из стран повышенного риска.

Общие недостатки:

- более жесткие меры контроля, применяемые подотчетными учреждениями в отношении клиентов, которые проживают в странах повышенного риска, при этом в отношении операций, инициированных в странах повышенного риска / из стран повышенного риска, никаких конкретных мер не применяется (например, отсутствуют сценарии специального или усиленного мониторинга).

Основной вопрос 4.5

Обязательства в отношении направления сообщений (I)

- Внутренние СПО и СПО, направленные в ПФР;
- направление сообщений о незавершенных операциях;
- сценарии мониторинга для выявления подозрительной деятельности, связанной с: а) ФТ; б) ОД.

Общие недостатки:

- в небольших ФУ и УНФПП количество внутренних и внешних СПО существенно не отличается, что ставит под сомнение эффективность мониторинга (подлежит оценке с учетом характера, размеров, масштаба коммерческой деятельности и клиентуры подотчетного учреждения);
- отсутствуют (или почти отсутствуют) специальные сценарии мониторинга для выявления ФТ; ФТ трактуется в более узком смысле;
- непонимание типологий, связанных с ФТ и ОД (в частности, по конкретным секторам);
- мониторинг ограничивается проверками операций; очень мало внимания уделяется поведению клиентов (ретроспективный мониторинг) и сторонам сделок;
- малое количество направляемых сообщений (небольшие финансовые учреждения и УНФПП).

Основной вопрос 4.5 Предотвращение утечки информации (II)

- Имеются ли практические меры для предотвращения утечки информации? Отражено ли это (и если да, то как) в учебных программах по ПОД/ФТ?
- Были ли проблемы в прошлом? (например, раскрытие конфиденциальной информации; проблемы с задержкой денежного перевода и взаимодействия с клиентом и т.д.)
- Является ли обратная связь с ПФР достаточно быстрой, чтобы исключить опасения по поводу утечки информации? (См. также Р.20-21.)

Основной вопрос 4.6

Меры внутреннего контроля

Области оценки:

- распределение обязанностей (3 линии защиты: передняя, соответствие и функция аудита);
- управление рисками и внутренний контроль (привлечение высшего руководства к решению вопросов ПОД/ФТ, управленческая отчетность, мониторинг, взаимодействие, принятие решений и т.д.);
- программы обучения в сфере ПОД/ФТ (обучение персонала);
- групповые политики и процедуры и т.п.

Непосредственный результат 3: НАДЗОР

Оценка надзора, мониторинга и регулирования ФУ и УНФПП и подтверждение выводов по Основным вопросам:

- уровень соответствия требованиям Рекомендаций 14, 26, 27, 28, 34 и 35 (и элементам Рекомендаций 1 и 40);
- повышенное внимание к конкретным секторам (в соответствии с рисками и факторами, определяемыми ситуацией; результаты НОР, оценка отраслевого риска и т.п.).

Выводы по Основным вопросам должны подтверждаться данными других источников информации, такими как:

1. размер, состав и структура секторов ФУ и УНФПП;
2. процедуры лицензирования;
3. данные надзорных органов: а) данные выездных проверок: оценки отраслевого/институционального риска; б) данные удаленных проверок (всесторонние данные надзорных органов, статистика, серьезность нарушений в сфере ПОД/ФТ и т.п.);
4. руководства по надзору (оценки и контрольные списки, составленные во время выездной проверки, документы, в которых показано, как рейтинговая оценка риска подотчетного учреждения влияет на масштаб и частоту будущих надзорных мероприятий);
5. информационно-разъяснительные инициативы (методические указания, пособия, тренинги, семинары) и т.д.

Основной вопрос 3.1

Лицензирование/регистрация и другие меры контроля

- Уровень соответствия требованиям Р.26 и Р.28.

Новые соискатели:

- проверки профессиональной пригодности и добропорядочности (объем, тщательность и периодичность; критерии, факторы; сотрудничество с компетентными органами власти; лица, подлежащие проверкам, наличие уголовного прошлого, проверки репутации; подтверждающие данные и документация, источник благосостояния и т.д.);
- оценка более широкого спектра рисков ОД/ФТ (профиль риска соискателя, бизнес модель, географические риски, негативная информация и т.д.);
- решение о выдаче лицензии / об отказе в выдаче лицензии;
- лица из близкого окружения преступников (проверки);
- статистика (полученные / отклоненные / отозванные / предоставленные заявки на получение лицензии - причины отзыва, отказов и т. д.)

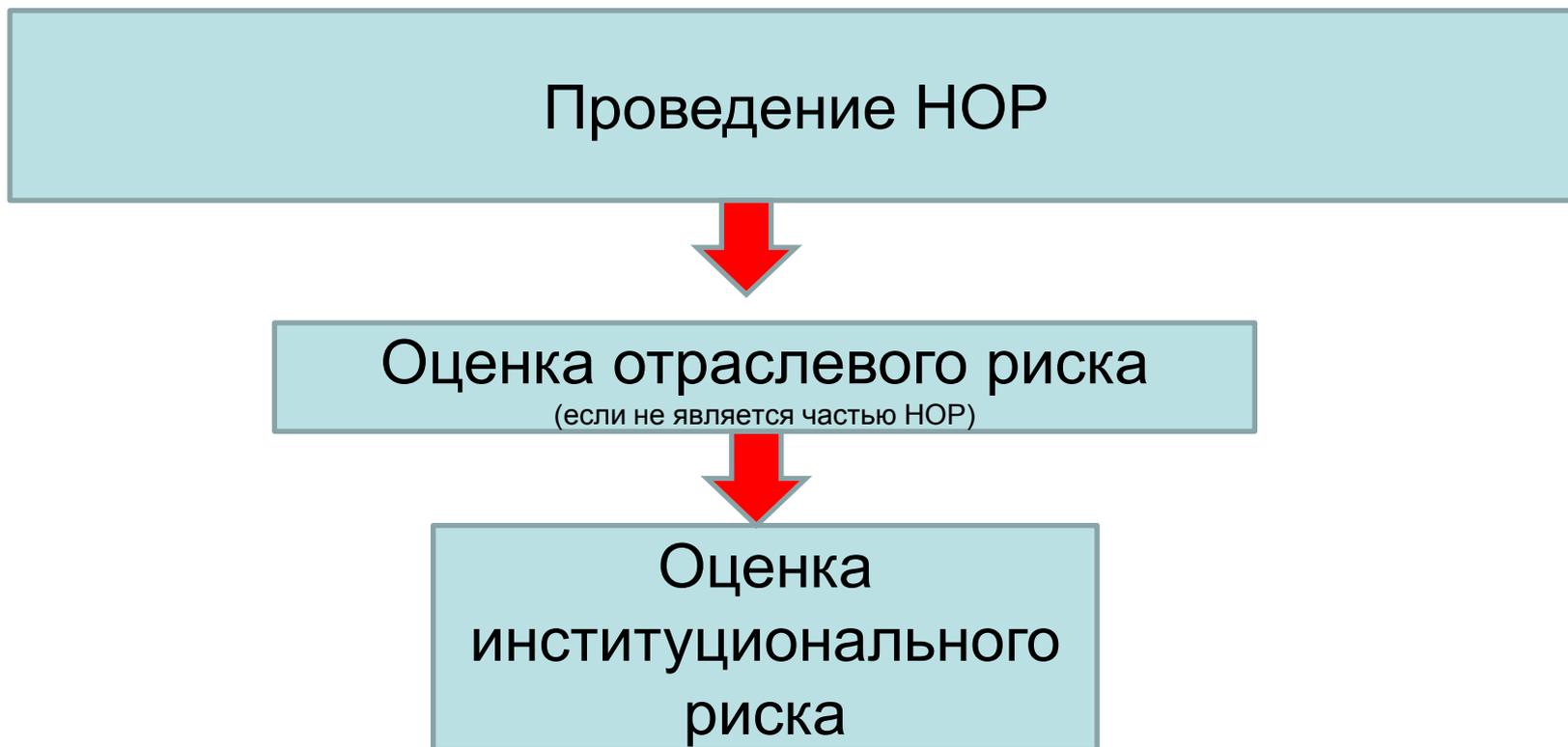
Обладатели лицензий:

- изменения имеющейся лицензии;
- изменения участия в акционерном капитале;
- назначения на ключевые посты;
- непрерывный мониторинг (для обладателей лицензий);
- статистика (отозванные лицензии, причины отзыва лицензии и т. д.).

Прочие факторы:

- исключения, нерегулируемые сектора;
- нелицензируемые виды деятельности.

Основной вопрос 3.2 Понимание надзорными органами рисков ОД/ФТ



Основной вопрос 3.3

Надзор на основе оценки риска

- Уровень соответствия требованиям Р.26-28;
- ресурсы надзорных органов, полномочия в сфере надзора;
- инструменты и методики удаленного надзора, соответствие оценок отраслевого и институционального риска (охват, частота, критерии);
- как уровень риска субъекта влияет на объем и периодичность будущих надзорных действий?
- выездной надзор (методологии, планирование выездной проверки, процесс проверки и пост-проверки);
- сотрудничество с компетентными органами (отечественными и зарубежными);
- групповой надзор.
- Примеры надзорных мер: удаленные проверки, тематические проверки (выездные и удаленные), целевые проверки, полномасштабные проверки, встречи с ключевыми лицами (например, с сотрудником по вопросам соблюдения требований по борьбе с отмыванием денег, руководящим составом), другие формы взаимодействия с частным сектором.

Основывается ли надзор на риске? Как органы надзора могут это продемонстрировать?

Основной вопрос 3.4

Санкции за нарушения в сфере ПОД/ФТ

- Уровень соответствия требованиям Р.35;
- политика применения санкций;
- процесс принятия решений (с защитой от неправомерного влияния, четкие критерии и т.д.);
- эффективность, соразмерность и сдерживающее воздействие санкций (в зависимости от серьезности нарушений и т.д.);
- санкции налагаются:
 - на основании результатов выездной проверки;
 - на ином основании (например, нарушение лицензионных требований) и т.п.;
- примеры последующих мер;
- уголовные санкции (включая дела, переданные правоохранительных органам, если применимо, и т.д.);
- санкции за нарушения, связанные с направлением СПО;
- санкции за нарушения, связанные с утечкой информации;
- публикация санкционных списков;
- санкции в отношении высшего руководства и директоров;
- штрафы.

Основной вопрос 3.5 Надзорные меры - влияние на соответствие

Влияние может быть продемонстрировано:

- на отраслевом уровне (например, на основе удаленных оценок, выявленных надзорными органами тенденциями к снижению риска: количественных (например, количество клиентов из высокорисковых стран) или качественных (например, определенные меры контроля));
- на институциональном уровне (по отношению к физическому лицу), на примерах из жизни (например, последующие меры);
- данные выездной проверки (всесторонние данные надзорных органов, обычно выявляемые нарушения и т.п.).

! Для подтверждения выводов необходимо привести примеры из практики/обобщенные данные по надзору (в дополнение к указанным выше данным).

Основной вопрос 3.6

Содействие ясному пониманию обязательств в сфере ПОД/ФТ и рисков ОД/ФТ

- Уровень соответствия требованиям Р.34.

Возможные примеры:

- указания;
- обязательные руководящие указания;
- тренинги, семинары;
- обратная связь (например, обобщенные отзывы об отраслевых рисках, ежегодные отчеты, результаты тематических обзоров или стратегического анализа; обобщенные отзывы об общих недостатках, выявленных в ходе выездных проверок);
- обратная связь с ПФР (типологии и т.д.);
- иные формы информационно-разъяснительной работы (консультации);
- совещания (например, ежегодные/ежеквартальные совещания с лицами, занимающими ключевые посты (например, членами совета директоров, специалистами по борьбе с отмыванием денег и т.д.).

Частота и содержание тренингов, семинаров, консультаций (обсуждаемые темы).



Council of Europe
Conseil de l'Europe
www.coe.int

МАНИВЭЛ

Спасибо!



**Роль ассоциативных организаций в формировании
механизмов коммуникаций в сфере ПОД/ФТ**

**Комитет по комплаенс-рискам и ПОД/ФТ
Ассоциации Банков России**

Казань, 26-27 сентября 2019г.



Ассоциация «Россия» - центр аналитической, экспертной работы банковского сообщества

- **координирует членов Ассоциации по вопросам:**
 - оценки нормативно-правового регулирования в сфере противодействия незаконным финансовым операциям
 - разработки подходов к управлению риском легализации
 - применения международного опыта управления комплаенс-рисками с целью дальнейшей выработки предложений по их применению для национальной системы ПОД/ФТ и системы управления рисками в целом
 - обсуждения и внедрения новых подходов и инициатив, направленных на сокращение издержек кредитных организаций при сохранении высокого уровня комплаенса
- **обеспечивает эффективное взаимодействие членов Ассоциации:**
 - с представителями Банка России, Росфинмониторинга, иными государственными органами и общественными организациями
 - с экспертами российских и международных практик
 - с Советом по профессиональным квалификациям финансового рынка



Координация и взаимодействие с членами Ассоциации «Россия»:

- непосредственное взаимодействие Ассоциации с кредитными организациями по рабочим вопросам, возникающим в их текущей деятельности (вопрос-ответ);
- проведение опросов кредитных организаций в целях публичного обсуждения проектов документов Банка России и законодательных актов в целях обеспечения непрерывности диалога в регуляторах;
- **функционирование Комитета по комплаенс-рискам и ПОД/ФТ Ассоциации**



Комитет по комплаенс-рискам и ПОД/ФТ

- привлечение интеллектуального и организационно-ресурсного потенциала членов Ассоциации к решению наиболее актуальных проблем в области управления комплаенс-рисками и ПОД/ФТ;
- выработка согласованной идеологии и политики членов Ассоциации по приоритетным направлениям работы Комитета;
- подготовка рекомендации, стандартов, правил и регламентов по решению отдельных проблем на данном направлении;
- осуществление экспертизы проектов законов и других нормативных актов, с целью их совершенствования, а также внесения изменений и дополнений в действующее законодательство Российской Федерации.



Комитет по комплаенс-рискам и ПОД/ФТ

Председатель Комитета

**Ассоциация: Вице-президент, Куратор
Комитета**

**Группа по международным
стандартам и законодательству**

**Группа по противодействию
отмыванию доходов и
финансированию терроризма**

Группа по работе с информацией

**Группа по новым технологиям
и инструментам в практике
управления комплаенс-
риском**



Функции Комитета по комплаенс-рискам и ПОД/ФТ :

- мониторинг и анализ текущего состояния, проблем и тенденций в области управления комплаенс-рисками и ПОД/ФТ;
- изучение инициатив банковского и бизнес сообщества в области управления комплаенс-рисками и ПОД/ФТ, их проработка с представителями деловых кругов и разработка необходимых предложений по их внедрению;
- изучение международного опыта по вопросам управления комплаенс-рисками и ПОД/ФТ и выработка предложений по их применению в России;
- представление позиции Ассоциации в Банке России и других органах государственной власти;
- проведение конференций, круглых столов, семинаров и иных мероприятий.



Темы заседаний в части работы по ПОД/ФТ

2018

Организация участия частного сектора в национальной оценке рисков

Внедрение механизмов «реабилитации клиента» кредитной организации

Обсуждение новых трендов, типологий, схем и методов ОД/ФТ

Вопросы информационного взаимодействия с Росфинмониторингом

2019

Вопросы повышения качества СПО

Оценка законодательных инициатив

Профессиональные стандарты и требования к сотрудникам служб финансового мониторинга



Задачи Комитета в сфере ПОД/ФТ на 2020г.

Организация участия частного сектора в национальной оценке рисков

Развитие КУС процедур

Обсуждение новых трендов, типологий, схем и методов ОД/ФТ

2020

Повышение эффективности информационного обмена с
Росфинмониторингом

Оценка законодательных инициатив

Профессиональная подготовка сотрудников служб финансового мониторинга, повышение финансовой грамотности населения

Взаимодействие с международными профессиональными объединениями

Опыт Кореи в сфере криптовалют

Ким Чжи Вун
Корейское подразделение
финансовой разведки

Содержание

I. Корейский рынок криптовалют в 2017 году

II. Политика правительства

III. Планы по внесению изменений в Закон о ПОД/ФТ

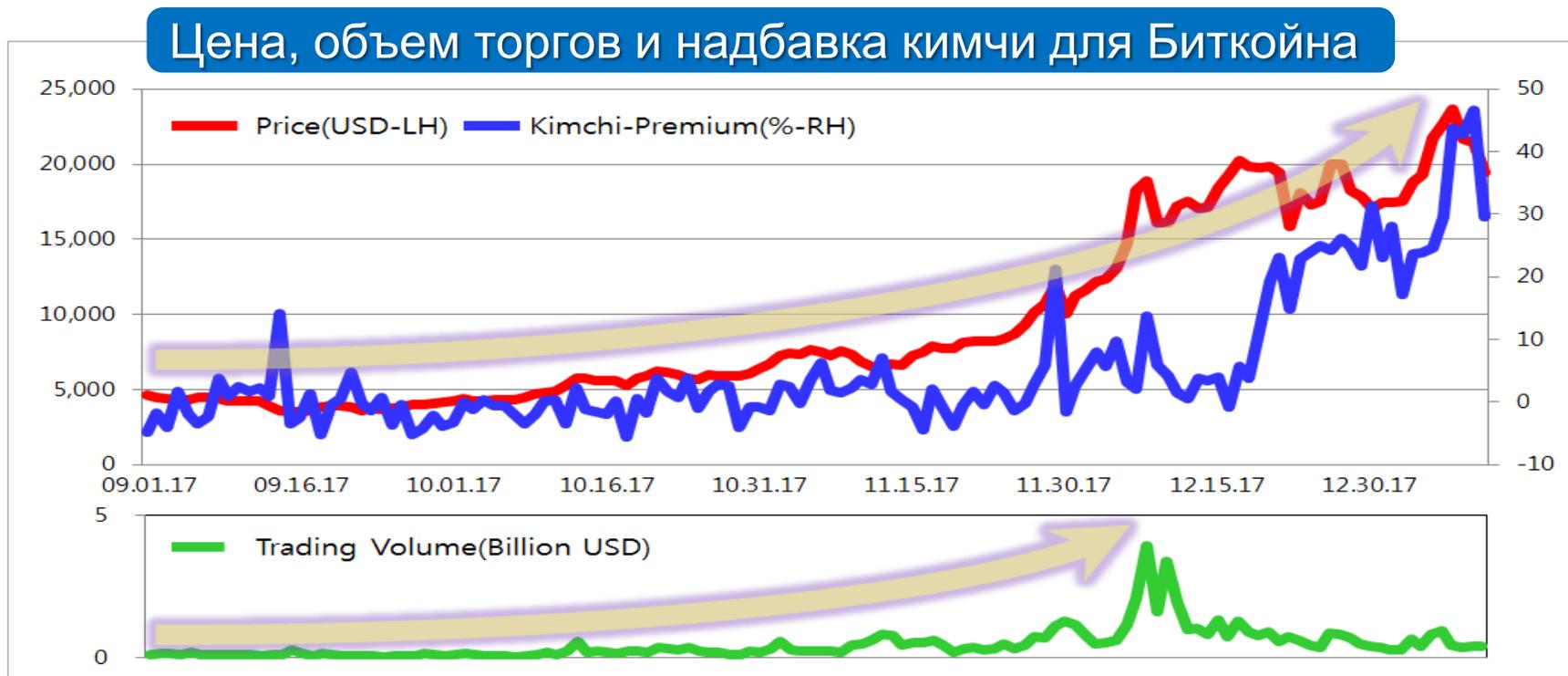
I. Корейский рынок криптовалют в 2017 году

Корейский рынок криптовалют в 2017 году

Перегретые спекуляции криптовалютами

Рост цен, стремительный рост объемов торгов
и увеличение "надбавки кимчи"

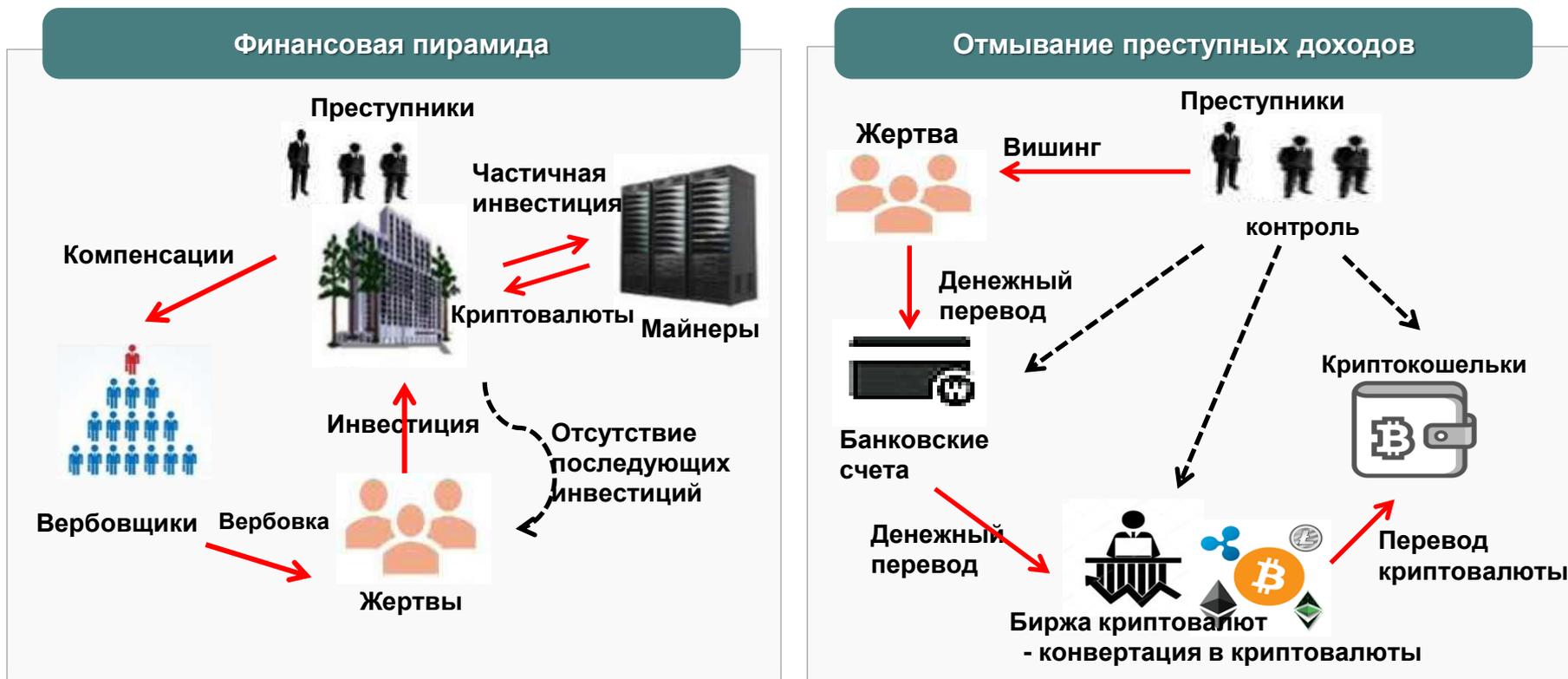
* Надбавка кимчи: Расхождение цен криптовалют на корейских биржах по сравнению с прочими биржами



Корейский рынок криптовалют в 2017 году

Широко распространенная незаконная деятельность, связанная с криптовалютой

Финансовая пирамида, незаконная деятельность по сбору средств и отмывание преступных доходов



II. Политика правительства

Меры Правительства в 2017 году

Совместная рабочая группа
по виртуальным валютам

Меры по
противодействию

1

Подавление незаконной деятельности, связанной с криптовалютами, правоохранительными органами (полицией, прокуратурой)

2

Защита пользователей бирж криптовалют

- Проверки на предмет нарушений статей о защите прав потребителей (Комиссия по добросовестной торговле)
- Инспекции по вопросам безопасности ИТ-систем (Корейская комиссия по связи)

3

Вынесение ряда предупреждений об инвестициях в криптовалюты и связанных с ними операциях (Комиссия по финансовым услугам, Служба финансового надзора)

4

Введение запрета на все виды первичного размещения криптомонет (Комиссия по финансовым услугам, Служба финансового надзора)

5

Обсуждение мер, позволяющих банкам идентифицировать пользователей бирж криптовалют

- Введение политики регистрации по удостоверению личности при осуществлении операций с криптовалютами (Комиссия по финансовым услугам, Служба финансового надзора)
- Установление руководящих принципов в отношении криптовалюты

Меры финансовых органов в январе 2018 года

1 Политика регистрации по удостоверению личности при осуществлении операций, связанных с криптовалютами

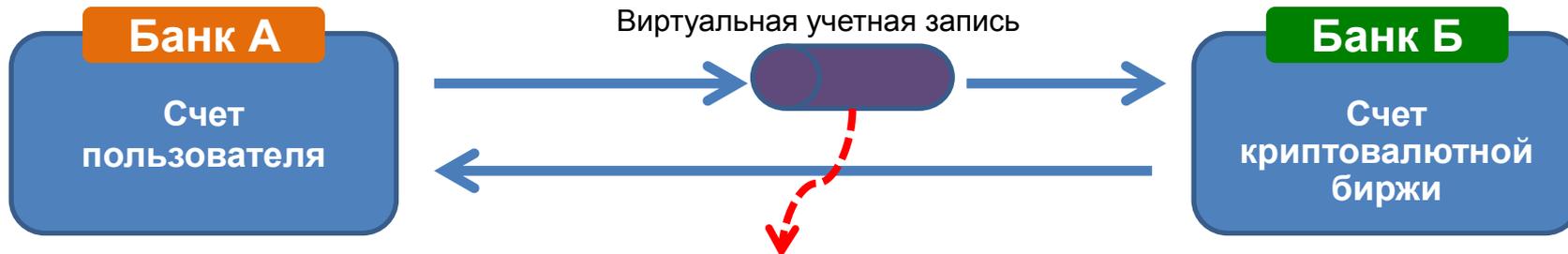
- ✓ Пользователи, желающие пополнять или снимать средства на криптовалютных биржах, обязаны пройти регистрацию по удостоверению личности
- ✓ Это позволяет банкам лучше идентифицировать пользователей

2 Руководящие принципы по ПОД в сфере криптовалют

- ✓ Распределение ролей и обязанностей финансовых учреждений, включая банки, в целях эффективного предотвращения отмыывания денег при осуществлении деятельности, связанной с криптовалютами



Ранее: Виртуальная учетная запись



Виртуальная учетная запись:

- Предоставлена **Банком Б**, но контролируется **криптовалютной биржей**
- **Банк Б** не может определить, кто отправил деньги на **криптовалютную биржу**

Теперь: Регистрация по удостоверению личности



Регистрация по удостоверению личности

- Осуществляется **Банком Б** и контролируется **Банком Б**
- Пользователи должны иметь банковские счета в том же банке, что и **криптовалютная биржа** (**Банк Б**)
- **Банк Б** может определить, кто отправил деньги на **криптовалютную биржу**

Руководящие принципы по ПОД в сфере криптовалют

Корейское подразделение финансовой разведки и Служба финансового надзора провели совместные выездные проверки соблюдения банками обязательств в области ПОД/ФТ (8 января - 16 января)

Результаты проверок были отражены в Руководящих принципах

1

- Обязанность по идентификации криптовалютных бирж

- Проведение расширенной комплексной клиентской проверки на криптовалютных биржах

Подтверждают ли криптовалютные биржи ① идентификацию пользователей и ② управляют ли депозитами пользователей отдельно от их собственных средств

2

Усиление мониторинга операций, относящихся к категориям, перечисленным в подробном перечне (направление отчетов о подозрительных операциях)

3

Усиление внутреннего контроля в финансовых учреждениях

- Четко определить обязанности совета директоров/исполнительного руководства в отношении операций с виртуальными валютами

III. Планы по внесению изменений в Закон о ПОД/ФТ

Планы по внесению изменений в Закон о ПОД/ФТ

1. Требования ПОД к криптовалютным биржам

Регистрация

Обязательная регистрация в ПФР

Меры
надлежащей
осмотрительности

Осуществление мер надлежащей осмотрительности в отношении клиентов, заключающих договоры на совершение сделок

ОПО

Направление ОПО в отношении операций с криптовалютой (включая обмен виртуальной валюты на финансовые активы)

Хранение документов

Хранение документов в отношении отчетов о подозрительных операциях, мерах надлежащей осмотрительности и т.п. в течение 5 лет

Внутренний контроль

Создание системы внутреннего контроля для оценки и управления риском ОД для каждой виртуальной валюты

Планы по внесению изменений в Закон о ПОД/ФТ

2. Дополнительные требования к криптовалютным биржам

- А. Записи об операциях должны храниться отдельно для каждого пользователя
- Б. Система управления информационной безопасностью должна быть сертифицирована

3. При работе с криптовалютными биржами финансовые учреждения обязаны:

А. Убедиться, что криптовалютная биржа:

①зарегистрирована в ПФР и ②сертифицировала свою систему управления информационной безопасностью

Б. Отклонить финансовые операции для криптовалютных бирж,

①не зарегистрированных в ПФР и ②не прошедших сертификацию своей системы управления информационной безопасностью



Спасибо
entro21@korea.kr



Financial Services
Commission



Взаимодействие государства и частного сектора в области регулирования финансовой деятельности в Интернете



Ключевые моменты

- Быстрый рост финансовой деятельности в Интернете: преимущества и проблемы
- Китайская национальная ассоциация по финансовой деятельности в интернете (NIFA) и ее уникальные преимущества
- Совместные усилия и первоначальные достижения РВС и NIFA
- Будущие работы



I. Быстрый рост финансирования через Интернет: преимущества и проблемы

- Повысить доступность, качество и эффективность финансовых услуг;
- Совершенствовать работы по идентификации личности, мониторингу транзакций и конфискации доходов, полученных преступным путем;
- Для руководителей: приоритеты, координация, применение регуляторных технологий RegTech, проведение перспективных исследований при ограниченности ресурсов....



II. Китайская национальная ассоциация по финансовой деятельности в интернете (NIFA) и ее уникальные преимущества

- **Сильная команда, обладающая опытом руководства, академическими и профессиональными знаниями;**
- **Широкий охват специалистов-практиков в области Интернет-финансирования;**
- **Уверенное руководство, управление и стимулирование работы всех участников.**

III. Совместные усилия и первоначальные достижения PBC и NIFA

- Принятие общего закона: *Административные меры для финансовых учреждений Интернета в борьбе с отмыванием денег и финансированием терроризма;*
- Подготовка производственного руководства;
- Создание мониторинговой платформы: *Онлайновая платформа мониторинга для борьбы с отмыванием денег и финансированием терроризма в индустрии Интернет-финансирования*

IV. Будущие работы

- **Активизировать сотрудничество с NIFA по вопросам Интернет-финансирования и других новых технологий;**
- **Изучить возможности сотрудничества с юристами, экономистами и др. специалистами для улучшения надзора за ОД в ОНФПП**

СПАСИБО!

Система контроля и надзора деятельности
коммерческих банков в целях ПОД/ФТ
в Кыргызской Республике.
Взаимодействие по вопросам ПОД/ФТ.

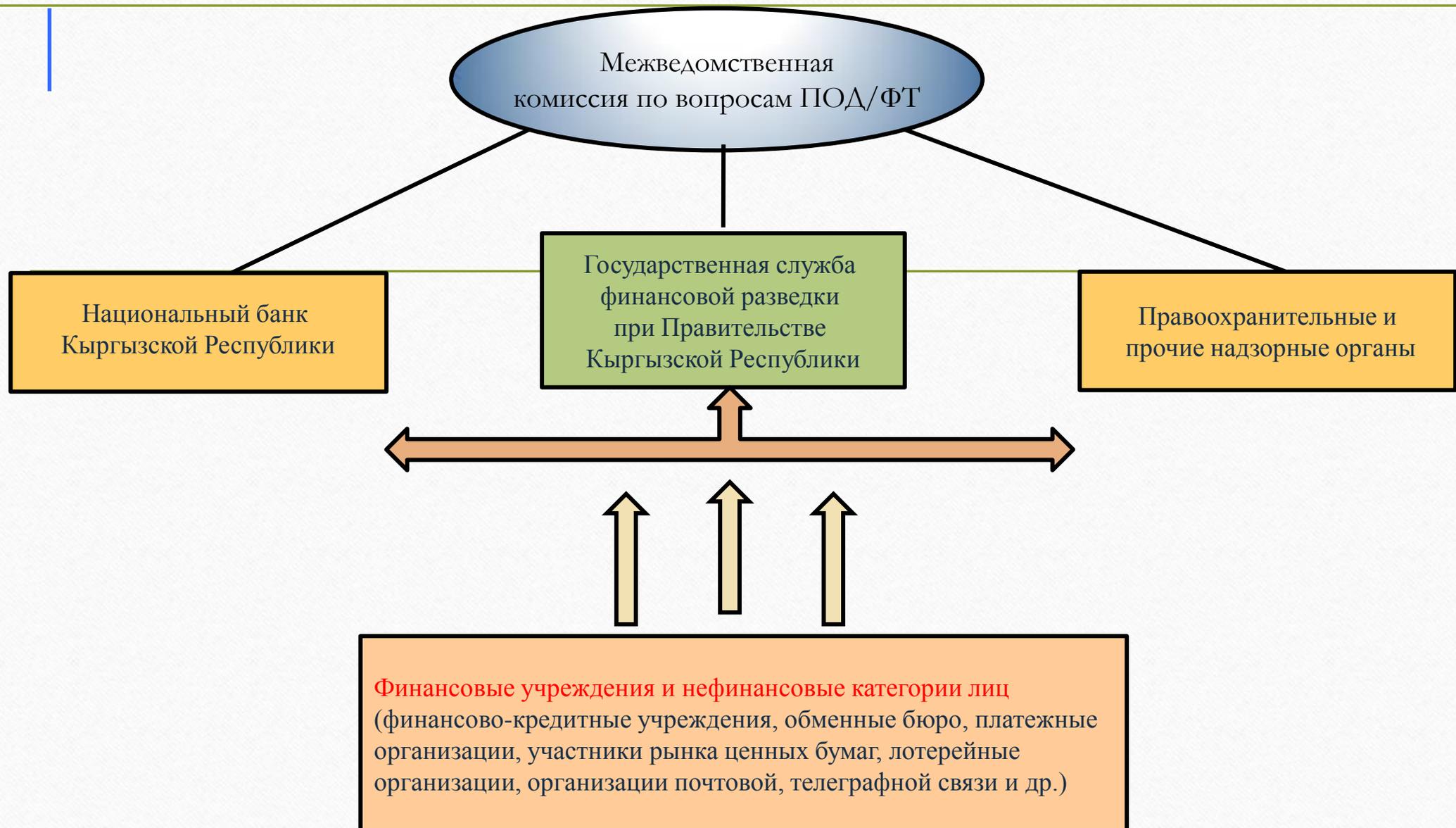
Национальный банк Кыргызской Республики

Управление банковского надзора 1

Иманбаева Жылдыз Бакытовна, ведущий инспектор

26-27 сентября 2019 г., г. Казань, РФ

Структура национальной системы по ПОД/ФТ



Банки и нефинансовые кредитные учреждения по состоянию на 04.09.2019 г.:

Поднадзорные субъекты	Количество
Коммерческие банки	24
Микрофинансовые организации (МФК, МКК, МКА)	140
Кредитные союзы и кредитные бюро	101
Специализированные ФКУ (Финансовая компания кредитных союзов)	1
Обменные бюро	410
Операторы платежных систем и платежные организации	22

Законодательство Кыргызской Республики в сфере ПОД/ФТ

Со второй половины 2018 года в законодательство КР в сфере ПОД/ФТ были внесены изменения и дополнения в целях приведения в соответствие с учетом Рекомендаций ФАТФ и результатов Взаимной оценки национальной системы по ПОД/ФТ.

- Закон Кыргызской Республики «О противодействии финансированию террористической деятельности и легализации (отмыванию) преступных доходов» от 6 августа 2018 года № 87;
- Постановление Правительства КР от 25 декабря 2018 года № 606 «О мерах по реализации Закона Кыргызской Республики «О противодействии финансированию террористической деятельности и легализации (отмыванию) преступных доходов», в соответствии с которой была (вновь) образована Комиссия по вопросам ПОД/ФТ, а также утверждены 13 нормативных правовых актов.

**Нормативные правовые акты, утвержденные постановлением
Правительства КР от 25 декабря 2018 года № 606 «О мерах по
реализации Закона КР «О ПОД/ФТ» (13 НПА):**

- 1) Положение о Комиссии по вопросам ПОД/ФТ;

- 2) Положение о порядке проведения проверки исполнения законодательства КР в сфере ПОД/ФТ;
- 3) Положение о порядке представления информации и документов в орган финансовой разведки КР;
- 4) Положение о порядке взаимодействия органа финансовой разведки с органами государственной власти КР;
- 5) Положение о перечнях физических и юридических лиц, групп и организаций, в отношении которых имеются сведения об их участии в террористической и экстремисткой деятельности, распространении оружия массового уничтожения и легализации (отмывании) преступных доходов;

**Нормативные правовые акты, утвержденные постановлением
Правительства КР от 25 декабря 2018 года № 606 «О мерах по
реализации Закона КР «О ПОД/ФТ» (13 НПА):**

- 6) Положение о порядке приостановления операции (сделки),
замораживания и размораживания операции (сделки) и (или) средств,
предоставления доступа к замороженным средствам и управления
замороженными средствами;
- 7) Положение об электронной базе данных бенефициарных владельцев
юридических лиц;
- 8) Положение об электронной базе данных задекларированных наличных
денежных средств или оборотных инструментов на предъявителя
перемещенных через таможенную границу Евразийского экономического
союза в КР ;

**Нормативные правовые акты, утвержденные постановлением
Правительства КР от 25 декабря 2018 года № 606 «О мерах по
реализации Закона КР «О ПОД/ФТ» (13 НПА):**

- 9) Положение о порядке применения мер (санкций) в отношении высокорискованных стран;
- 10) Положение об общих требованиях к программе внутреннего контроля;
- 11) Положение о порядке проведения надлежащей проверки клиента;
- 12) Положение о порядке осуществления международного сотрудничества;
- 13) Положение о проведении оценки рисков финансирования террористической деятельности и легализации (отмывания) преступных доходов.

Новшества в законодательстве в сфере ПОД/ФТ

Старая редакция	Новая редакция
Терминологии « риск-ориентированный подход » не было, но основные принципы и подходы содержались.	Риск-ориентированный подход
Правила внутреннего контроля	Программа внутреннего контроля
Бенефициарный собственник (выгодоприобретатель)	Бенефициарный владелец
Иностранные политические значимые лица	Публичные должностные лица: <ul style="list-style-type: none">- иностранное публичное должностное лицо;- национальное публичное должностное лицо;- публичное должностное лицо международной организации
-	Оценка рисков финансирования террористической деятельности и легализации (отмывания) преступных доходов (национальная оценка рисков → отчет о национальной оценке рисков)
-	Меры по защите некоммерческих организаций

Новшества в законодательстве в сфере ПОД/ФТ

Старая редакция	Новая редакция
-	Меры по защите некоммерческих организаций
-	Меры по обеспечению прозрачности бенефициарных владельцев юридических лиц <ul style="list-style-type: none">- Формирование информации юридическим лицом о своем бенефициарном владельце- Ведение электронной базы данных бенефициарных владельцев юридических лиц органом финансовой разведки
-	Электронная база данных задекларированных наличных денежных средств или оборотных инструментов на предъявителя, перемещенных через таможенную границу ЕАЭС в КР. Данная база данных формируется и хранится Государственной таможенной службой при Правительстве КР. Таможенная служба предоставляет органу финансовой разведки прямой доступ к базе данных.

Новшества в законодательстве в сфере ПОД/ФТ

Старая редакция

Терминология «НПК» отсутствовала, однако требования к идентификации и верификации имелись в соответствии с Рекомендациями ФАТФ.

Идентификация клиента и бенефициарного собственника по разовым операциям без открытия счета:

- Равная или более 1 млн сомов – полная идентификация;
- Менее 1 млн сомов – упрощенная идентификация клиента (установление личности клиента на основании документа, удостоверяющего личность);
- По обменным операциям с наличной иностранной валютой на сумму менее 50 000 сомов можно было не проводить идентификацию.

Новая редакция

Надлежащая проверка клиента

- Надлежащая проверка клиента и бенефициарного владельца при проведении разовых операций без открытия счета на сумму, равную или превышающую 70 000 сомов – полная идентификация;
- При совершении разовой сделки или нескольких взаимосвязанных операций по обменным операциям с наличной иностранной валютой на сумму 1 млн сомов и более – полная идентификация;
- При совершении разовой сделки или нескольких взаимосвязанных операций по обменным операциям с наличной иностранной валютой на сумму от 70 000 сомов до 1 млн сомов - упрощенная идентификация (установление личности клиента на основании документа, удостоверяющего личность);

Новшества в законодательстве в сфере ПОД/ФТ

Старая редакция	Новая редакция
<p>Операции, подлежащие обязательному контролю:</p> <ul style="list-style-type: none">- Операции, равные или более 1 млн сомов;- Операции, имеющие признаки подозрительных операций в соответствии с перечнем, утвержденным приказом Государственной службы финансовой разведки.	<p><u>Отсутствует общая для всех операций пороговая сумма 1 млн сомов.</u></p> <p>Операции (сделки), подлежащие контролю и сообщению:</p> <ul style="list-style-type: none">- сообщение о подозрительной операции (сделке);- сообщение об операциях (сделках) с физическими или юридическими лицами из высокорискованных стран;- сообщение об операциях (сделках) с физическими лицами, отбывшими наказание за осуществление ОД/ФТ;- сообщение об операциях (сделках) с наличными и безналичными денежными средствами, равную или превышающую пороговую сумму. <p>*Пороговая сумма на сегодняшний день не установлена.</p>

Операции (сделки), подлежащие контролю и сообщению

Вид сообщения	Сумма операции	Сроки предоставления сообщения в орган финансовой разведки
Сообщение о подозрительной операции (сделке):	Независимо от суммы операции в соответствии с перечнем критериев (кодов) подозрительных операций, утвержденный органом финансовой разведки.	в течение 5 (пяти) часов с момента признания в установленном порядке операции (сделки) подозрительной
Сообщение об операциях (сделках) с физическими или юридическими лицами из высокорискованных стран	Независимо от суммы совершенной операции (сделки)	в течение 2 (двух) рабочих дней со дня совершения операции (сделки)
Сообщение об операциях (сделках) с физическими лицами, отбывшими наказание за осуществление ОД/ФТ	Независимо от суммы совершенной операции (сделки)	в течение 2 (двух) рабочих дней со дня совершения операции (сделки)
Сообщение об операциях (сделках) с наличными и безналичными денежными средствами	На сумму, равную или превышающую пороговую сумму. *Перечень операций (сделок) с наличными денежными средствами и их пороговая сумма устанавливаются Правительством КР по результатам национальной оценки рисков. <u>На сегодняшний день пороговые суммы не установлены.</u>	<ul style="list-style-type: none">- в течение 3 (трех) рабочих дней со дня совершения операции (сделки);- по запросу СФР - в течение 10 (десяти) рабочих дней со дня получения запроса

Новшества в законодательстве в сфере ПОД/ФТ

Старая редакция

Требование наличия сертификата о прохождении курса по вопросам ПОД/ФТЭ, выданный образовательной организацией, при успешной сдаче экзамена/тестирования сотрудником банка

Новая редакция

- Лица, закончившие обучение в образовательной организации в соответствии с программой обучения в сфере ПОД/ФТ, проходят **итоговую аттестацию** в Учебно-методическом центре Государственной службы финансовой разведки КР;
- ГСФР направляет в образовательную организацию список лиц, успешно прошедших итоговую аттестацию;
- На основании информации ГСФР образовательная организация выдает сертификат об освоении образовательной программы.

Постановлением Правления Национального банка КР от 14 августа 2019 года № 2019-П-12\42-1-(НПА) внесены изменения и дополнения в НПА Национального банка КР (вступает в силу с 01 ноября 2019 г.):

- Положение о минимальных требованиях к организации внутреннего контроля в коммерческих банках в целях ПОД/ФТ;
- Инструкция по работе с банковскими счетами, счетами по банковским вкладам (депозитам) (включает требования к политике «знай своего клиента»);
- Постановление Правления НБКР «Об установлении требований по определению субъектов и перечня оффшорных зон»;
- Положение о порядке проведения обменных операций с наличной иностранной валютой в Кыргызской Республике
- и другие.

Новые НПА НБКР, охватывающие требования к управлению комплаенс риском и риском ОД/ФТ

- Правила формирования системы внутреннего контроля и внутреннего аудита в банках и небанковских финансово-кредитных организациях, лицензируемых и регулируемых НБКР (утверждено постановлением Правления НБКР от 15 июня 2017 года № 2017-П-12/25-3-(НПА), раздел 4 «ОРГАНИЗАЦИЯ СИСТЕМЫ КОМПЛАЕНС-КОНТРОЛЯ»
- Положение о минимальных требованиях по управлению рисками в банках Кыргызской Республики (утверждено постановлением Правления НБКР от 15 июня 2017 года № 2017-П-12/25-8-(НПА), раздел 13 «КОМПЛАЕНС-РИСК»

Управление комплаенс-риском и риском ОД/ФТ

Риск-ориентированный подход

- **Риск** - вероятность того, что ожидаемые или непредвиденные события могут оказать негативное влияние на капитал банка или его доходы.
- **Система управления рисками** - это процесс, включающий четыре основных элемента: определение риска, измерение риска, контроль риска и мониторинг риска.
- **Комплаенс-риск** - вероятность возникновения потерь вследствие несоблюдения банком и его работниками требований законодательства КР, нормативных правовых актов НБКР, внутренних документов банка, включая организацию внутреннего контроля по ПОД/ФТ, регламентирующих порядок оказания банком услуг и проведения операций на финансовом рынке, а также законодательства иностранных государств, оказывающего влияние на деятельность банка.
- **Риск ОД/ФТЭ** - это риск прямых или косвенных убытков, которому подвержен банк в результате нарушения банком требований законодательства, правил или стандартов в области ПОД/ФТЭ, вследствие вовлечения банка, его клиентов и партнеров в процессы, связанные с ОД/ФТЭ.
- **Риск-аппетит** – это совокупный уровень и виды рисков, которые банк готов принять на себя для достижения своих стратегических целей и бизнес-плана, с учетом сложно измеряемых рисков, такие как репутация банка и неэтичная практика. Риск-аппетит учитывается при разработке стратегии развития банка и бизнес плана банка.
- **Профиль риска банка** – это сводная информация всех текущих видов рисков и их уровней, которые отражают все ключевые проблемы в деятельности банка и выводы по итогам текущей (последней обновленной) оценки имеющейся информации по данным рискам.

Структура по управлению комплаенс-риском и ОД/ФТ в коммерческих банках

Старая структура

(внутренний контроль в целях ПОД/ФТ)

1 подразделение Службы внутреннего контроля в целях ПОД/ФТ, подотчетное Совету директоров Банка

Служба занималась только вопросами организации системы внутреннего контроля в целях ПОД/ФТ

Новая структура

(комплаенс контроль + ПОД/ФТ)

Служба комплаенс-контроля (подотчетен Совету директоров) включает 2 подразделения:

- Отдел по комплаенс
- Отдел по ПОД/ФТ

- управление и контроль комплаенс-рисками банка;
- организация в банке внутреннего контроля по ПОД/ФТ;
- контроль за проведением мониторинга соответствия деятельности банка согласно политикам и процедурам управления комплаенс-риском законодательству КР;
- контроль за организацией работы банка по рассмотрению жалоб (заявлений) клиентов банка;
- выявление, оценка и контроль конфликтов интересов;
- и другие функции

Надзорные мероприятия НБКР в рамках РОП



Меры воздействия, применяемые банкам

- Предписание
- Штраф:
 - По решению Комитета по надзору Национального банка КР (в размере не более 10% от норматива минимального размера уставного капитала (минимальный размер УК – 600 млн сомов), т.е. не более 60 млн сомов
 - В соответствии с Кодексом о нарушениях (по нарушениям, предусмотренным частями 1 и 2 статьи 216).
- Требование
- Повышение экономических нормативов и требований
- Ограничения или запреты (к примеру, приостановление, ограничение отдельных видов банковских операций)
- Отстранение или освобождение должностных лиц, смена органов управления
- Введение специального режима
- Отзыв лицензии

Кодекс КР о нарушениях от 13 апреля 2017 года № 58

- **Статья 18. Вина юридических лиц**

Юридическое лицо, совершившее нарушение, признается виновным, если физическое лицо, находящееся с ним в трудовых отношениях, или физическое лицо, выполняющее определенные действия в интересах юридического лица по договору, осознавало или могло и должно было осознавать противоправность своего деяния (действия или бездействия).

- **Статья 216. Нарушение требований законодательства о противодействии легализации (отмыванию) преступных доходов, финансированию террористической и экстремистской деятельности**

1. Нарушение требований относительно предотвращения или противодействия легализации (отмыванию) преступных доходов, финансированию террористической и экстремистской деятельности -

влечет наложение штрафа 4 категории (на юр.лицо - 230 расчетных показателей* – 23 000 сомов).

2. Нарушение требований относительно идентификации, верификации клиентов и установления бенефициарного собственника (выгодоприобретателя) или изучения финансовой деятельности клиентов -

влечет наложение штрафа 5 категории (на юр.лицо - 280 расчетных показателей – 28 000 сомов).

3. Нарушение порядка предоставления сообщений об операциях (сделках), подлежащих контролю, -

влечет наложение штрафа 7 категории (на юр.лицо - 450 расчетных показателей – 45 000 сомов).

4. Нарушение порядка замораживания средств и (или) операций (сделок) -

влечет наложение штрафа 8 категории (на юр.лицо - 550 расчетных показателей – 55 000 сомов).

** 1 расчетный показатель = 100 сомов*

Взаимодействие Национального банка КР с Государственной службой финансовой разведки КР

В рамках Соглашения о сотрудничестве и информационном обмене между Национальным банком КР и Государственной службой финансовой разведки КР от 12 марта 2012 года осуществляется:

- информационный обмен о выявленных нарушениях недостатках в деятельности банков и НФКУ в сфере ПОД/ФТ:
 - При обнаружении факта нарушения законодательства в сфере ПОД/ФТ в ходе комплексной (целевой) проверки Национальный банк КР не позднее 3 рабочих дней направляет Протокол о выявленных нарушениях;
 - По результатам комплексной (целевой) проверки не позднее 10 рабочих дней после отправки отчета в банк/ФКУ предоставляет итоговую информацию о выявленных нарушениях и недостатках системы внутреннего контроля;
 - При наличии подозрений, что операции (сделки) банка/ФКУ связаны с ОД/ФТ, сообщает о них в ГСФР КР для проведения финансового мониторинга (расследования).
- согласование проектов НПА, методических или иных инструктивных материалов в сфере ПОД/ФТ;
- организация и проведение обучающих семинаров, встреч, а также участие в семинарах через видеоконференц связь на базе ГСФР;
- И другое

Взаимодействие НБКР с коммерческими банками

- Вопросник по ПОД/ФТ
- Запрос информации по клиентам
- Консультации
- Обсуждение проектов НПА
- Циркулярные письма о рисках и мерах по их снижению
- Направление предписания, предупреждения
- Встречи по отдельным вопросам по мере необходимости

Национальный банк

Коммерческие банки

- Статистические данные и ответы на вопросник по ПОД/ФТ
- Направление информации по клиентам в соответствии с запросом НБКР
- Направление информации относительно выявленных рисков ОД/ФТ и комплаенс
- Отчет по исполнению предписаний и рекомендаций НБКР

Взаимодействие ГСФР с коммерческими банками

- Запросы по клиентам банка
- Консультация
- Встречи
- Семинары, круглые столы
- Обучение

Государственная
служба финансовой
разведки

Коммерческие банки

- Направление СПО
- Детальная информация о подозрительных операциях клиентов и схемах
- Участие в обсуждении НПА, направление предложений и замечаний

Взаимодействие НБКР с Союзом банков Кыргызстана

- Направление совместного мнения банков
- Участие в обсуждении проектов НПА
- Проведение семинаров, круглых столов
- Обучение по вопросам ПОД/ФТ

Национальный банк

Союз банков Кыргызстана

Консультации по вопросам ПОД/ФТ
Встречи руководителей служб
комплаенс-контроля

Коммерческие банки

- Членство
- Совместное продвижение интересов
- Представление интересов частного сектора
- Обсуждение спорных вопросов
- Лоббирование интересов банковского сектора

Взаимодействие НБКР с другими надзорными органами



Взаимодействие НБКР с надзорными органами других стран

- Заключены соглашения о сотрудничестве, включающие вопросы взаимодействия в области ПОД/ФТ между:

 - Центральным банком Российской Федерации;
 - Национальным банком Республики Беларусь;
 - Национальным банком Украины;
 - Центральным банком Кипра;
 - Народным Банком Китая.
- В случае необходимости получения дополнительной информации, взаимодействие с органами финансовой разведки, а также другими надзорными органами иностранных государств, осуществляется через Государственную службу финансовой разведки КР

Благодарим за внимание!

СПО: опыт оценки стран, механизмы обратной связи, ключевые измерители эффективности



МЕТОДОЛОГИЯ ОЦЕНКИ ТЕХНИЧЕСКОГО СООТВЕТСТВИЯ РЕКОМЕНДАЦИЯМ ФАТФ И ЭФФЕКТИВНОСТИ СИСТЕМ ПОД/ФТ



Вопрос 4.5.

- В какой степени финансовые учреждения и УНФПП выполняют свои обязанности сообщать о подозрениях относительно доходов, полученных преступным путем, и средствах в поддержку терроризма?

Примеры специфических факторов, которые могут подтверждать выводы по вопросу 4.5.



- Позволяют ли внутренняя политика и средства контроля финансовых учреждений и групп, а также УНФПП своевременно рассматривать: (i) сложные или необычные операции, (ii) предполагаемые СПО для направления в ПФР, и (iii) возможные ложноположительные результаты? В какой степени переданные СПО содержат полную, точную и адекватную информацию о подозрительной операции?
- Какие принимаются меры для повышения эффективности направления СПО?
- Насколько хорошо обеспечивается обратная связь для содействия финансовым учреждениям и УНФПП в выявлении подозрительных операций и передаче сообщений о них?

Информирование о подозрительных операциях

Основные недостатки стран



- Несвоевременность информирования и низкое качество сообщений
- Направление сообщений только на основании (настораживающих) признаков, а не на основании подозрений
- Незначительное количество сообщений от УНФПП
- Недостаточная адресная обратная связь от ПФР

Информирование о подозрительных операциях

Передовая практика



- **Выявление и информирование о ФТ**
- **Сотрудничество между государственным и частым сектором**
- **Обмен оперативными данными**
- **Качественная обратная связь по направленным сообщениям**
- **Принятие мер для снижения количества сообщений, направляемых «на всякий случай, для галочки»**

Режим СПО в странах



Государство Характеристика режима СПО

Количество
СПО

Испания



Финансовые институты перед подачей сообщения заполняют специальный отчет включающий структурированный анализ потенциально подозрительной деятельности со всеми связанными операциями, сторонами, вовлеченными в сделку, решение о том, следует ли представлять СПО. Такая система помогает устранить «ложные срабатывания» и защитную отчетность. Количество СПО не так низко, как могло бы показаться. Качество подтверждено **высоким уровнем использования СПО (около 40 %)** и конкретными кейсами значимых расследований.

≈ 3000

УНФПП. Нотариусы обязаны выгружать всю информацию о нотариальных действиях в централизованную базу данных, доступ к которой имеет ПФР, а также самостоятельно направляют СПО.

Бухгалтеры-криминалисты, занимающиеся расследованием случаев мошенничества, вообще не направляют СПО, поскольку считают, что мошенничество не связано с отмыванием денег.



Режим СПО в странах

Бельгия



УНФПП, обязанные направлять сообщения об операциях на основании установленных пороговых значений / критериев (в частности, казино), часто направляют только **такие «объективные» сообщения и не присылают сообщения, основанные на анализе подозрительности проводимых ими операций.** Однако, похоже, что нотариусы, бухгалтеры и налоговые консультанты учитывают «субъективные» факторы при принятии решения о направлении СПО. При этом юристы и торговцы алмазами практически не направляют СПО. Такой подход может затруднить выявление случаев ОД и привести к тому, что некоторые преступления останутся безнаказанными.

Риелторы практически полностью полагаются на «объективные» факторы при направлении СПО (в соответствии со Статьей 20 Закона о ПОД/ФТ).

Италия



Существенное увеличение количества СПО у банков, после проверки ПОД/ФТ **72000** связали с **наличием элемента «оборонительной» отчетности.**

За исключением нотариусов (для которых были разработаны специальные руководства), СПО секторами УНФПП направляется в небольшом объеме. В относительном выражении, работа нотариусов по направлению СПО отражает тесное взаимодействие государства и частного сектора. 72% СПО было направлено в течение двух месяцев, а 6% - более чем через семь месяцев после события. **Оценщики положительно отметили повышение оперативности направления СПО.**

Режим СПО в странах



Португалия



Требования к подаче СПО понятны финансовым организациям, и их отчетность соответствует уровню их риска. Тем не менее, **финансовые организации указывают, что есть сложности в обнаружении подозрительных транзакций, связанных с финансированием терроризма.** Финансовые институты просят дополнительные руководства (рекомендации) в этой области.

Нет данных

Швеция



Большинство **УНФПП** подают **очень мало СПО**, несмотря на высокую уязвимость в некоторых секторах (таких как провайдеры трастовых и корпоративных услуг, юристы и агенты по недвижимости). Это может свидетельствовать о **низкой осведомленности о рисках, с которыми они сталкиваются.** Надзорные органы признают эту проблему и пытаются улучшить уровень отчетности, **сосредоточив внимание на описании подозрительных действий клиента**, а также указывая на требования по направлению СПО при осуществлении проверок. Например, надзорные органы понимают, что агенты по недвижимости подают небольшое количество СПО и подозревает, что это не из-за недостатка знаний, а скорее, потому что **имеют высокий уровень ожидания определенного уровня «доказательств», прежде чем принять решение о подаче СПО.**

≈ 10000

У больших банков, постоянно взаимодействующих с ПФР имеется возможность получить информацию, которая помогает в их подаче СПО, они в целом удовлетворены уровнем получаемой от ПФР информации.

Режим СПО в странах



Государство Характеристика режима СПО

Кол-во

Сингапур



Представители **УНФПП**, похоже, не понимают, что цель СПО состоит в том, чтобы предоставить властям информацию, которая могла бы привести к раскрытию преступного поведения. Для УНФПП требуются руководства с описанием конкретных примеров подачи СПО.

≈ 28000

Гонконг
Китай



За 6 лет произошло увеличение количества СПО в 4 раза, что по мнению оценщиков отражает повышение осведомленности в банковском секторе. Объем оборонительных СПО хотя и снижается, но остается проблемой. Финансовые организации указали, что отзывы, которые они получают от ПФР, могут быть улучшены **путем предоставления информации о полезности и качестве информации, дополненной стратегическим анализом и типологиями с учетом потребностей их конкретных секторов.** ПФР предоставляет ежеквартальные отчеты по анализу СПО, а также обсуждает вопросы СПО в рамках специальной рабочей группы

≈ 86000

Режим СПО в странах



Государство Характеристика режима СПО

Кол-во

Малайзия



Группа оценщиков отметила, что подотчетные субъекты с которыми она встречалась, недостаточно осведомлены о масштабах обязательств **по сообщению о попытках совершения транзакций.**

Принимая во внимание контекст и риск в Малайзии, показатели СПО, связанных с ФТ, являются низкими. Несмотря на то что юридические обязательства являются всеобъемлющими и общепринятыми, существует необходимость в более целенаправленных руководствах (индикаторы риска ФТ и «красные» флажки), относящиеся к конкретным секторам.

Почти полное отсутствие СПО от профессиональных юристов, по-видимому, отражает отсутствие надзорного внимания, а не правовых препятствий.

≈30000

Мексика



Уровень отчетности представляется довольно неравномерным по учреждениям в некоторых секторах. Например, отчеты, поданные пятью ведущими организациями в каждом секторе в 2016 году, составляют большой процент от общего объема, поданного всем сектором: банками (75 процентов), брокерскими фирмами (89 процентов) и обменными центрами (70 процентов).

Стремясь улучшить качество отчетов, ПФР предоставляло подробные отзывы отдельным финансовым организациям, а также на уровне секторов. **СПО крупных фирм не всегда бывают такими быстрыми, как это должно быть.**

≈
120000

Режим СПО в странах



Приблизительно 11 % всех СПД подаются в тот же день, когда обнаружена подозрительная активность. Среднее количество времени в течение 30-дневного окна подачи СПД с момента идентификации новой подозрительной активности по подаче SAR составляет 17 календарных дней.

FinCEN **опубликовал свои рекомендации**, касающиеся торговли людьми. Число СПД, связанных с торговлей людьми, **увеличилось за год в 7 раз**. Это изменение отражает способность банков настроить свои системы мониторинга, чтобы лучше фиксировать определенные виды подозрительной деятельности и управлять рисками.

Частный сектор хорошо сотрудничает с ФБР по вопросам выявления операций, связанных с ФТ.

По закону финансовые институты обязаны немедленно уведомить правоохранительные органы по телефону и подать своевременное СПД, когда они идентифицируют ситуацию, связанную с нарушением, **требующим немедленного внимания**, независимо от какого-либо порога.

1 млн.
600

Режим СПО в странах



Великобритания



Банкам предоставлено время 30/60 дней для того, чтобы провести собственное расследование до подачи СПД, однако **существует требование сообщить о вопросах, требующих немедленного внимания в ПФР**, и все подтвердили, что они направляют СПД, как только они достигают порога подозрения.

440
тыс.

ПФР совместно с надзорными органами проводятся мероприятия по повышению эффективности режима СПО. Это включает в себя **отраслевые отчеты, рекламные кампании и отраслевые мероприятия, посвященные направлению СПД**. Кампания "Flag It Up" Министерства внутренних дел, которая ориентирована на юридический и бухгалтерский секторы, привела к заметному увеличению числаскачиваний соответствующего руководства ПФР по представлению СПД.

Количество СПД увеличилось в результате взаимодействия между государственным и частным секторами посредством JMLIT, а также работы специализированной группы в ПФР.

Австралия



Аустрак, совмещает функции ПФР и регулятора. Внедрена система при которой финансовые институты имеют возможность уведомить ПФР о предстоящей подаче СПО, а также напрямую провзаимодействовать с правоохранительными органами относительно востребованности СПО. Подотчетные организации особо **отметили проблемы при обнаружении операций, связанных с ФТ** при отсутствии конкретной информации, и принятие эффективных превентивных мер.

Нет
данных

Режим СПО в странах



Канада



Финансовые институты при выявлении подозрительных операций полагаются как на автоматизированные системы мониторинга, так и на квалифицированных сотрудников.

В специальных разделах СПО описывается причина подозрений. Оценщики положительно отметили эволюцию этого элемента СПО от базового резюме до очень тщательного и сложного анализа фактов. СПО, как правило, подаются в **30 дней**. В конце процесса внутренней оценки, если СПО не подано, производится запись с обоснованием ненаправления отчетности.

≈ 92000

УНФПП. Большие казино **выявляют подозрительные транзакции** не только через сотрудников фронт-офиса, но и **через аналитические инструменты мониторинга, разработанные на корпоративном уровне**, а также на основе **видео-расследований для выявления возможных необычных действий клиентов**.

Тот факт, что бухгалтеры и нотариусы не подают СПО, а количество СПО, поступающих из сектора недвижимости, невелико, вызывает беспокойство.

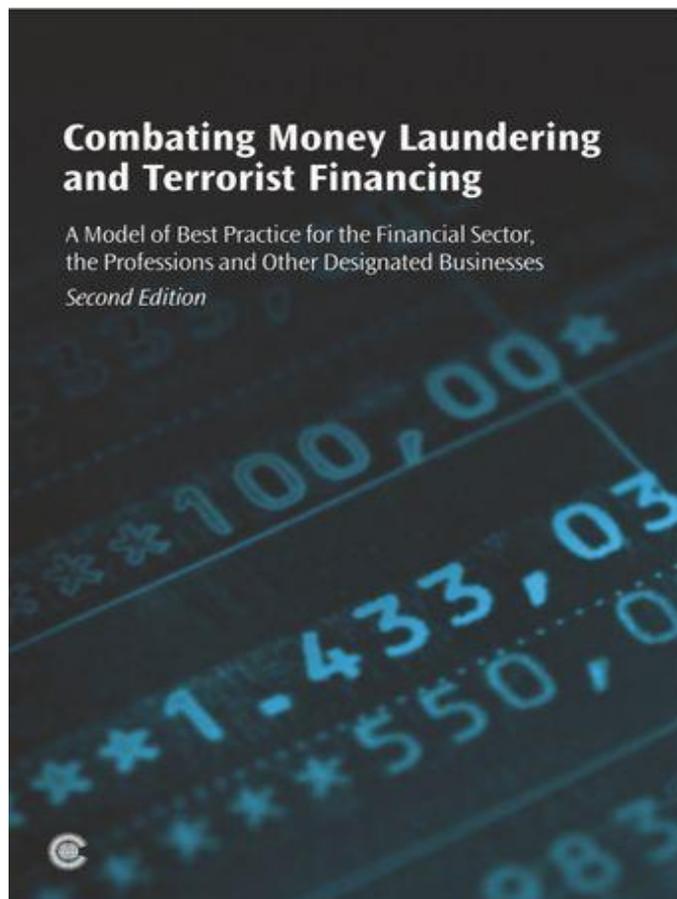
В ряде секторов значительно **увеличилось количество поданных СПО, в основном в результате информационно-разъяснительной деятельности со стороны ФИНТРАК.**

Крупные финансовые институты имеют хорошие каналы связи с FINTRAC и они получают адекватные отзывы на ежегодной основе о качестве их СПО и количестве осужденных лиц по делам инициированным FINTRAC. В ФИНТРАК было создано специальное подразделение для обеспечения обратной связи с финансовыми институтами.

Руководство ФАТФ: предоставление обратной связи подотчетным субъектам и иным лицам



FATF Guidelines: Providing Feedback to Reporting Institutions and Other Persons



■ Меры по борьбе с ОД будут более эффективными, если министерства и ведомства **будут работать в партнерстве с финансовым сектором**

■ Что касается СПО, важным элементом этого партнерского подхода является **необходимость предоставления обратной связи учреждениям или лицам, которые сообщают о подозрительных операциях**



Для чего необходима обратная связь?

- ✓ Уполномоченные сотрудники делают более качественные отчеты, которые с большей вероятностью позволяют правильно идентифицировать транзакции, связанные с преступной деятельностью;
- ✓ Уполномоченные сотрудники учреждений обеспечивают лучшую фильтрацию отчетов, которые на самом деле не являются подозрительными. Правильная идентификация операций, связанных с ОД или другими видами преступлений, позволяет более эффективно использовать ресурсы как ПФР так и подотчетной организации;
- ✓ Позволяет учреждению принимать адекватные меры, например закрывать счет клиента, если он осужден за преступление, или снимать с него подозрения (снижать риски), если расследование показывает, что в в его операциях нет ничего подозрительного;
- ✓ Может привести к **совершенствованию процедур предоставления отчетности и расследования** и часто приносит пользу надзорным органам, которые регулируют подотчетные учреждения;
- ✓ Это один из способов, с помощью которого правительство и правоохранительные органы могут внести свой вклад в **партнерские отношения с финансовым сектором**, и она предоставляет информацию, которая демонстрирует финансовому сектору, что **ресурсы и усилия, приложенные ими для сообщения о подозрительных операциях, имеют смысл и что есть конкретный результат.**



Формы обратной связи

- Предоставление макро статистики (количество СПО и результатах, полученных ПФР /расследований, связанных с ОД/ФТ
- Информация об актуальных типологиях и трендах в сфере ОД/ФТ
- Обезличенные примеры фактических случаев ОД/ФТ



- Количество СПО за период (общее и в разбивке по секторам или учреждениям), объем СПО, географические районы, из которых были переданы СПО, типы транзакций, по которым направляют СПО.
- Информация о количестве открытых расследований, количестве закрытых дел, а также дел, переданных в органы прокуратуры (разбивка по типам совершенных преступлений и сумме денег, а также гражданству вовлеченных сторон и какой из трех этапов отмывания денег имел место)



Примеры иной информации

- объяснение причин ОД описание процесса и трех этапов ОД, включая практические примеры;
- объяснение юридических обязательств сообщать, к кому оно относится и санкций (если таковые имеются) за непредставление отчета;
- процедуры и процессы, с помощью которых составляются, анализируются СПО;
- краткое изложение законодательных изменений в связи с режимом отчетности или преступлениями, связанными с ОД/ФТ



- письменная обратная связь (ежегодные отчеты и регулярные информационные бюллетени)
- путем личных встреч с финансовыми учреждениями, в том числе для конкретного учреждения или его персонала, или для более широкого круга учреждений.
- учебные видеокурсы
- электронные информационные системы, (информация с веб-сайтов, из других электронных баз данных или систем электронных сообщений)

ПФР Великобритании

United Kingdom Financial Intelligence Unit (UKFIU)



Журнал «Сообщение о подозрительной деятельности, как оно используется»



A United Kingdom Financial Intelligence Unit (UKFIU) publication aimed at all stakeholders in the Suspicious Activity Reports (SARs) regime

Что такое СПД?

- это информация, которая предупреждает правоохранительные органы, что в самом клиент или его деятельности являются подозрительными, что может указывать на его связь с ОД или ФТ.

Роль ПФР

ПФР ответственно за получение, анализ, проведение финансового расследования на основе полученного СПД

Как направить СПД?

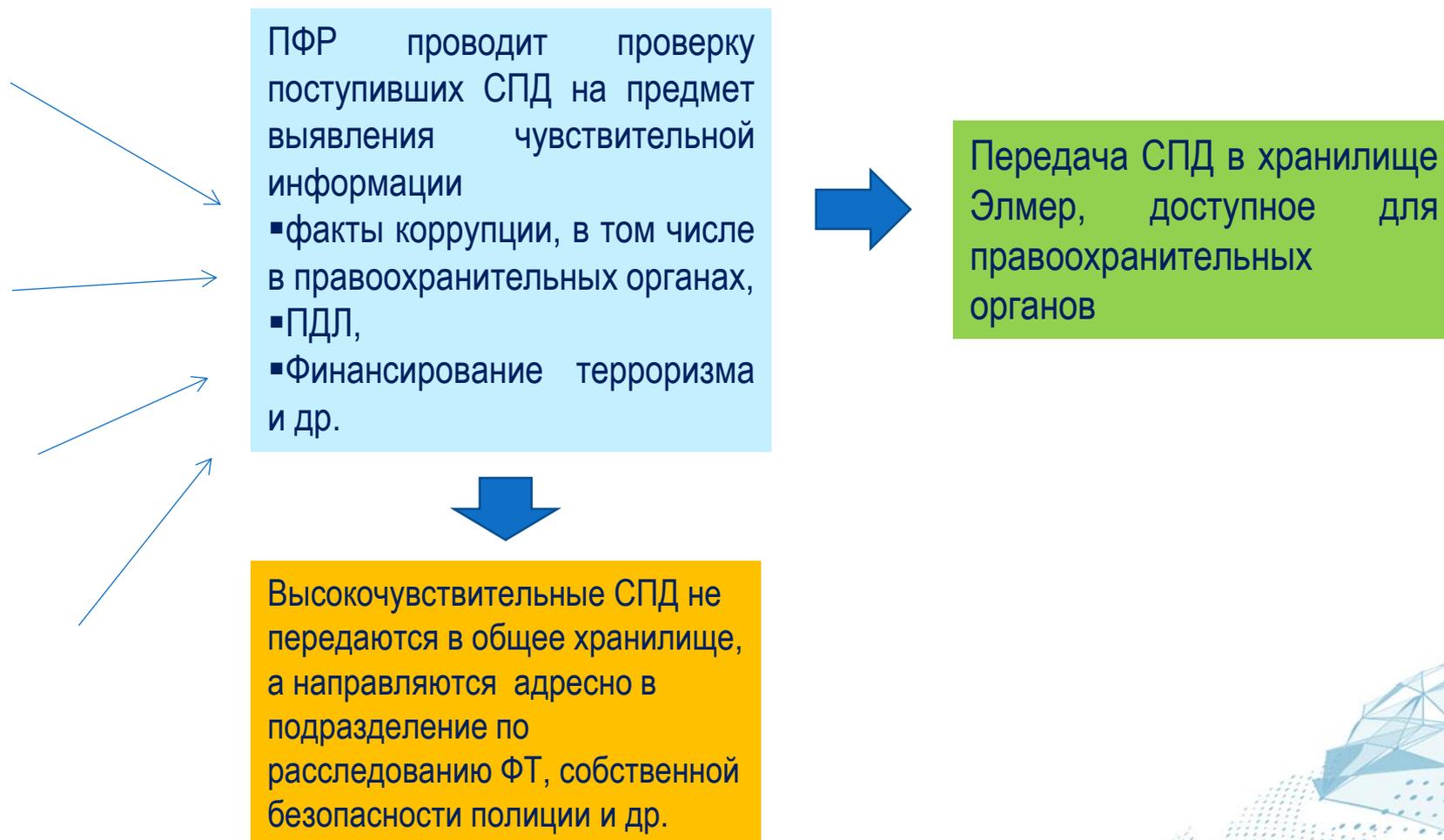
Самый простой способ представить СПД – через безопасную систему SAR Online, бесплатный сервис обеспечивающий мгновенное подтверждение приемки СПД. Отчеты можно направить в режиме 24/7. SAR Online может быть доступен с домашней страницы сайта NCA - www.nationalcrimeagency.gov.uk

ПФР Великобритании

Распределенная модель анализа СПД



Жизненный путь СПД в Великобритании



ПФР Великобритании

United Kingdom Financial Intelligence Unit (UKFIU)



Suspicious Activity Reports (SARs) Annual Report 2018

- Заявление директора Национального агентства по борьбе с преступностью о приоритетности вопроса повышения эффективности СПД
- Подробная статистика направленных СПД (в разрезе секторов)
- Мероприятия проводимые ПФР совместно с надзорными органами по повышению эффективности информирования о подозрительных операциях
- Общая статистика использования СПД с указанием эффективности финансовых расследований
- Конкретные примеры полезности СПД для расследований

ПФР Великобритании United Kingdom Financial Intelligence Unit (UKFIU)



Руководство по повышению качества СПД



Guidance on submitting better quality Suspicious Activity Reports (SARs)

This is a United Kingdom Financial Intelligence Unit (UKFIU) product. It is aimed at all reporters of SARs and is produced in line with the National Crime Agency's commitment to share perspectives on the SARs regime.

May 2019
V3.0

Буклет для подотчетных субъектов



SARs Reporter Booklet

July 2019

This is a UK Financial Intelligence Unit (UKFIU) product for reporters of Suspicious Activity Reports, produced in line with the National Crime Agency's commitment to share perspectives on the SARs regime.



Адресная работа с финансовыми институтами:

- **направление писем с благодарностью за предоставленные сведения, которые были использованы при проведении финансовых расследований.**
- **ежеквартальное направление в адрес крупнейших финансовых институтов результатов анализа их СПО.**

■ Совет комплаенс, как механизм обратной связи по направляемому СПО



Федеральная служба
по финансовому мониторингу

Поиск по сайту



О Росфинмониторинге **Деятельность** Гражданам Организациям Государственная служба Контакты Пресс-служба

Главная / Деятельность / Надзорная деятельность / Совет Комплаенс

Совет Комплаенс

Что такое Совет комплаенс?

Совет комплаенс это консультативный орган при Межведомственной комиссии по противодействию легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения (в соответствии с Положением о Совете комплаенс от 06.07.2016 года).

Основная цель создания данного консультативного органа - формирование эффективной «обратной связи» с частным сектором по вопросам информационного обмена.

Аналогичные проекты реализуются и в других странах. Так, Австралийское подразделение финансовой разведки **Аустрак** (Australian Transaction Reports and Analysis Centre) реализует проект оперативного взаимодействия с банками **Финтел Альянс** (Fintel Alliance), включающий помимо банков и систем перевода денег Western Union и Pay Pal также федеральную полицию и налоговую службу. Помимо оперативной составляющей Финтел Альянс работает над инновациями в сфере ПОД/ФТ и управления рисками новых финансовых технологий (блокчейн, криптовалюты).

В Великобритании реализуется аналогичный, но с большим акцентом на правоохранительную составляющую проект **Джимлет** (JMLIT), организованный по инициативе Национального криминального агентства объединяющий представителей крупнейших банков, Британской банковской ассоциации, регулятивных органов, а также представителей научного сообщества. Работа Джимлет основана на модели экспертных групп, каждая из которых работает по определенной тематике, например, по борьбе с коррупцией. Банкам-участникам предоставляется расширенный доступ к информации, аккумулируемой финразведкой, при этом участники несут обязательства по неразглашению конфиденциальных сведений.

В настоящее время Совет комплаенс объединяет представителей крупнейших финансовых институтов и так называемых установленных нефинансовых предприятий и профессий. Помимо обмена информацией о новых рисках, выработке критериев о подозрительных операциях Совет комплаенс занимается вопросами совершенствования СПО, информационного обмена. Такого рода адресное взаимодействие с организациями, которые по сути генерируют основной объем информации позволяет влиять на параметры качества информационного потока.

Одним из приоритетных направлений деятельности Совета комплаенс является разработка критериев и моделей финансового поведения преступников в целях повышения эффективности и оперативности выявления операций, сопряженных с соответствующими рисками (в соответствии с Концепцией работы Совета комплаенс).

Стратегическая
цель:

Повышение качества СПО на основе риск-ориентированного подхода

Надзорная деятельность

Результаты проверок

Результаты анализа и обобщения правоприменительной практики контрольно-надзорной деятельности

Совет Комплаенс

Взаимодействие и координация

Международное сотрудничество

Государственные закупки

Информационные системы

Административные регламенты

Показатели деятельности и отчеты об их исполнении

Результаты проверок

Использование бюджетных средств

Федеральные целевые и государственные программы

Годовые отчеты

Государственные услуги

Сведения о признании судом недействующими нормативных правовых актов Росфинмониторинга

Судебный и административный порядок обжалования нормативных правовых актов, решений, действий (бездействия) Росфинмониторинга, его территориальных органов и их должностных лиц

В режиме видеоконференцсвязи принимают участие региональные советы, созданные на площадках Межрегиональных управлений. В общей сложности Совет объединяет более 100 участников – ведущих экспертов руководителей подразделений внутреннего контроля организаций.



Ли Ольга Хен-Дюновна (Нижегород),
Начальник отдела финансового мониторинга, ПАО «НБД-Банк»

«Считаем создание Совета комплаенс, как консультативного экспертного органа, важным мероприятием, благодаря которому мы получили полезную площадку с широким и представительным кругом участников для обсуждения актуальных вопросов в области ПОД/ФТ, имеем возможность ознакомиться с передовыми практиками организации системы внутреннего контроля в финансовых организациях...»



Лопатко Андрей Борисович (Москва)
Первый вице-президент
Начальник Управления финансового мониторинга АО ЮниКредит Банк

“Создание Совета Комплаенс в нашей сфере можно сравнить с долгожданной встречей “живую” людей после длительного общения “по переплюске”. Гораздо эффективнее, быстрее и понятнее можно донести и обсудить взаимные вопросы, вместе работать над повышением эффективности системы ПОД/ФТ. На данной площадке собрались специалисты не только из финансовой, но и из телекоммуникационной и других отраслей, что позволяет создавать максимально продуманные и реалистичные решения, учитывающие коллективный опыт и точку зрения...”



Марасеева Наталья Владимировна (Москва)
Руководитель Службы риск-менеджмент и комплаенс ПАО «ТрансФин-М», член Правления

«Совет комплаенс предоставляет уникальные возможности коммуникаций с российскими и зарубежными экспертами в сфере ПОД/ФТ. Обмен опытом и лучшими практиками позволяет нам внедрять новые эффективные подходы в комплаенс нашей компании...»



Использование Личного кабинета на сайте Росфинмониторинга

- доведение типологий ОД/ФТ и секторальных оценок рисков до всех субъектов ПОД/ФТ и надзорных органов.
- доведение аналитических отчетов о результатах направления СПО определенным сектором и проблемных вопросах информированного взаимодействия.
- доведение индекса качества информационного потока.

Обратная связь с финансовыми институтами через Личный кабинет на сайте Росфинмониторинга



Качество информационного взаимодействия



Банк России

**АКТУАЛЬНЫЕ ВОПРОСЫ
РЕАБИЛИТАЦИИ БИЗНЕСА, ЕСЛИ
ФИНАНСОВЫЕ ОРГАНИЗАЦИИ
ОТКАЗЫВАЮТ В ПРОВЕДЕНИИ
ОПЕРАЦИИ ИЛИ В ЗАКЛЮЧЕНИИ
ДОГОВОРА БАНКОВСКОГО СЧЕТА
(ВКЛАДА)**

2019 год





Федеральный закон № 115-ФЗ: инструменты пресечения подозрительных операций



отказ от проведения операции



отказ от заключения договора банковского счета (вклада)



решение о расторжении договора банковского счета (вклада)

Целями создания межведомственной комиссии являются:



- внесудебный порядок защиты прав клиентов



- всестороннее и полное исследование обстоятельств, изложенных в обращении клиента



- снижение напряженности в процессах применения противозаконных мер

Взаимодействие с кредитной организацией в целях реабилитации



1. Убедиться в характере ограничительных действий КО



2. Обратиться в КО за разъяснениями о причинах отказа (при необходимости)



3. Представить в КО документы и (или) сведения об отсутствии оснований для принятия решения об отказе

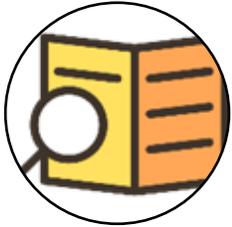


4. Получить от КО сообщение об устранении оснований для отказа либо о невозможности устранения оснований



5. В случае получения сообщения о невозможности устранения оснований для отказа – обратиться с заявлением в межведомственную комиссию при Банке России

Процесс функционирования межведомственной комиссии



Взаимодействие с межведомственной комиссией



Причины отказа от рассмотрения обращения в межведомственной комиссии



Принятие решения межведомственной комиссией и уведомление заявителя и финансовой организации

- если решение положительное

- если решение отрицательное

ПОД/ФТ и реабилитация клиентов: инструкции и практические советы для предпринимателей:

Рабочей группой, в которую вошли представители Банка России, Торгово-промышленной палаты РФ, общественных объединений «Деловая Россия» и «ОПОРА РОССИИ», Агентства стратегических инициатив, разработаны методические рекомендации, которые помогут предпринимателям разобраться в причинах отказах от проведения операций и заключения договора банковского счета кредитными организациями по закону о ПОД/ФТ





Банк России

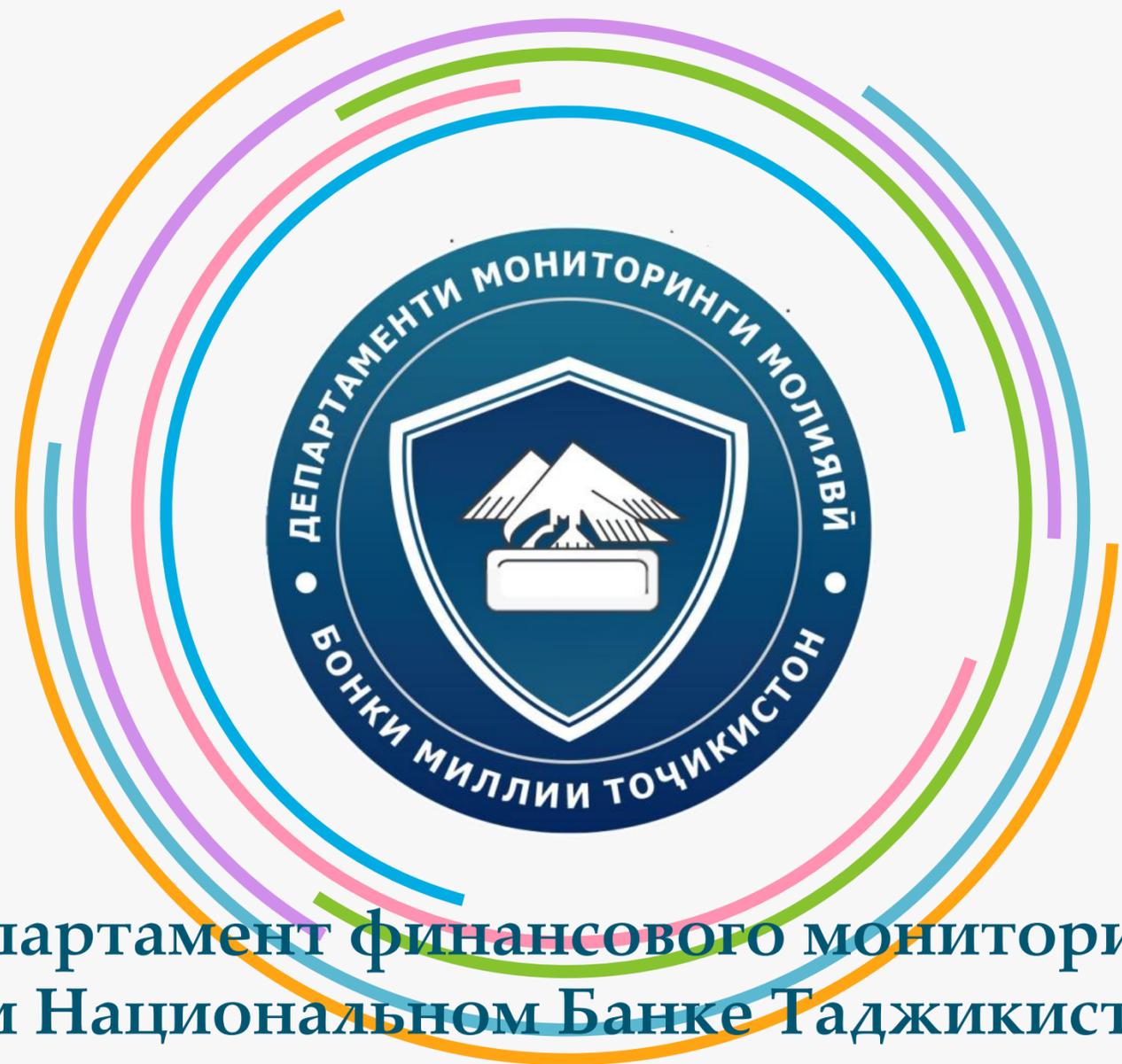
СПАСИБО ЗА ВНИМАНИЕ!

**Начальник Управления финансового мониторинга и валютного контроля
Волго-Вятского ГУ Банка России
Е.В. Лещева**

**Контактные
данные** **тел.: 8 (831) 438-18-60
с 9:00 до 18:00 (MSK)**

**Электронная
почта** **22gupost@cbr.ru**

ВВГУ Банка России
2019 год



Департамент финансового мониторинга
при Национальном Банке Таджикистана

Обязательства подотчетных организаций, согласно Порядку о проведении мероприятий по замораживанию и размораживанию финансовых средств или иного имущества физических лиц и организаций, включенных в список лиц, связанных с терроризмом №129 от 29.03.2019 :

Назначает ответственного сотрудника, а также сотрудника, заменяющего его в период его отсутствия.

При установлении деловых отношений с физическим или юридическим лицом и при осуществлении операции/сделки проверяют наличие или отсутствие лиц в списках

Замораживает средства лиц, включенных в перечни террористов

ПОДОТЧЕТНЫЕ ОРГАНИЗАЦИИ ОБЯЗАНЫ:



Департамент финансового
мониторинга

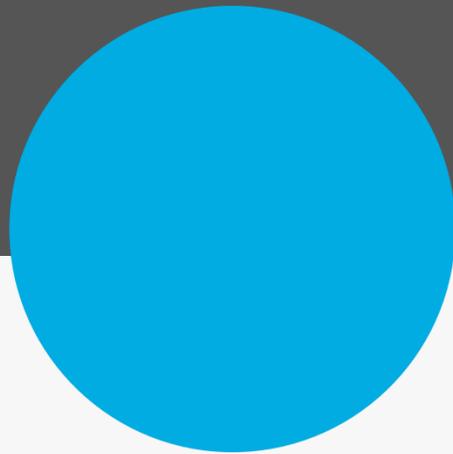


Подотчетные
организации



Государственный комитет
Национальной безопасности

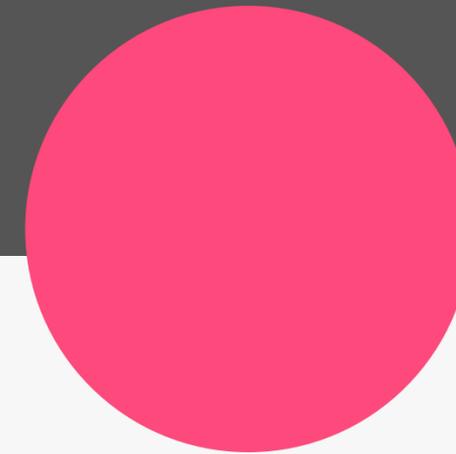
В перечень Республики Таджикистан входят следующие списки:



Объединенный
СПИСОК



Международный
СПИСОК



Национальный
СПИСОК



ИНФОРМАЦИОННАЯ СТРАНИЦА ДЕПАРТАМЕНТА ФИНАНСОВОГО МОНИТОРИНГА НАЦИОНАЛЬНОГО БАНКА ТАДЖИКИСТАНА

Содержание
Главная страница
Законы и другие нормативно-правовые акты
Рекомендации ФАТФ и международные нормативно-правовые акты
Консультации ФАТФ
Руководящие принципы резолюций Совета Безопасности ООН для частного сектора
Взаимодействие по правовым актам, международным стандартам и принципам с финансовыми институтами и УНФПП
Перечни террористов и экстремистов
Типологическое исследование
Годовой отчёт:
за 2010-2011 г.
за 2012 г.
за 2013 г.

Новости

24.08.2018 **В перечень утверждённый резолюцией СБ ООН внесены изменения**

Комитет учреждённый на основании резолюций Совета Безопасности ООН 1267/1989/2253 утвердил изменения в перечень лиц и учреждений связанных с ИГИЛ (ДАИШ) и "Аль-Каиды"

15.08.2018 **Семинар на тему ПОД/ФТ/ФРОМП для некоммерческих организаций**

14 августа 2018 года в здании Министерства юстиции РТ Департамент финансового мониторинга и Министерство юстиции РТ провели совместный семинар с участием представителей некоммерческих организаций на тему «Противодействие легализации доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового поражения».

13.08.2018 **В перечень утверждённый резолюцией СБ ООН внесены изменения**

Комитет учреждённый на основании резолюций Совета Безопасности ООН 1267/1989/2253 утвердил изменения в перечень лиц и учреждений связанных с ИГИЛ (ДАИШ) и "Аль-Каиды"

09.08.2018 **Проведение семинара для адвокатов и государственных нотариусов по тематике ПОД/ФТ/ФРОМП**

По инициативе Департамента финансового мониторинга 7 августа 2018 года в Национальном банке Таджикистана состоялся семинар для Союза адвокатов РТ, адвокатов и государственных нотариусов по тематике "Противодействие легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового поражения" (ПОД/ФТ/ФРОМП).

06.08.2018 **Очередное заседание постоянно действующей межведомственной Комиссии по вопросам ПОД/ФТ/ФРОМУ**

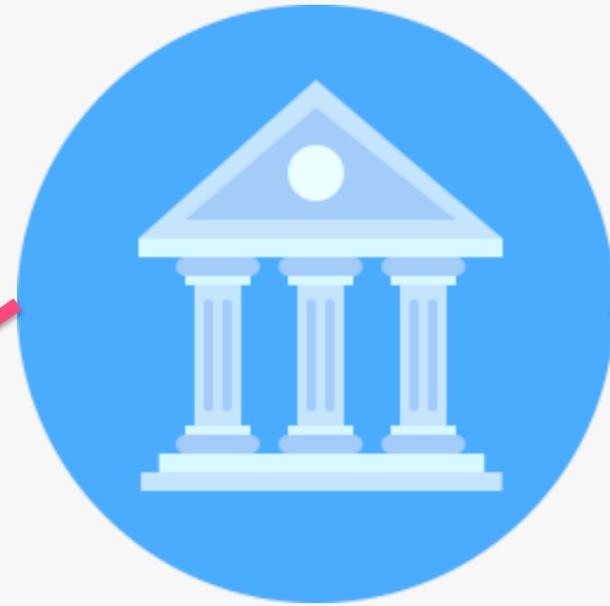
3 августа 2018 г. в Национальном банке Таджикистана состоялось очередное заседание постоянно действующей межведомственной Комиссии (Комиссия) по вопросам противодействия легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения (ПОД/ФТ/ФРОМУ) под руководством Помощника Президента Республики Таджикистан по правовым вопросам г-на



Замораживание активов террористов на территории Республики Таджикистан



Департамент финансового
мониторинга



Подотчетные
организации



Государственный комитет по
Национальной безопасности

Подотчётные организации, не выполняющие или не надлежащим образом выполняющие настоящий Порядок, несут ответственность в порядке установленном законодательством РТ.

(пункт 59 Порядка №129).



Взаимная заморозка с Российской Федерацией



**Департамент
финансового
мониторинга**

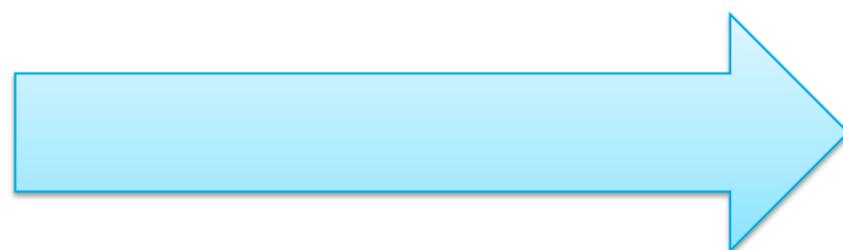


**Федеральная
служба по
финансовому
мониторингу**

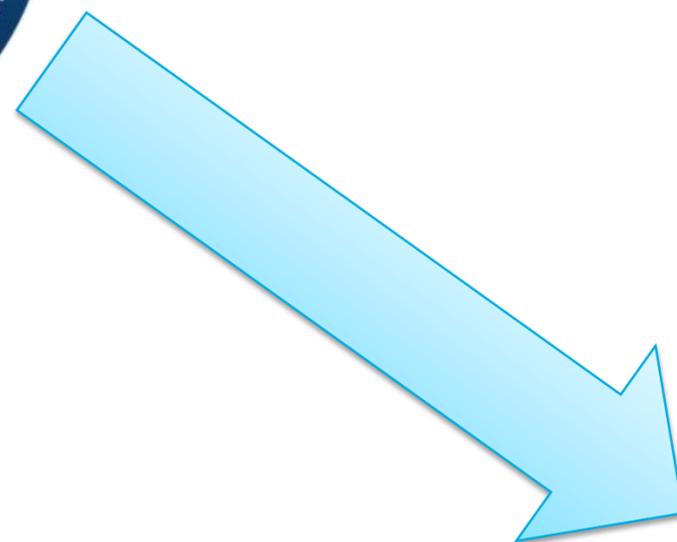
Взаимная заморозка с Российской Федерацией



Департамент
финансового
мониторинга



Принятие решения о заморозке средств
или иного имущества лиц из
Национального списка Российской
Федерации



Направление соответствующего запроса
в подотчетные организации

Взаимная заморозка с Российской Федерацией



Межведомственной комиссии по противодействию финансированию терроризма были заморожены/блокированы активы лиц из Национального списка Республики Таджикистан

В итоге на территории Российской Федерации были заморожены/блокированы 240 банковских счетов 163 лиц из Национального списка Республики Таджикистан



Спасибо за
внимание!



Профилирование участников
криптовалютной среды с целью выявления
криминогенного поведения.
Риски для криптовалютных провайдеров
и традиционного частного сектора и
способы мониторинга.

май 2019



Текущие риски

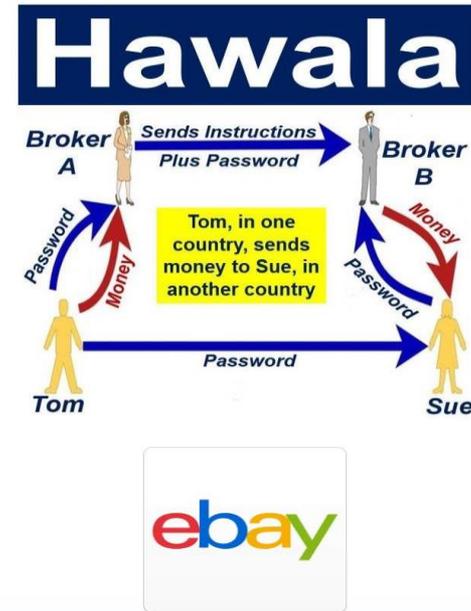
- Финансирование незаконного оборота наркотиков
- Риск перевода внешнеэкономической деятельности в тень с целью ухода от уплаты налогов и таможенных пошлин
- Вывод средств за границу с целью легализации доходов полученных преступных путем
- «Мультипликатор» теневого оборота наличных денежных средств
- Финансирование киберспреступности





Возможные риски в будущем

- Увеличение существующих и появление новых угроз в кредитно-финансовой сфере в связи появлением новых технологий оборота финансовых инструментов
- Хавала – Hi-tech
- Существенное контрпродуктивное влияние на национальные экономики за счет увеличения криптовалютной денежной массы
- Переход розничных агрегаторов и маркетплейсов на криптовалютный оборот





Основные уязвимые места

- Отсутствие контроля регуляторов AML на организованных площадках обмена криптовалют на фиат и криптовалют между собой.
- Отсутствие контроля за регулярным частным обменом наличных на криптовалюты
- Отсутствие возможности учета криптовалют для финансирования внешнеэкономической длительности и контроля этих финансовых потоков





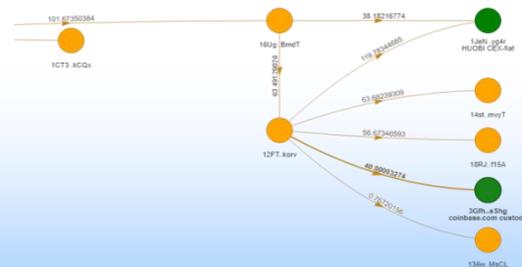
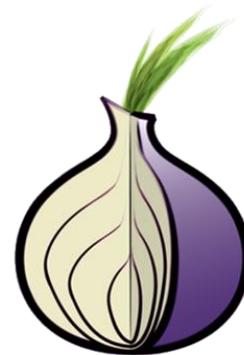
Источники информации для профилирования

- Интернет среда, публикации в интернет, раскрытие информации участниками криптовалютной деятельности площадками, корпоративные сайты
- Официальные документы о регистрации и получение лицензий в официальных органах регистрации деятельности различных юрисдикций
- Характер транзакций по адресам, которыми распоряжается субъект криптовалютной деятельности, анализ контрагентов.



Методы мониторинга

- Сканирование Internet и Darknet среды на предмет публикаций, объявлений и обмена информации
- Запрос официальных регистрационных документов и лицензий подтверждающих деятельность
- Сканирование и анализ криптовалютных транзакций и сопоставление типовыми примерами





Группы профилей участников криптовалютной среды

- Поднадзорные участники криптовалютной среды

- Биржи СЕХ
- Платежные системы
- Обменные пункты
- Майнинг пулы

- Пользователи криптовалютной среды

- Инвесторы
- Майнеры
- Торговые точки

- Криминогенная среда и среда повышенного риска

- DarkMarkets
- Миксеры
- Пирамиды
- Malware
- Киберпреступность



FATF рекомендации

- VASPs должны предоставлять друг другу следующие данные :
 - имя отправителя и данные о его цифровом кошельке;
 - имя получателя и данные о его цифровом кошельке;
 - физический адрес отправителя, его паспортные данные или пользовательский идентификатор, которые привязывает его к компании, дате или месту рождения.
- Делистинг анонимных криптовалют



Гибридность деятельности большинства участников

- Circle
 - Трансграничная платежная система
 - Обмен валюты через карточки
 - Одна из крупнейших ОТС площадок
- Coinbase
 - Хранилище биткоинов – веб кошелек
 - Обменный пункт
- XAPO
 - Хранилище биткоинов – веб кошелек
 - Обменный пункт



Направления работы с участниками финансовой инфраструктуры с целью ПОД/ФТ





Работа ПОД/ФТ с криптовалютными биржами, агрегаторами и платежными системами использующими криптовалюты

- ◎ Контроль за наличием процедур AML KYC
- ◎ Анализ объема трафика с «токсичных» объектов в сети
- ◎ Реакция биржи на токсичные объекты



Работа с банками с целью ПОД/ФТ

- ◎ Деаннонимизация транзакция и проведение соответствие банковских транзакций в случае частных сделок по купле продажи криптовалюты
- ◎ Приведение в соответствие транзакций по кредитным картам и транзакций в блокчейне
- ◎ Контроль за взаимодействие с «токсичными» объектами



Выявление нелегальных объектов и расчетов на черном рынке

- Выявление черных рынков
- Установление взаимосвязей
- **Проведение работы по пресечению операций**



КYT (Know Your Transaction) Решение знай свою транзакцию

- ⦿ Автоматизация мониторинга входящих и исходящих потоков криптовалюты, с автоматическим уведомлением в случае превышения параметра риска

Оценка риска

Наивысший риск (Входы) ☐ -

Средневзвешенный риск: 50

Показывать по Поиск:



Что такое адрес в биктоин

[English](#) | [Français](#) | [German](#) | [Dutch](#) | [Português](#) | [Русский](#) | [Spanish](#) | [Italiano](#) | [Українська](#) | [Türk](#) | [Polski](#) | [中文](#)



WalletGenerator.net

Universal Open Source Client-Side Wallet Generator

Выберите валюту :

[Единичный кошелек](#)

[Бумажный кошелек](#)

[Несколько кошельков](#)

["Умственный" кошелек](#)

[Подробности о кошельке](#)

[Поддержка](#)

[Generate New Address](#)

[Print](#)

Открытый адрес



ОТКРЫТЫЙ

1DtgrfyfNMy1q8JSSjyExSV4o51UNEAAMN

Закрытый ключ (в формате импорта в кошелек - WIF)



СЕКРЕТНЫЙ

5Jcj3odVLZAuaCMCft6Gx57TrhbbvFLvUFgoHx4q1NrKivzZ6BE



Что такое кошелек в биткоин

Electrum 2.6.4 - wallet_2

Файл Кошелек Инструменты Помощь

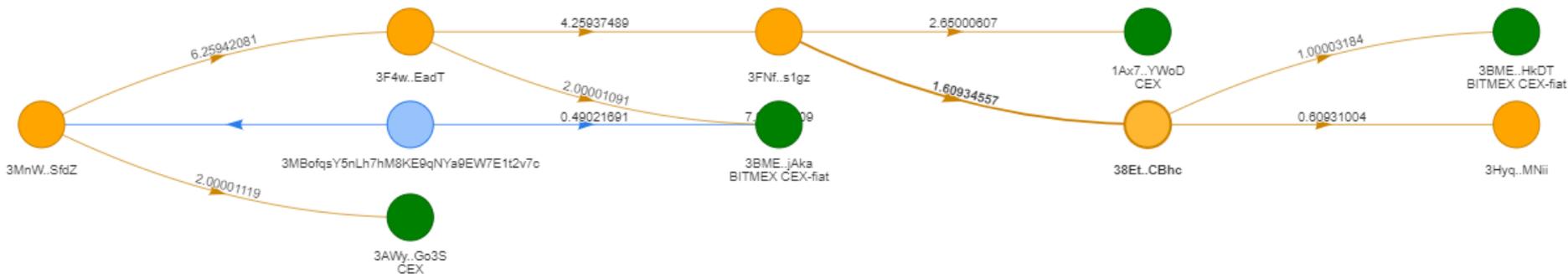
История Отправка Получение Адреса Контакты Консоль

Адрес	Метка	Баланс	Транзакции
Получение			
Потрачено			
17AyPVXxC36zFPehEXxB8UBqzwFYAkrGx8		0,	0
13tFdEaX9Sd59citgaXzzJJb4CLEUbTVFo		0,	0
1NuTShwiq3qHhdSbGgToAjHN5MugpFqw1y		0,	0
1PZgreuAxKi4CGN34J9z1ZpWAFy41ChLai		0,	0
1AmoyM8hHebDjiJght6Haf6jgkT22KSSBD		0,	0
19KpQ2vXUimANKgVvYJRR8GhxtRSMfUEwS		0,	0
16SEaJfqVFvHZHuUK4QLzgvKWRZNZY55fx		0,	0
1KEWLzCzifThpgycPs3iLZSSumRdtPyxU7		0,	0
1KgcPudBtYJt7UrZSZBGvzY4Q8ubuJ3hvw		0,	0
16ABQnEkjn16Enio6QeAe94FruFvH1XbXA		0,	0
1ECgFHYr8YJDxfz2NV9NfqUGaoAf4Avnan		0,	0
125CGQZaCcn5pxNtmtAh9FosSTgRgkomhY		0,	0
19VBY8W8iaqXutbfkCirFLg1NGg9RSCnQ		0,	0
1MZ9T2spRhLR1znhUifxaL3JRwPXKCYRHc		0,	0
1MNYLB8eZUsin8gTamxeNA8DXK2HSxQJGY		0,	0
16zyQuKKJ26qy9j63t19SDs5xq6mwTAgGW		0,	0
1dZx4PArxN7Ggrt9qSW7dUavn3QPUnonA		0,	0
13zqAkApv5et45SLZLjXWhxfgoyfA9tbp7		0,	0
19BKGewcbqufnmuPX7dYpzR4T1hYsLbZ45		0,	0
1H17FgsyWf67JmeJ3LBWnHc9nCExFVNjAw		0,	0
Сдача			

Баланс: 0, BTC (0.00 USD) 1 BTC~611.88 USD



Отслеживается с помощью функции трейсинга по основным средствам





Композиция аналитических данных



Преступность и
криптовалюты носят
глобальный характер





Международной сотрудничество для решения следующих задач



Обмен информацией по криминальным операторам и средствам



Противодействие средствам сокрытия



Обмен информацией по операторам услуг для криптовалютных активов



Спасибо за внимание!

Алексей Юров

**Главный специалист ФИАН
исследования блокчейн**



Currency.com

***Практика применения мер ПОД/ФТ
оператором криптоплатформы в
Республике Беларусь.***

***Перспективы развития регулирования
данных мер***

Общие сведения об ООО «Карренси Ком Бел» и проекте «Currency Com»

ООО «Карренси Ком Бел» – коммерческая организация, созданная в Республике Беларусь для реализации **инвестиционного проекта «Currency.com»** (резидент Парка высоких технологий).

«Currency.com» – **международный проект**, основанный на применении **технологий распределенного реестра (блокчейна)** и использовании **криптовалют и других токенов**.

Проект **«Currency.com»** состоит в **создании и коммерциализации программного обеспечения**, предназначенного для **осуществления инвестиций посредством совершения сделок с токенами**.

При реализации проекта **«Currency.com»** ООО «Карренси Ком Бел» **создает и размещает собственные токены** (на блокчейне Ethereum), а также **планирует оказывать услуги по организации ICO** (создание и размещение токенов) для других лиц.



ПВТ – среда для организованного рынка токенов

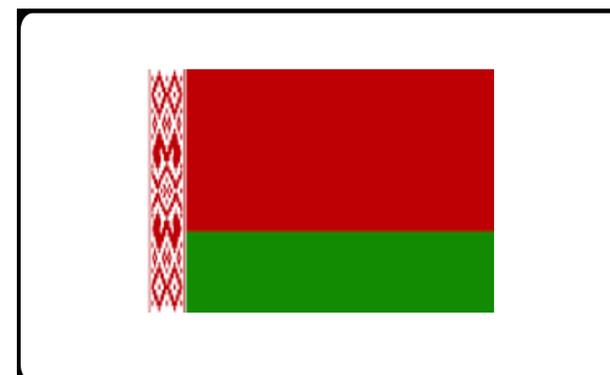


«Центр тяжести» проекта «Currency.com» приходится на белорусскую юрисдикцию, в которой создано качественное, всеобъемлющее и либеральное регулирование обращения токенов, основу которого составляют:

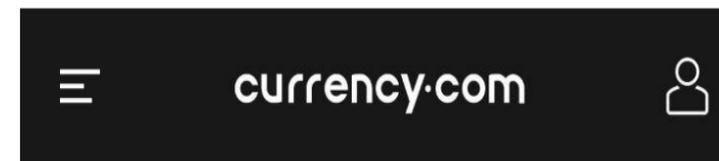
- Декрет Президента Республики Беларусь от 21.12.2017 № 8 «О развитии цифровой экономики»;
- акты Наблюдательного совета Парка высоких технологий.

Парк высоких технологий (ПВТ) – среда для функционирования организованного рынка токенов.

«Профессиональные» участники рынка токенов должны быть зарегистрированы в качестве резидентов ПВТ.



14:40      85 %



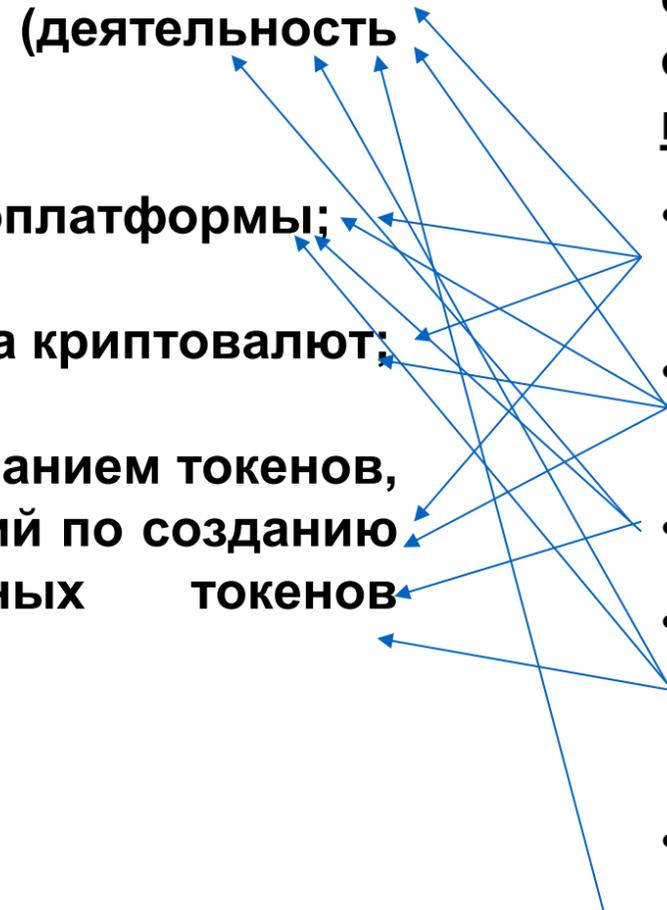
1. Общество с ограниченной ответственностью «Карренси Ком Бел» (УНП 193130368) расположено по адресу: 220030, г.Минск, ул. Интернациональная, 36-1, офис 724, помещение 2.
2. ООО «Карренси Ком Бел» является резидентом Парка высоких технологий (решение о регистрации в качестве резидента Парка высоких технологий, протокол №08/НС-6пр от 19 декабря 2018 г.) и осуществляет свою деятельность в соответствии с Декретом Президента Республики Беларусь от 21 декабря 2017 г. № 8



ПВТ – среда для организованного рынка токенов

Виды деятельности профессиональных участников рынка токенов в ПВТ:

1. оказание услуг, связанных с созданием и размещением токенов организатора ICO);
2. деятельность оператора криптоплатформы;
3. деятельность оператора обмена криптовалютой;
4. иная деятельность с использованием токенов, а также осуществление операций по созданию и размещению собственных токенов (проведение собственного ICO).



Определение провайдера услуг в сфере виртуальных активов в Рекомендациях ФАТФ:

любое физическое или юридическое лицо, которое осуществляет в качестве предпринимательской деятельности один или более из следующих видов деятельности или операций для или от имени другого физического или юридического лица:

- обмен между виртуальными активами и фиатными валютами (купля-продажа); 1, 2, 3, 4
- обмен между одной или более формами виртуальных активов; 1, 2, 3, 4
- перевод виртуальных активов (от имени других лиц); 1, 2, 4
- хранение и/или администрирование виртуальных активов или инструментов, позволяющих осуществлять контроль над виртуальными активами; 1, 2, 4
- участие в и предоставлении финансовых услуг, связанных с предложением выпускающего лица и/или продажей виртуального актива. 1

ООО «Карренси Ком Бел»
осуществляет виды
деятельности №№ 1, 2, 4



Создание ПОД/ФТ регулирования в рамках ПВТ

ПОД/ФТ регулирование предусмотрено в Положении о требованиях к правилам внутреннего контроля резидентов Парка высоких технологий, утвержденном решением Наблюдательного совета ПВТ от 23 октября 2018 г. (протокол №08/НС-5пр).

За образец (шаблон) взяты требования к правилам внутреннего контроля **форекс-компаний**, установленные Правлением Национального банка Республики Беларусь. **Анализировался имевшийся зарубежный опыт.**

- AML/CFT Guidance for Virtual Currencies prepared by **Isle of Man** Gambling Supervision Commission in 2017;
- Consultation paper «Regulating digital currencies under Australia's AML/CTF regime» prepared by the Attorney-General's Department of the **Australian** Government 2016;
- **FATF** Guidance for a Risk-based approach to virtual currencies of June 2015;
- Tracfin (**France**) recommendations to prevent virtual currencies from being used for fraudulent purposes and money laundering «Regulating virtual currencies» 2014;
- **FinCEN** Guidance «Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies» 2013;
- Regulations of the Superintendent of Financial Services: Virtual Currencies. Adopted by the **New York** State Department of Financial Services.

Заимствованы **меры ПОД/ФТ, практикуемые применительно к сделкам с токенами**, в том числе:

- о таких способах верификации идентификационных данных, как получение данных о клиенте **из коммерческих баз данных** (World-Check, Accuity, Dow Jones и других); отслеживание адрес **интернет-протокола клиента**; применение **web-ID** при совершении сделки на определенную сумму;
- о таких признаках подозрительных финансовых операций, как использование клиентом при передаче токенов «anonymiser software», «IP mixers», «coin mixers», иных **программ-анонимайзеров** (в т.ч. виртуальных кошельков, которые исключают возможность отслеживания операций, например, Dark Wallet); использование для совершения финансовой операции адреса виртуального кошелька, примененного площадках «**Silk Road**», «**AlphaBay**», «**Hansa**», «**Dream Market**», «**CGMC**» и т.п.;
- об использовании программных решений для **анализа транзакций в блокчейне** (Elliptic, Chainalysis, Coinfirm и др.);
- об исключении работы с токенами, основанными на принципе **полной анонимизации** совершаемых с ними сделок (Dash и т.п.);
- о проведении **независимого тестирования (оценки)** правил внутреннего контроля.



Требования к деятельности резидентов ПВТ в части ПОД/ФТ (требования к правилам внутреннего контроля)



Порядок управления рисками, связанными с отмыванием денег и финансированием терроризма (трехвекторная модель: 1. риск по профилю клиента; 2. риск по географическому региону; 3. риск по видам операций)

Идентификация и верификация всех клиентов, осуществляющих финансовые операции

AML compliance officer
(соответствующее образование, опыт работы по экономической или юридической специальности, AML подготовка)

Отказ в совершении операции (в отношении анонимных токенов, токенов на сумму, превышающую 2000 б.в., если расчет осуществляется не посредством банковского перевода или перевода электронных денег, и др.)

AML / KYC

ПО по мониторингу проведения транзакций и определению связанных с преступной деятельностью переводов (программные решения Elliptic, Chainalysis, Coinfirm и др.)

Возможность замораживания средств и (или) блокирования финансовых операций лиц, причастных к террористической деятельности

Направление специальных формуляров в орган финансового мониторинга (при отнесении финансовых операций к операциям особого контроля, замораживании средств или блокировании финансовой операции)

Выявление финансовых операций, подлежащих особому контролю (соотнесение каждой операции с критериями и признаками подозрительных финансовых операций)

Развитие ПОД/ФТ регулирования применительно к резидентам ПВТ

1. Обеспечение реализации **Interpretive Note to Recommendation 15 on New Technologies** и **Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers of 21 June 2019** в полном объеме.
2. Предусмотреть право резидентов ПВТ **использовать иностранные системы идентификации** (digital ID, например, GBG, England), не противоречащие Рекомендациям ФАТФ.

Система идентификации – совокупность банков данных, информационных технологий и программно-технических средств, предназначенных для сбора, обработки, хранения и представления данных о клиентах, их представителях в целях их идентификации, и позволяющая получить идентификационные данные клиентов без получения от клиентов содержащих эти данные документов (их копий, изображений).

3. Предусмотреть право резидентов ПВТ применять расширенный перечень документов, которые могут выступать источником идентификационных данных – в дополнение к документу, удостоверяющему личность – дописать указание на **водительское удостоверение** (иной аналогичный документ), **удостоверение избирателя, карту налогоплательщика, карту трудоустройства**, выдаваемые в стране, гражданином которой является идентифицируемое физическое лицо, и (или) в стране, где оно постоянно проживает.

Согласно Рекомендации ФАТФ № 11 к документам, на основании которых должна проводиться идентификация клиентов, помимо паспорта, также относятся и такие официальные идентификационные (удостоверяющие) документы как *идентификационные карты, водительские права или иные аналогичные документы*.

4. Предусмотреть право резидентов ПВТ **завершить идентификацию клиентов после установления договорных отношений с ними**.

Развитие ПОД/ФТ регулирования: отсрочка завершения идентификации

Предлагается предоставить резидентам ПВТ, осуществляющим виды деятельности с токенами, право **завершить проверку (идентификацию) клиентов в течение 15 дней после установления с ними отношений либо до передачи клиентам («вывода» ими) средств, если они обращаются за ней (за ним) до истечения этого срока.**

Опыт реализации: Кипр (с. 3 Циркуляра CySEC 24.06.2016 № C157), а также Мальта и Литва.

Рекомендация ФАТФ № 10:

«Страны могут разрешить финансовым учреждениям завершить проверку клиентов в разумно сжатые сроки после установления деловых отношений в том случае, если **риски отмывания доходов и финансирования терроризма практически сведены к минимуму** и если это крайне важно для бесперебойного осуществления нормальной деятельности.».

А) Почему риски отмывания доходов и финансирования терроризма практически сведены к минимуму :
клиент передает средства (например, деньги, токены) резиденту ПВТ, но **до завершения его проверки клиент лишен возможности получить средства на руки («вывести» их) и распорядиться ими по своему усмотрению**, ввиду чего он **никак не сможет отмыть доходы или профинансировать террористов.**

Б) Почему крайне важно для бесперебойного осуществления нормальной деятельности:

Пункт 11 Пояснительной записки к Рекомендации ФАТФ №:

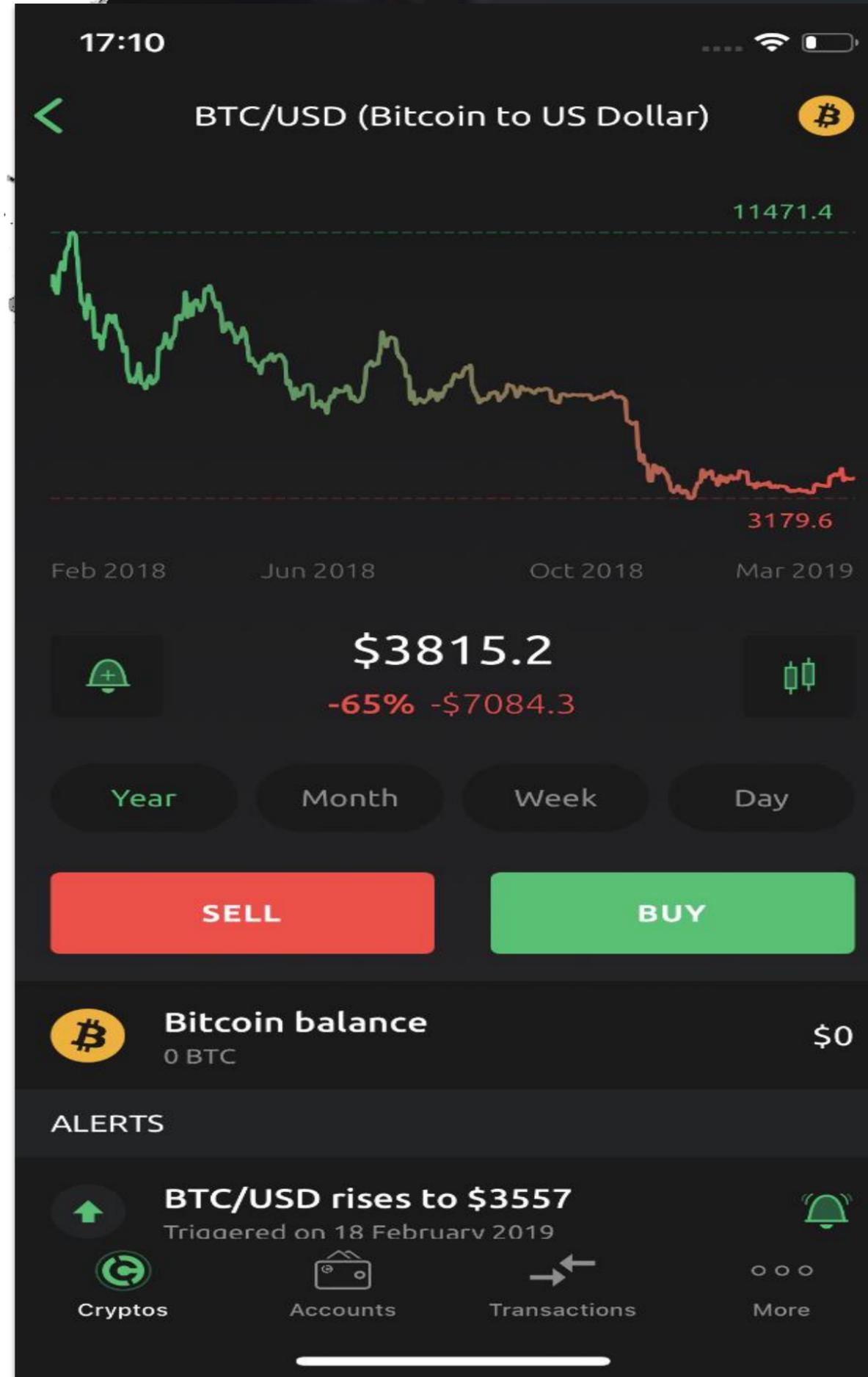
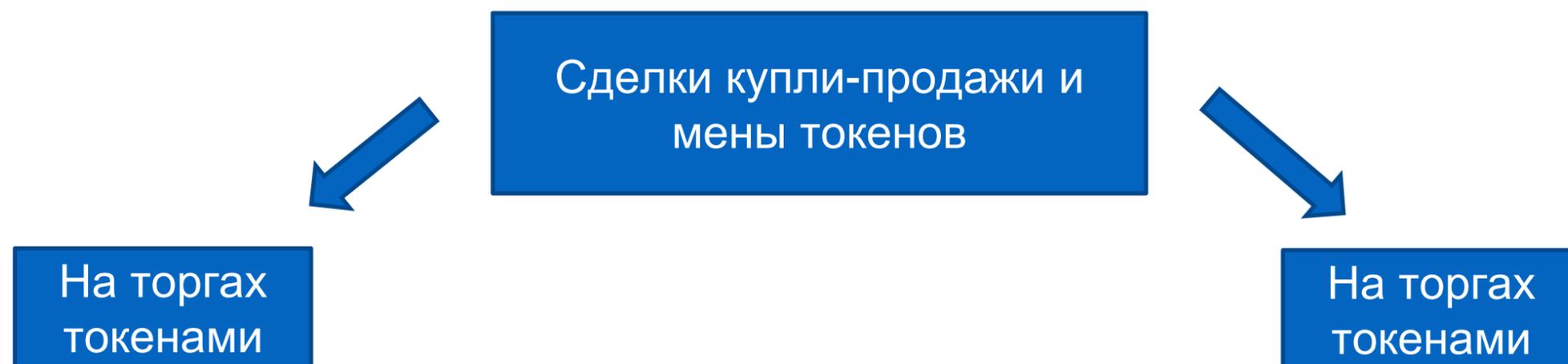
«Примеры типов обстоятельств, при которых было бы допустимо завершать проверку после установления деловых отношений из-за того, что исключение пауз в обычном ведении бизнеса имеет особое значение, включают следующие: **бизнес без присутствия сторон (non face-to-face business)**». При этом резиденты ПВТ, осуществляющие виды деятельности с токенами, всегда работают с клиентами удаленно (т.е. без их личного присутствия).

Основное программное обеспечение проекта «Currencys.com»



1. Криптоплатформа (торговая платформа) «Currencys.com» (криптовиржа);
2. Мобильное приложение «Currencys.com Exchange» (криптовиржа для мобильных устройств);
3. Мобильное приложение «Currencys.com – Купить Bitcoin» (криптообменник для мобильных устройств).

Основную массу сделок, совершаемых с использованием данного программного обеспечения, составляют сделки купли-продажи и мены токенов.



Основное программное обеспечение проекта «Currency.com»



Программное обеспечение ООО «Карренси Ком Бел» позволяет совершать сделки с:

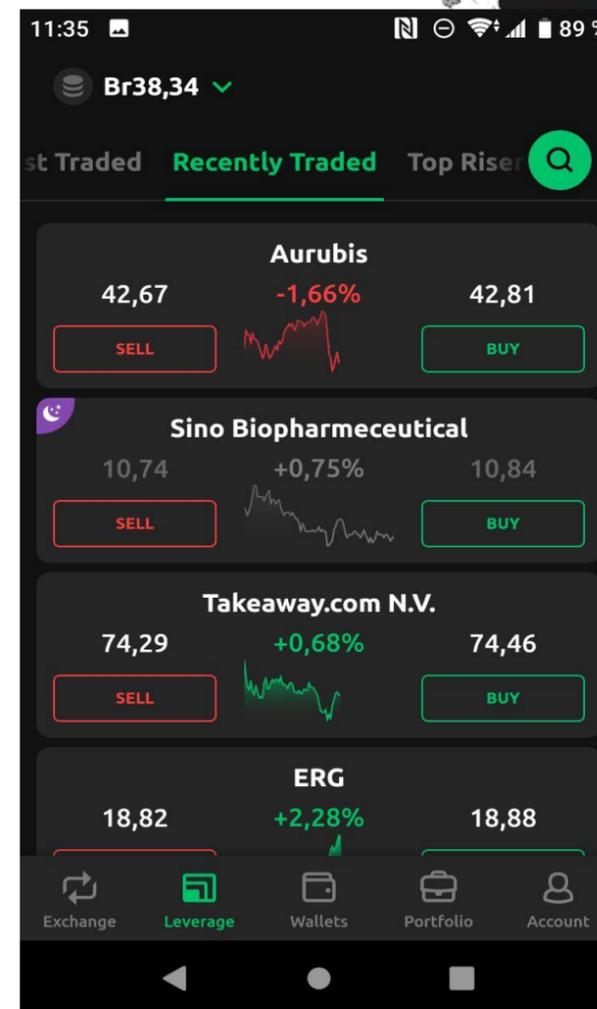
1) криптовалютой:

- Биткоин (Bitcoin);
- Эфириум (Ethereum);
- Лайткоин (Litecoin).



2) собственными токенами ООО «Карренси Ком Бел»:

- токены, репрезентующие валюты;
- токенизированные биржевые активы;
- токенизированные облигации.



Совершая и организуя сделки с токенами, ООО «Карренси Ком Бел» действует по модели централизованной криптоплатформы.

Для обеспечения расчетов по сделкам ООО «Карренси Ком Бел» принимает на свои банковские счета, электронные кошельки, адреса виртуальных кошельков средства клиентов (деньги, электронные деньги, токены).

Система внутреннего контроля ООО «Карренси Ком Бел»

- ***идентификация*** (до установления отношений) ***и верификация*** в отношении всех клиентов;
- ***хранение сведений, содержащих идентификационные данные клиентов*** (в том числе полученных по итогам верификации, обновления (актуализации) этих данных);
- ***мониторинг*** всех финансовых операций клиентов с целью выявления финансовых операций, подлежащих особому контролю, документальное фиксирование таких операций и передача соответствующих сведений в орган финансового мониторинга;
- принятие обоснованных (разумных) и доступных в сложившихся обстоятельствах мер по ***определению источников происхождения*** токенов и средств клиентов.



Управление рисками, связанными с легализацией

- осуществляется с учетом **риск-ориентированного подхода**;
- принимаются меры по определению, классификации, описанию и оценке рисков с учетом факторов риска, влияющих на **повышение (понижение)** степени рисков;
- риск работы с клиентом **оценивается по шкале рисков**, которая состоит из трех степеней (низкая, средняя и высокая);
- используется **трехвекторная модель** распределения рисков, включающая следующие векторы: риск по профилю клиента, риск по географическому региону, риск по видам операций;
- для присвоения работе с клиентом итоговой степени риска используется **матрица** присвоения работе с клиентом итоговой степени риска на основе трехвекторной модели распределения рисков (с использованием балльной шкалы).



Идентификация клиентов

До приема на обслуживание ООО «Карренси Ком Бел» получает от клиентов следующие данные:

- фамилию, собственное имя, отчество (при наличии);
- гражданство;
- дату и место рождения;
- адрес места жительства и (или) пребывания;
- реквизиты документа, удостоверяющего личность;
- сведения о выгодоприобретателе (при наличии таких сведений);
- контактные данные клиента, позволяющие установить с ним связь (адрес электронной почты).

При получении этих данных от физического лица Общество запрашивает от него **уточнение** того, действует ли оно от своего имени и в своих интересах.



Порядок проведения идентификации

1-й этап идентификации:

Клиенту предоставляется для заполнения **электронная регистрационная карта**, размещенная посредством веб-интерфейса.

Заполнение осуществляется на основании документа, удостоверяющего личность (паспорт, идентификационная карта, вид на жительство).

2-й этап идентификации:

Клиент направляет **графические образы** документа, удостоверяющего личность клиента, открытого на страницах, содержащих личные данные и отметку о месте жительства, а если место жительства, отличается от фактического места проживания (или оно не указано), то также и **графические образы** документов, подтверждающих факт проживания (счета на оплату коммунальных услуг и т.п.).



Web-ID

Вместо заполнения клиентом электронной регистрационной карты и для верификации может использоваться процедура web-ID (***форма удаленной идентификации посредством установления видеосвязи с клиентом в сети Интернет***).

Во время процедуры клиенту ***необходимо держать документ, удостоверяющий личность, и иные необходимые документы перед веб-камерой*** для осуществления сравнения лица клиента с фотографией, размещенной в документе, удостоверяющем личность, а также получения (восприятия) данных этого и иных документов, подтверждения достоверности ранее представленных данных.

Процедура web-ID проводится Обществом в обязательном порядке перед совершением сделки купли-продажи токенов на сумму 5000 БВ и более (**приблизительно 61500 USD**)



Обязательные мероприятия

ООО «Карренси Ком Бел» осуществляет **проверку сведений о клиентах (до принятия на обслуживание):**

- с целью отнесения их к **иностранным публичным должностным лицам, должностным лицам публичных международных организаций, лицам, занимающим должности**, включенные в определяемый Президентом Республики Беларусь перечень государственных должностей Республики Беларусь, членам их семей и приближенным к ним лицам;
- с целью отнесения их к **лицам, участвующим в террористической деятельности, причастным к распространению оружия массового поражения либо находящимся под контролем таких лиц** (перечень – на сайте КГБ Республики Беларусь).



Анкетирование

- **Для каждой группы** клиентов (физические лица, индивидуальные предприниматели, юридические лица) разработаны **анкеты клиента** (на основании вопросника идентификации).
- Анкета может быть **стандартной или расширенной формы** (в зависимости от итоговой степени риска работы с клиентом).
- Анкеты заполняются **в электронном виде** посредством программного комплекса **«User admin area»**.



User Admin Area

#10827419 -



10 USD

Type	Name	Curr.	Equity	UPL	Margin	Equity / Margin	Balance	Available for WD
	Total	USD						0.00
No records found								
No records found								

- Details
- Balances
- Positions
- Positions History
- Orders
- Orders History
- Exchange Orders
- Exchange Orders History
- Transactions
- Sessions Log
- Communication

Locale	en	Print
Email		
User Type	RETAIL	
Qualified investor	No	
LTV Category		
Invite Code		
Gender		
First Name		
Mid Name		
Last Name		
Second Surname		
Previous Last Name		
Date of Birth	-	
Country of Birth		
Country of residence	United States Minor Outlying Islands	

Categories: [Edit](#) CAD: [Set](#)

Status

Account status: NEW

License	HTP - NEW
Appropriateness Score	0
Target Market Score	
Registered	2019-09-22 21:53:37
Email Confirmed	2019-09-22 21:55:08
First Deposit	
Reg Form Submitted	2019-09-22 21:53:37 REGULAR
Terms Confirmed	2019-09-22 21:53:37 #4
AML Risk	Check History

Passport [Upload](#)



User Admin Area

- **ведение истории** анкет клиентов с возможностью просмотра изменений и (или) дополнений, в том числе на основании верификации, и дат их внесения по каждому клиенту;
- **ведение истории обновления** (актуализации) анкеты клиента (когда и кем анкета клиента была обновлена (актуализирована));
- **ведение журнала (реестра) изменений** (когда, кем и какие были внесены изменения в анкеты клиентов);
- **наличие поисковых систем**, позволяющих делать выборку (фильтр) анкет клиентов, удовлетворяющих заданным параметрам;
- **отображение информационных связей** между клиентами;
- **печать** анкет клиентов.



Верификация

Для осуществления верификации ООО «Карренси Ком Бел» применяет следующие **меры**:

- осуществляет **сверку** представленных клиентом идентификационных данных с данными о нем, полученными из общедоступных и других источников, в том числе, в социальных сетях;
- **контактирует** с клиентом по телефону, письменно, посредством электронной почты или установления видеосвязи с клиентом в сети Интернет;
- **отслеживает адрес** интернет-протокола клиента;
- осуществляет **изучение общедоступных источников** информации (в том числе сети Интернет) на предмет наличия в отношении клиентов компрометирующей информации;
- применяет **процедуру web-ID** для подтверждения достоверности ранее представленных клиентом идентификационных данных;
- получает от клиента направленные с электронной почты, указанной при регистрации, **фотоизображение, на котором изображен клиент с документом**, удостоверяющим его личность, открытым на страницах, содержащих личные данные и фотографию.



Порядок мониторинга

В ООО «Карренси Ком Бел» в целях осуществления мониторинга разработана **система алертов**, позволяющая выявлять **операции, подлежащие особому контролю, автоматическим способом**, например, при:

- достижении клиентом определенной суммы (начиная с эквивалента 10000 долларов США и более);
- использование клиентом для расчетов с ООО «Карренси Ком Бел» более 1 банковской платежной карты;
- использование клиентом для расчетов с ООО «Карренси Ком Бел» более 1 адреса виртуального кошелька;
- использование несколькими клиентами для расчетов с ООО «Карренси Ком Бел» 1 адреса виртуального кошелька и иные.



Мониторинг сделок (операций) с токенами

ООО «Карренси Ком Бел» использует **программное обеспечение** (Coinfirm и Crystal), **выполняющее обобщение и анализ использования клиентами** (потенциальными клиентами) **их адресов** (идентификаторов) **виртуальных кошельков**, а также осуществляющее **оценку риска** применения адресов (идентификаторов) виртуальных кошельков клиентов (потенциальных клиентов) **для осуществления противоправной деятельности (участия в ней)**.



Статистика

За период с 15.01.2019 по 24.09.2019 ООО «Карренси Ком Бел» выявило **86 подозрительных финансовых операций**, сведения по которым были направлены в орган финансового мониторинга.

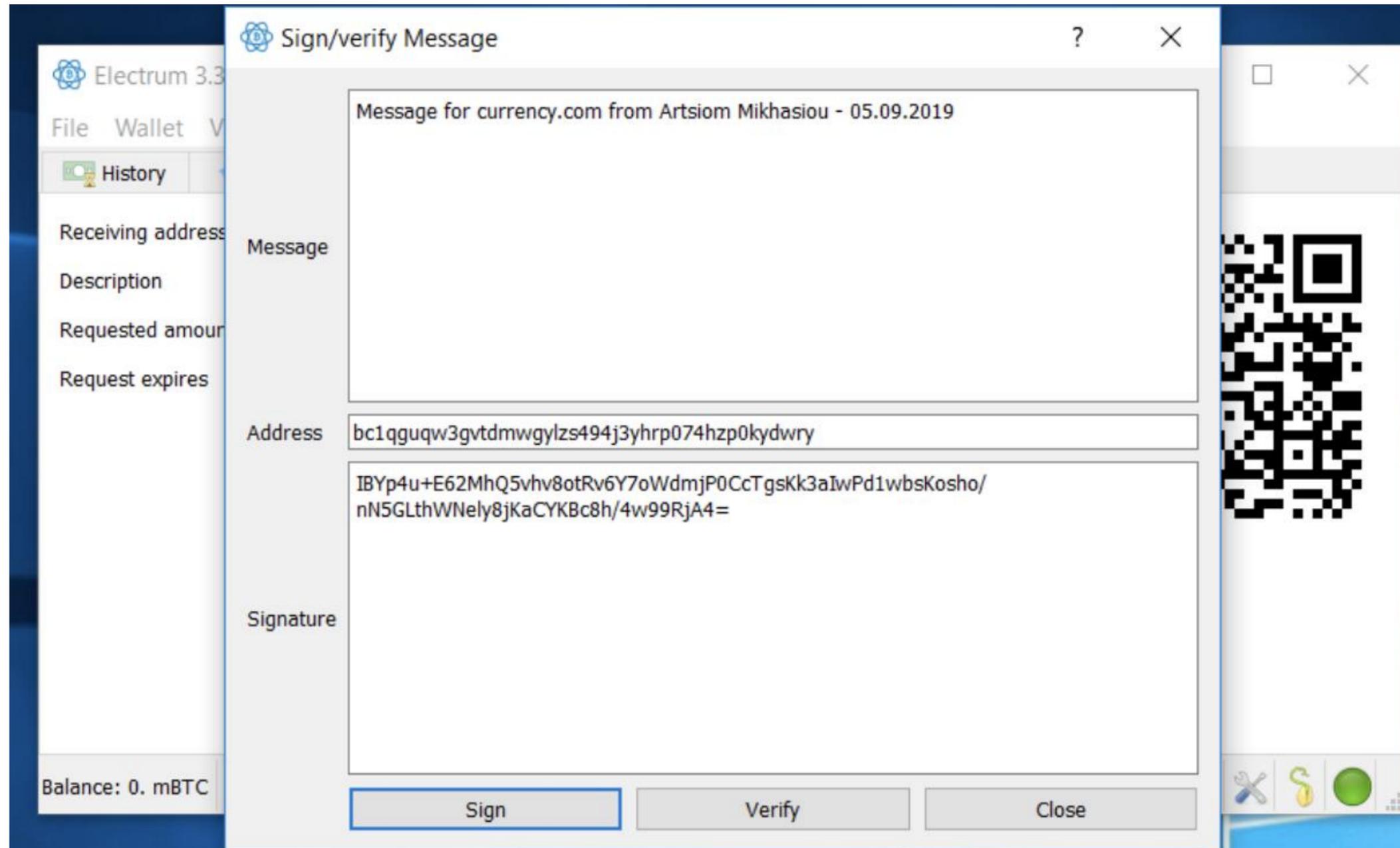
Наиболее часто встречаемые признаки подозрительности:

- 1) использование клиентом для расчетов с резидентом ПВТ или другими лицами через резидента ПВТ банковского счета либо электронного кошелька, открытого в оффшорной зоне, или банковского счета либо электронного кошелька третьего лица, или банковского счета, открытого в стране, отличной от страны его регистрации (резидентства);
- 2) представление клиентом вызывающей подозрение информации, в том числе такой, которую невозможно (чрезвычайно сложно) проверить или проверка которой является чрезмерно дорогостоящей;
- 3) представление клиентом документов (их копий), вызывающих сомнение в их подлинности (достоверности), либо подложных документов;
- 4) немотивированный отказ клиента от представления запрашиваемых документов (сведений) или неоправданные (необычные) задержки в их представлении либо чрезмерная обеспокоенность клиента вопросами конфиденциальности;
- 5) представление клиентом письменного подтверждения об отсутствии другого лица, в интересах которого совершается финансовая операция, в случае если по итогам взаимодействия с клиентом по вопросу определения данного другого лица у резидента ПВТ сохранилась уверенность (сохранились подозрения) в его существовании.



Проблемы в операционной деятельности

2) проверка принадлежности адресов виртуальных кошельков клиентов:



Благодарим за внимание!

**Управляющий ООО «Карренси Ком Бел»,
кандидат юридических наук
Шевченко Александр Петрович**

**Ведущий специалист по финансовому
мониторингу ООО «Карренси Ком Бел»
Симоненко Дарья Дмитриевна**



Currency.com



ПОД/ФТ: от данных к решениям

Смещение фокуса на онлайн-контроль

«Мы живем в разгар потопа данных»

2.5

квинтиллиона (10^{18})
байт данных
формируется ежедневно

Более
90%
информации

которую мы в настоящее
время храним, было
создано только в
прошлом десятилетии

От данных к решениям



Пост-контроль



ОБЩИЕ ПРАВИЛА

- Законодательство
- Методические рекомендации ЦБ РФ



КЛИЕНТСКИЙ ПРОФИЛЬ И ОКРУЖЕНИЕ

- Негативный профиль
- Негативное окружение, контрагенты



ТРАНЗАКЦИОННЫЕ ХАРАКТЕРИСТИКИ

- Транзакционные признаки
- Негативные паттерны/схемы



СКОРИНГ

- Постоянное добавление новых источников данных
- Отбор высоко-рисковых сегментов для будущего анализа



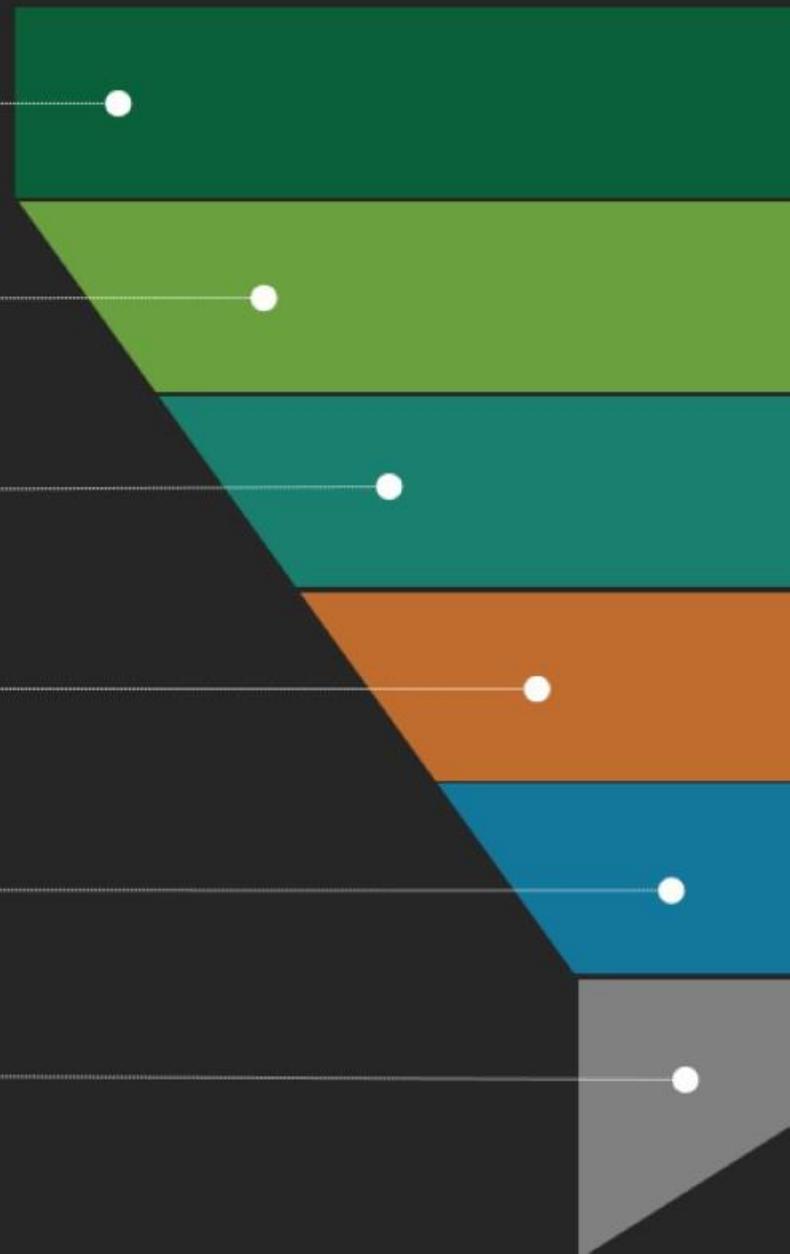
КЛИЕНТСКАЯ СЕГМЕНТАЦИЯ

- Каждая модель работает для своего сегмента
- Различные модели покрывают различные схемы



СОРТИРОВКА

- Объем потенциально сомнительных операций
- 85% попаданий





Ансамбль моделей для входа нового клиента в Банк

Выявление AML-клиентов еще до приема на обслуживание



Модели раннего выявления AML-клиентов / схем

Снижение уровня вовлеченности Банка



Распознавание документов

Снижение трудозатрат при анализе документов



Модели поиска аномалий

Снижение уровня вовлеченности Банка

Элементы AI в AML



Рекомендательные системы

Помощь в принятии решений сотрудникам комплаенс



Прогнозирование AML-оборотов

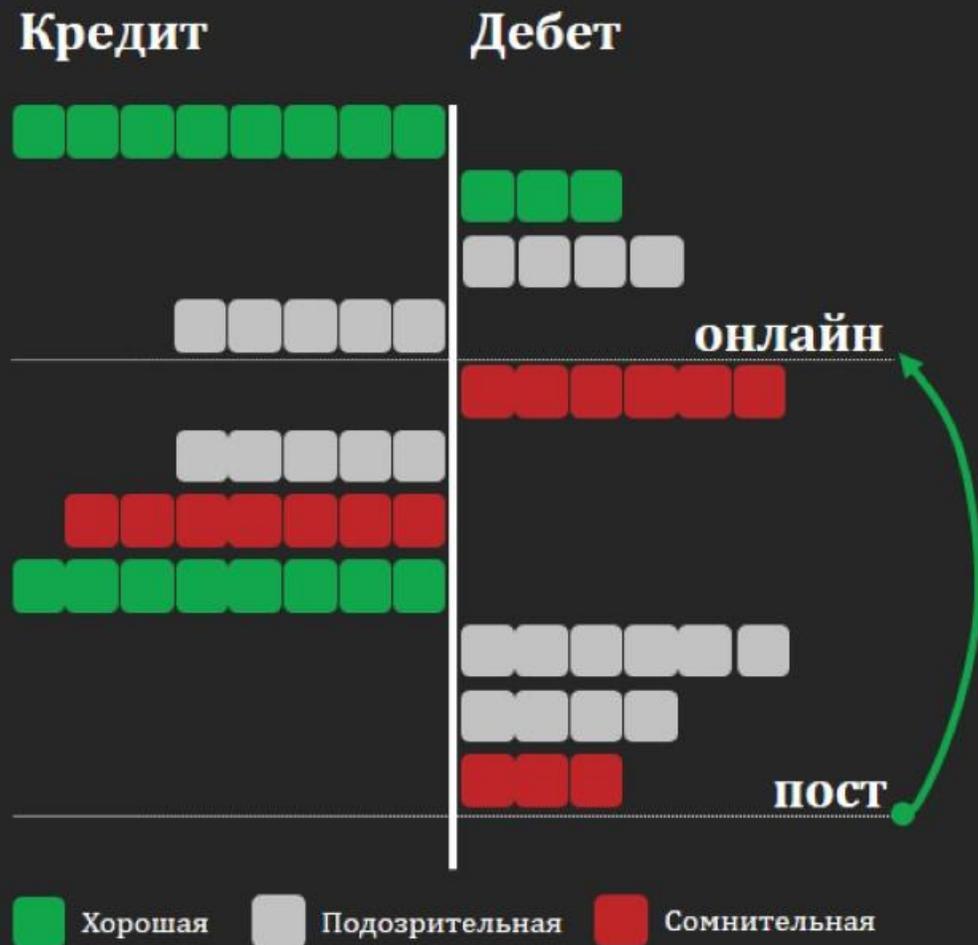
Помощь в принятии решений сотрудником комплаенс



Модели старта

Снижение среднего чека нового AML-клиента

Смещение фокуса на онлайн-контроль



Основная цель:
смещение фокуса с пост-контроля на онлайн

Новые модели в онлайн помогуткратно снизить объем сомнительных операций

Смещение фокуса на Онлайн-контроль

Снижение

в **5 раз**
объема AML операций

Начало

0.1 млн руб

TO BE

X млрд руб

AS IS

5X млрд руб

Новые модели в онлайн помогуткратно снизить объем сомнительных операций и прогнозировать планируемое нарушение

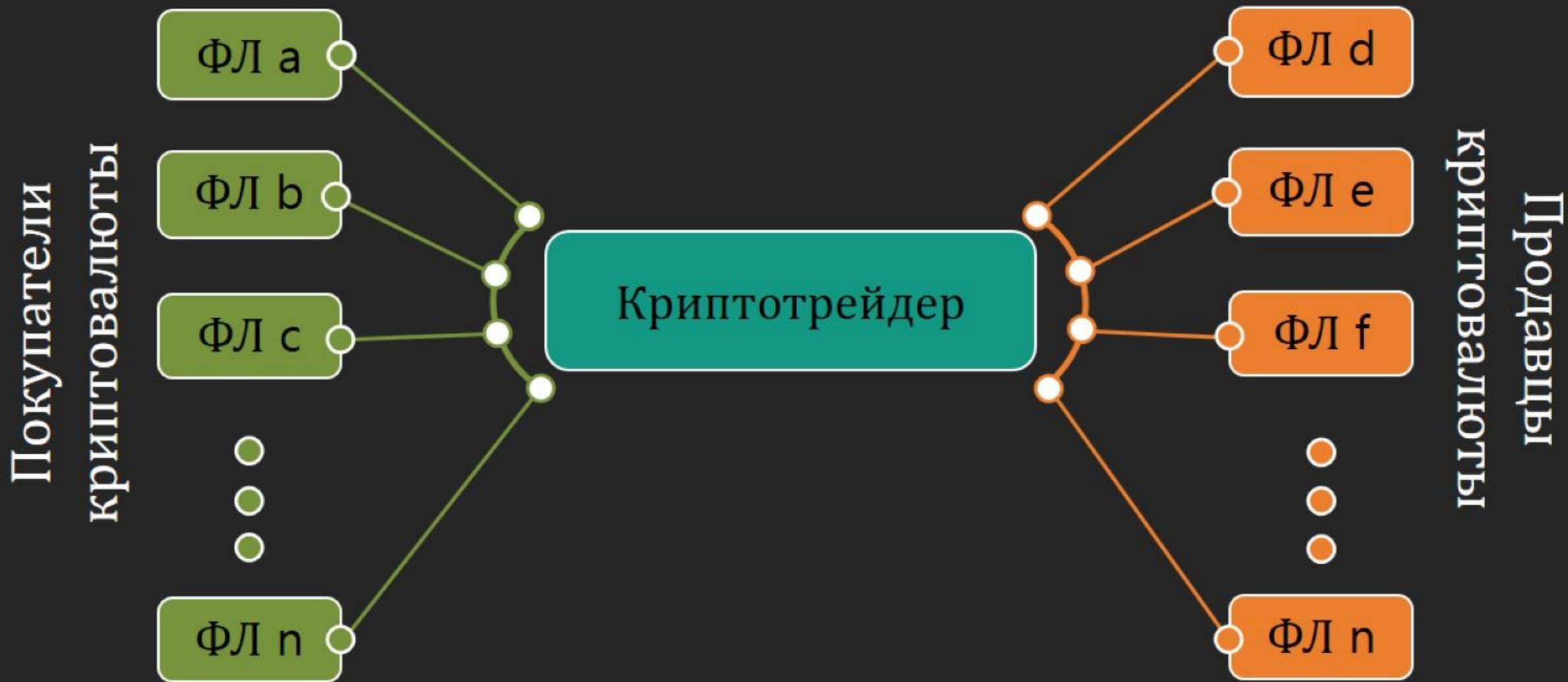


ПОД/ФТ: риски использования криптовалют

Риск вывода капитала за рубеж с использованием криптовалют



Риск легализации с использованием криптовалют



Сентябрь 2019

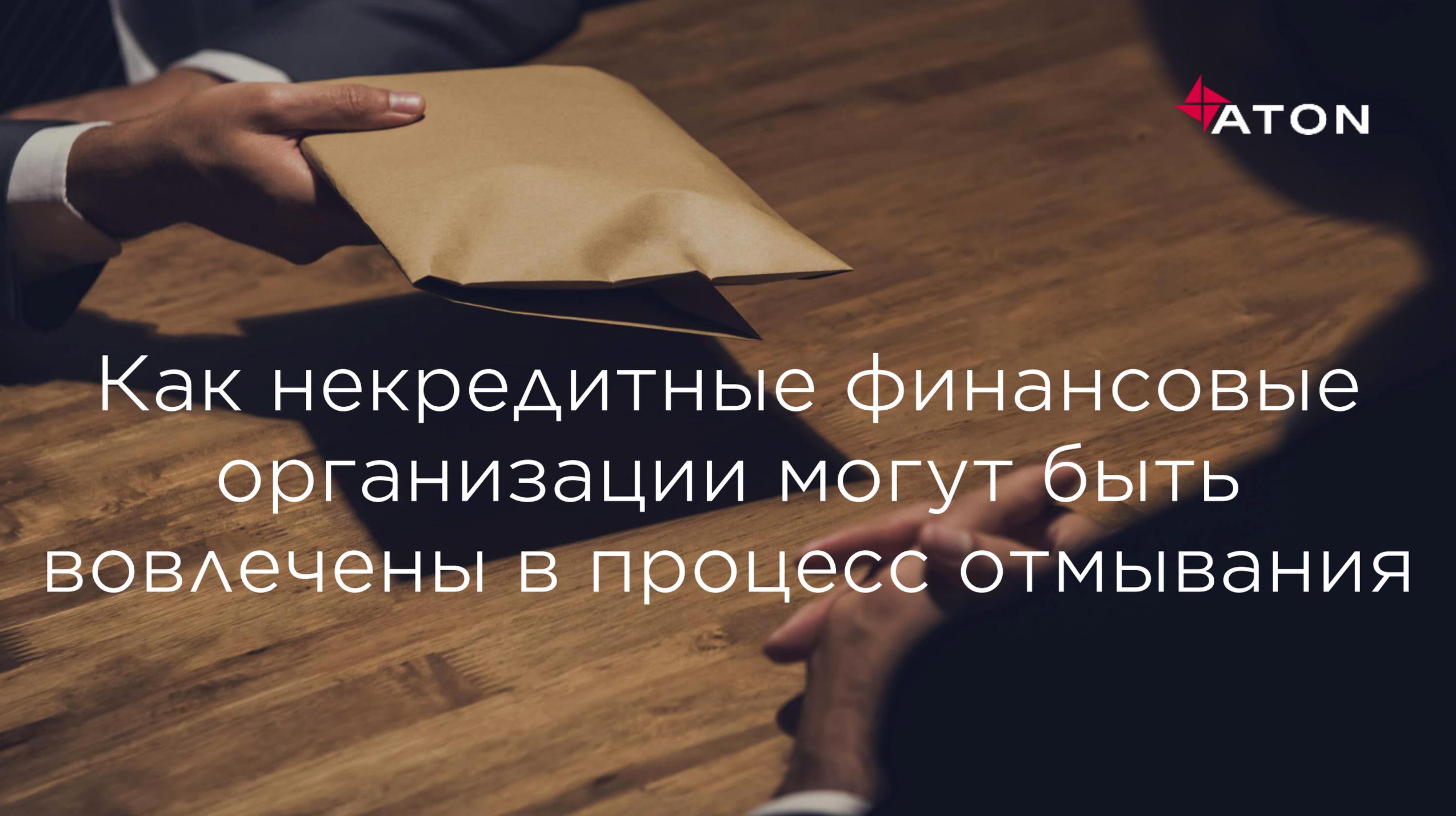
Сомнительные операции с финансовыми активами

ОСНОВНЫЕ ВЫВОДЫ



Случаи **отмывание денежных средств, полученных преступных путем**, участились на **финансовом рынке** в период после 2008 года после ужесточения регулирования банковской деятельности. Будучи **менее урегулированными и более сложными**, листингованные ценные бумаги **становятся уязвимыми для ОД/ФТ**.

Риск-ориентированный подход, основанный на аналитике, позволяет выделить **операции по отмыванию** среди общего объема совершаемых клиентами операций.

A background image showing a close-up of a person's hands in a dark suit holding a brown paper envelope over a wooden table. Another person's hands are visible in the lower right, also in a suit, suggesting a business meeting or transaction.

Как некредитные финансовые
организации могут быть
вовлечены в процесс отмывания

От банков к финансовому рынку



Как это работает?

Активом, полученным от нелегальной деятельности, постепенно передается вид законных через серию операций

Преимущества:

- Скорость исполнения
- Вариативность

Как некредитные организации могут быть вовлечены?



1. Преступление

образуются нелегальные доходы

2. Размещение ДС

с использованием инструментов
финансового рынка

3. Расслоение

запутывание следов источника
происхождения преступных
доходов

4. Интеграция

денежные средства и имущество
становятся легальными

Неликвидные финансовые активы как инструмент отмывания денег

Ликвидность – способность актива быть реализованным в короткие сроки и с наименьшими денежными потерями

Российский рынок



Низкая ликвидность на рынке

После кризиса 2008-2009 годов с рынка ушли иностранные инвесторы и фонды

Большая часть сделок заключается на OTC

Биржевые стаканы не отражают реальную ситуацию на рынке

В отсутствие достоверных рыночных данных

Стороны управляют ценой

Ликвидные активы:

20 – 25 акций

около 60%
всего рынка

70 бондов

около 30-35%
всего рынка

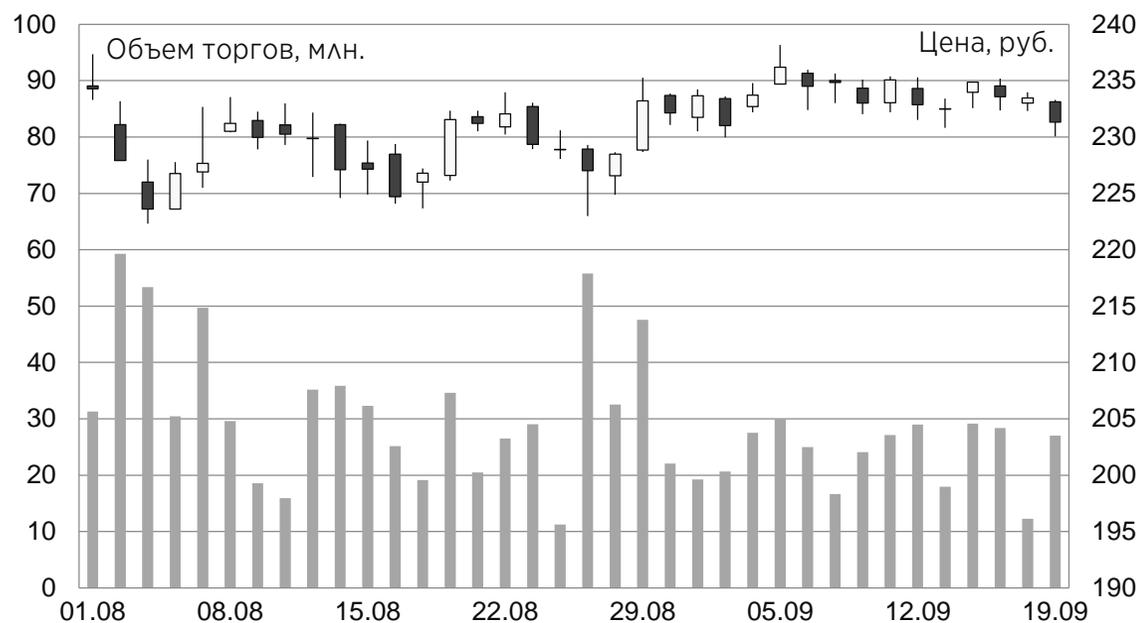
Результат: Посредством манипулирования рынком правонарушители могут намеренно искажать биржевые данные, чтобы они не отражали реальную стоимость ценных бумаг

Различие в торгах по ценным бумагам



Высоколиквидная бумага

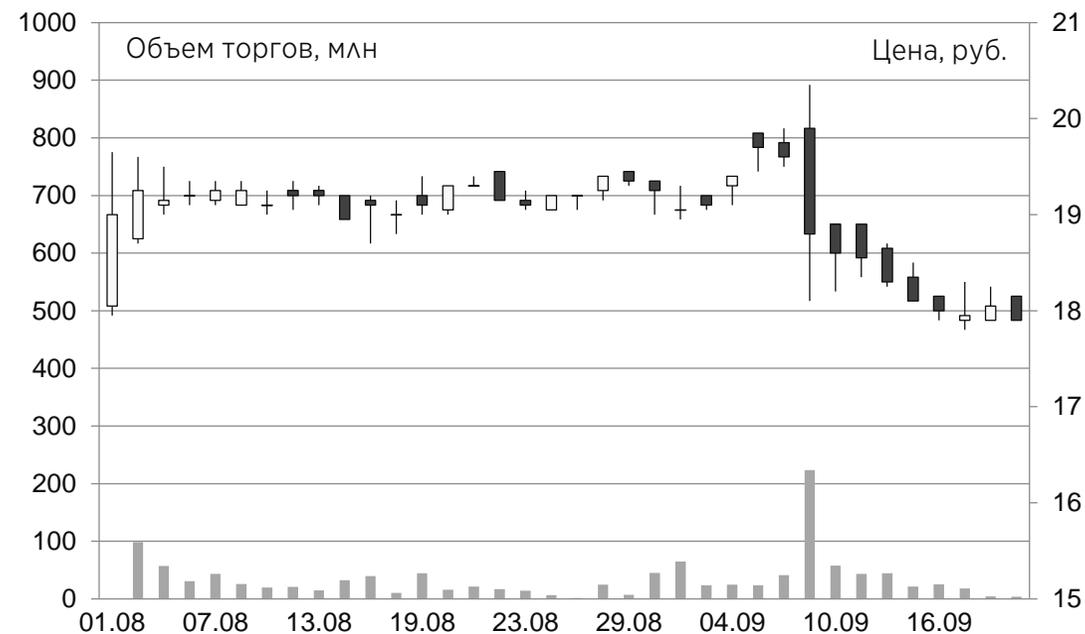
ПАО «Газпром»



Источник: Bloomberg

Низколиквидная бумага

ПАО «Пермэнергосбыт»



Источник: Bloomberg

Основные цели использования неликвидных ценных бумаг

1. Вывод капитала за пределы РФ
2. Смена права собственности
3. Уклонение от уплаты налогов (налоговая оптимизация)
4. Расчетные операции

Вывод капитала за пределы РФ

Как это происходит?

Заключается контрагентская сделка между двумя профучастниками с неликвидным активом на большую сумму

Что для этого характерно?

- ✓ Сделка заключается на бирже/либо OTC;
- ✓ Вторая сторона по сделке – российский профучастник или иностранная финансовая организация из юрисдикции с высоким рейтингом ФАТФ;
- ✓ Сделка заключается на большую сумму;
- ✓ В результате сделки происходит перемещение актива через границу

Какие инструменты используются?

Акции / Облигации / Инвестиционные паи / Деривативы

Смена права собственности



Как это происходит?

Ценные бумаги перемещаются из одного депозитария в другой посредством заключения OTC сделки

Что для этого характерно?

- ✓ OTC сделка;
- ✓ При смене депозитария происходит также смена юрисдикции;
- ✓ Стоимость актива может быть любой в зависимости от целей правонарушителей;
- ✓ Реальная оплата отсутствует

Какие инструменты используются?

Акции / Облигации

Уклонение от уплаты налогов



Как это происходит?

Физическое или юридическое лицо заключает через профучастника серию сделок, в результате которой одна сторона получает прибыль, другая несет убытки (уменьшение размера налогооблагаемой прибыли)

Что для этого характерно?

- ✓ Сделки заключаются на бирже;
- ✓ Сделка между подконтрольными лицами;
- ✓ Несколько похожих сделок заключается с одной и той же стороной;
- ✓ В результате всегда одна сторона «выигрывает», а другая несет убытки

Какие инструменты используются?

Акции / Облигации / Инвестиционные паи / Деривативы

Расчетные операции



Как это происходит?

Клиент оплачивает через профучастника покупку неликвидных активов на большую на большую сумму с целью маскировки оплаты товаров услуг

Что для этого характерно?

- ✓ Сделка заключается на бирже/либо ОТС;
- ✓ Сделка заключается на большую сумму;
- ✓ Оплата по сделке происходит через профучастника

Какие инструменты используются?

Акции / Облигации / Инвестиционные паи / Деривативы

Некредитным финансовым организациям следует обращать внимание на:



Финансовый инструмент

Историю торгов, Объем выпуска, Спред, Эмитент (финансовая отчетность, Реальность осуществления деятельности) Площадку (насколько быстро и дешево происходит листинг бумаг на площадке)

Участников

Использование большого количества лицензированных посредников (администраторы, депозитарии, банки и т.д.), Готовность контрагентов раскрыть конечного бенефициара по сделке

Юрисдикция

Происходит смена юрисдикции, Активы переводятся в низконалоговую юрисдикцию

Валюта

Валюта расчетов по сделке отличается от валюты, в которой номинирован инструмент

Разовая сделка на внебиржевом рынке



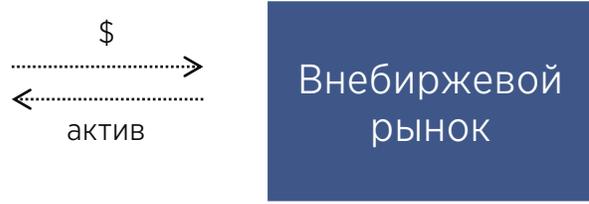
1

Ввод \$ на счет
в брокере



2

Подача поручения
на покупку актива



2

Подача поручения
на продажу актива



Результат: \$50тыс. на счете компании-нерезидента за пределами РФ

Актив – низколиквидный евробонд. Спрос/предложение отсутствует. Невозможно определить рыночную стоимость (=0)

Сделки на «раз-два-три»



1

Ввод \$ на счет
в брокере



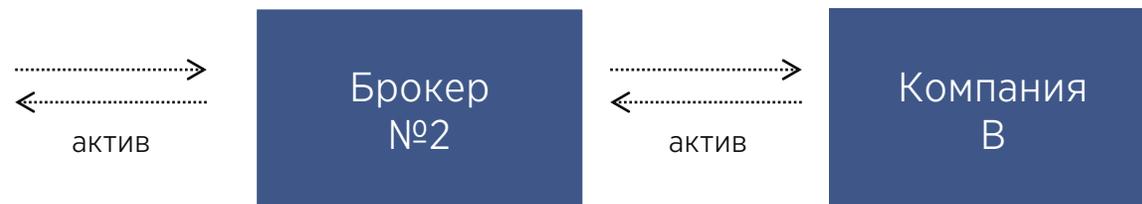
2

Подача поручения
на покупку актива
150 заявок, V - 450 000 шт.



2

Подача поручения
на продажу актива
150 заявок, V - 450 000 шт.



- 1) 72 руб./шт.
- ⋮
- 54) 250 руб./шт.
- ⋮
- 100) 400 руб./шт.
- ⋮
- 150) 480 руб./шт.

Результат: 1) цена 2 - 480 руб./шт. 2) 200 млн. руб. на счете компании В

Актив - биржевая низколиквидная корпоративная облигация Рыночная цена - 72 руб./шт.

Усложненная схема



1

Ввод \$ на счет в брокере

3

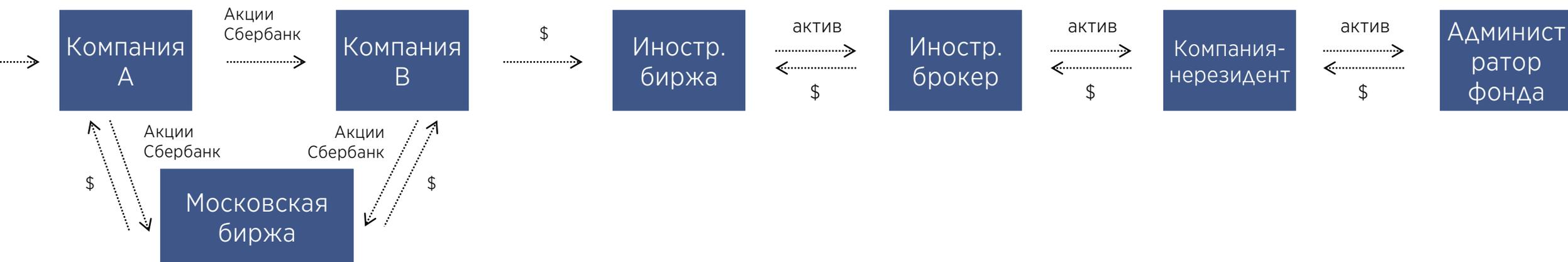
Неторговый перевод. Оплата без участия брокера. Подтверждения оплаты нет

5

Подача поручения на покупку актива

5

Подача поручения на продажу актива



2

Покупка высоколиквидных цб

4

Перевод высоколиквидных цб в денежную форму

Результат

- 1) Смена УВО через Администратора фонда
- 2) Вывод \$ за пределы РФ

Актив – биржевая низколиквидная корпоративная облигация
Рыночная цена – 72 руб./шт.

Мониторинг рисков операций электронного кошелька, его автоматизация и алгоритмизация

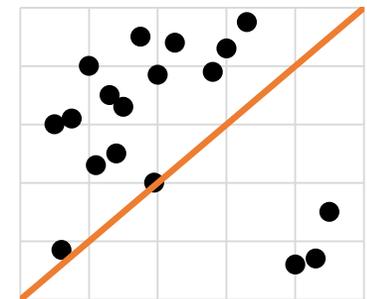
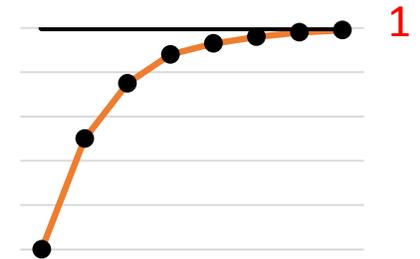
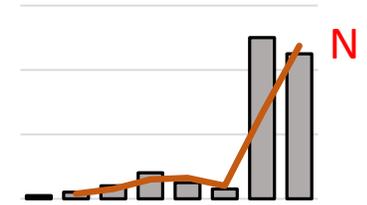
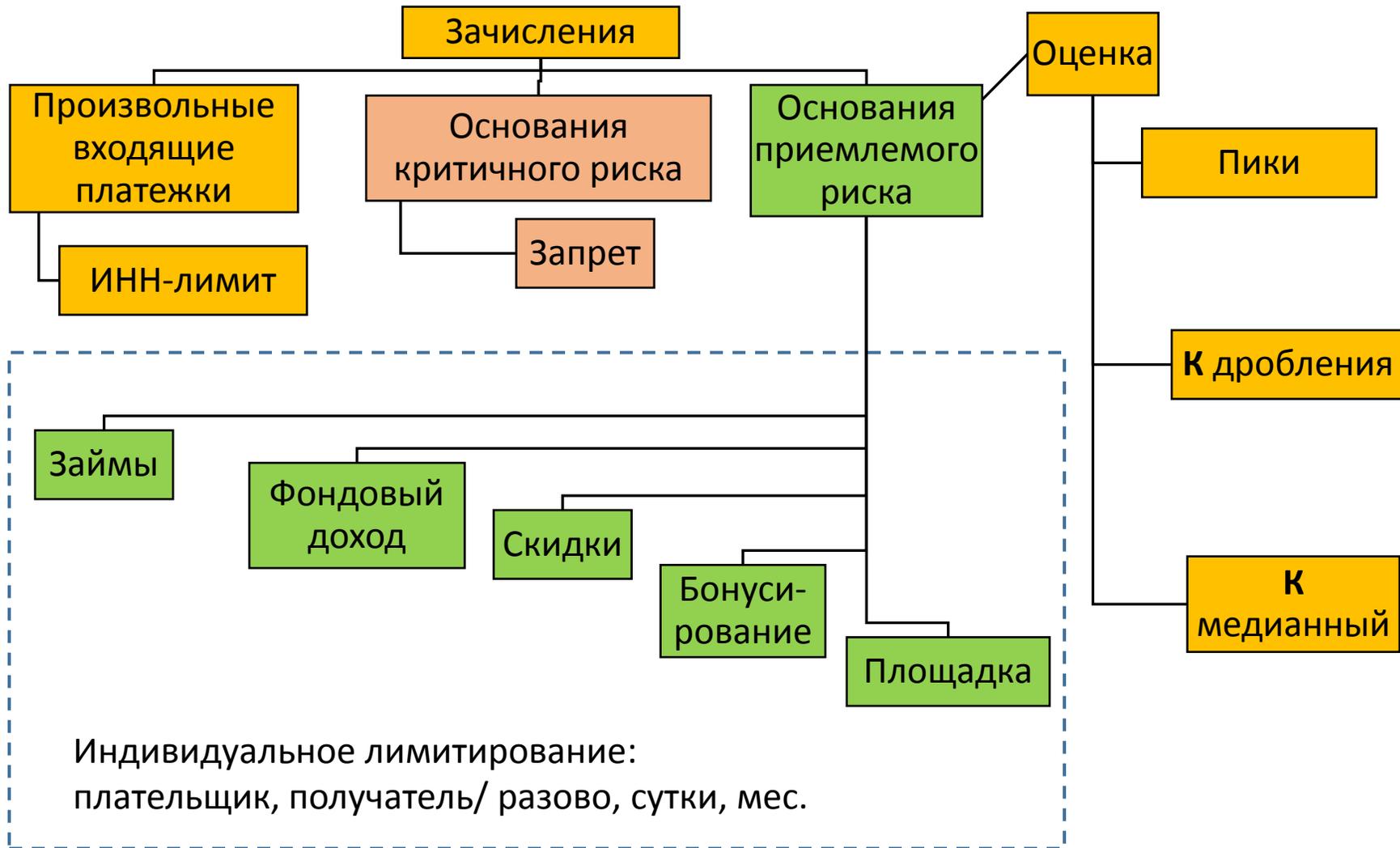
Дмитрий Гронин,

Руководитель службы внутреннего контроля

Василий Сергацков,

Начальник департамента информационной безопасности и противодействия мошенничеству

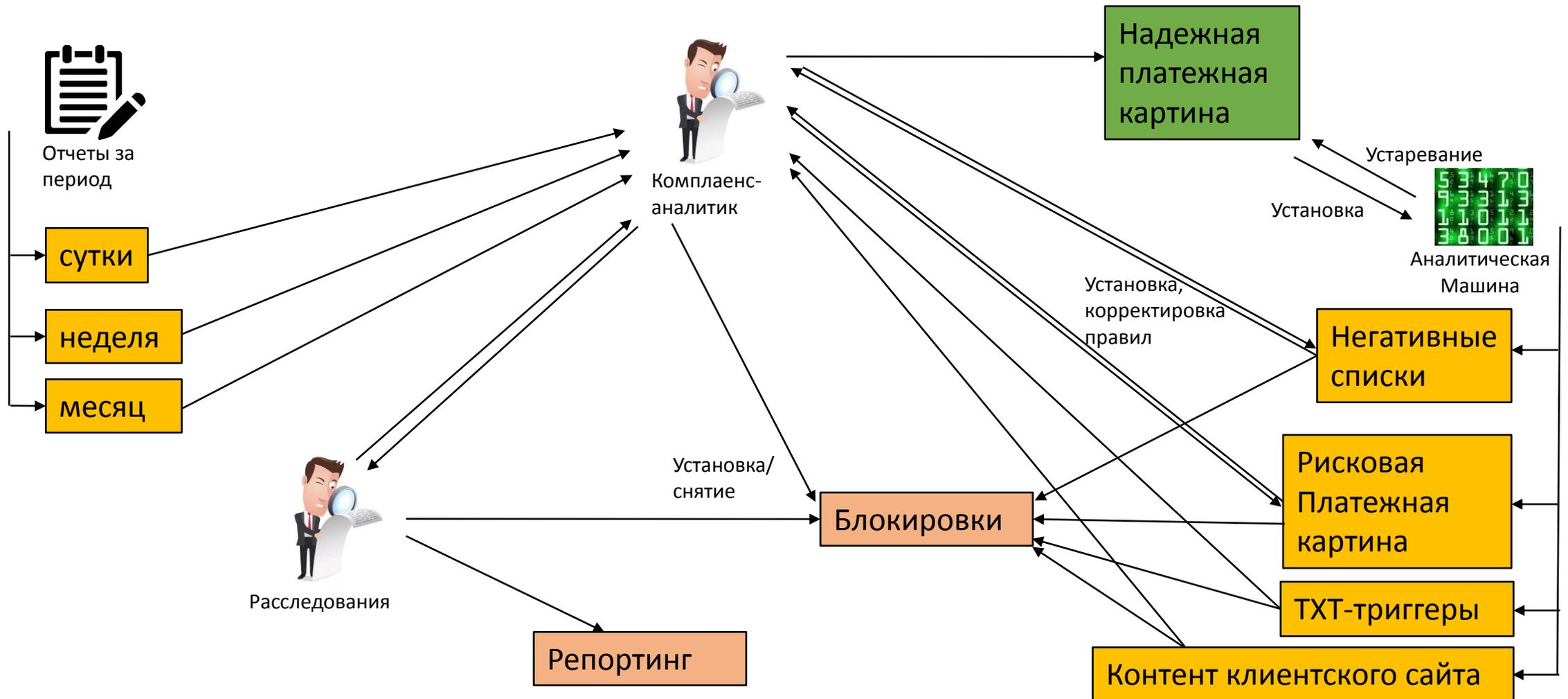
Управление входящими потоками ЭДС



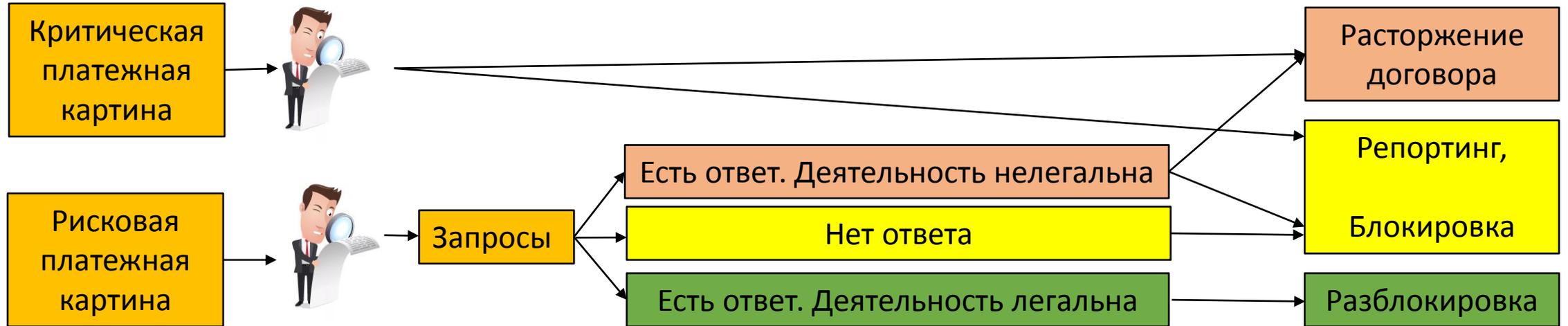
Показатели периодического мониторинга

- **Пики:** доля крупнейших N реквизитов получателей в общем объеме выплат. Указывает на наличие выделяющихся на общем фоне по объему крупнейших получателей.
- **Коэффициент дробления:** отношение общей суммы выплат к числу платежных реквизитов получателей, являющихся уникальными, и сумме установленного лимита на реквизит. Приближение коэффициента снизу к единице указывает на то, что суммы фактических выплат консолидируются в районе установленных лимитов.
- **Медианный коэффициент:** доля числа уникальных реквизитов получателей, на которые приходится 50% выплат. Является показателем неравномерности выплат.

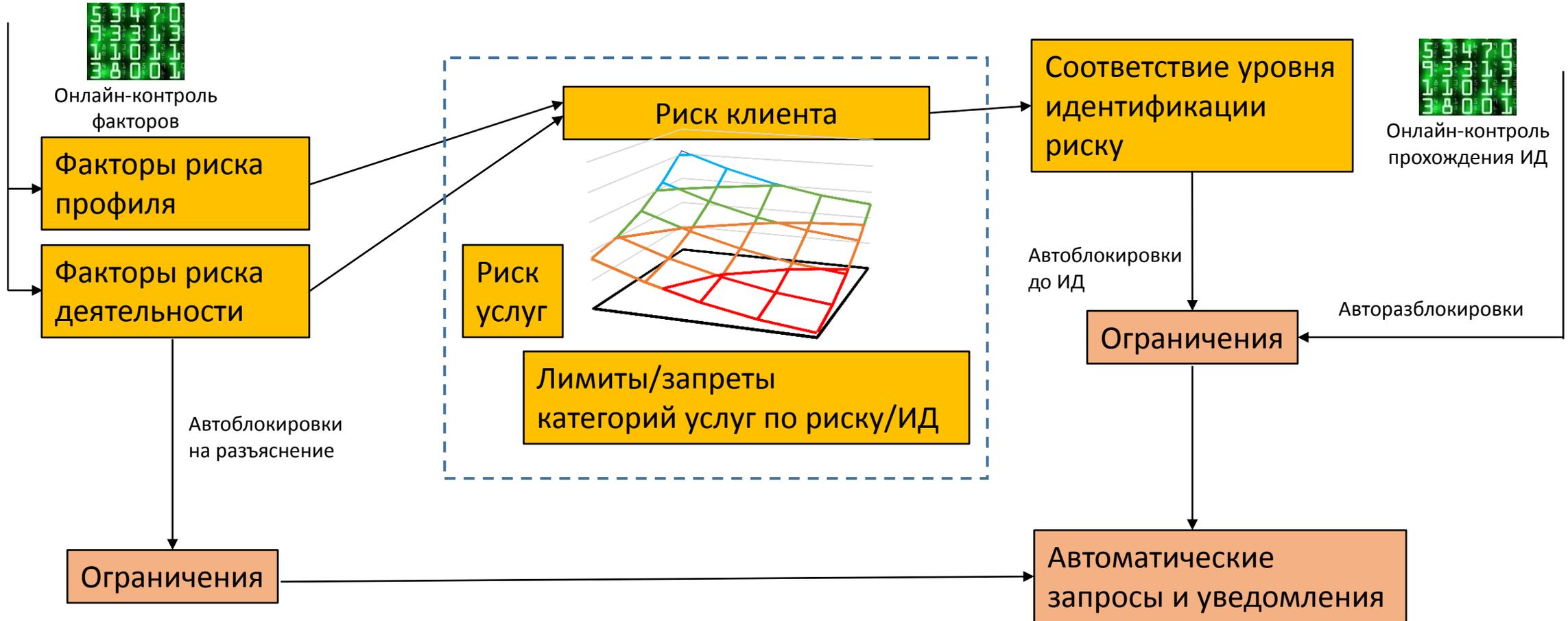
Управление исходящими потоками ЭДС



Расследования и репортинг



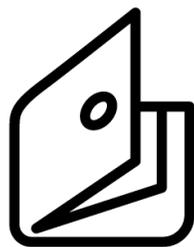
Управление риском и идентификацией клиента



Что у нас есть



Карты



Кошелёк



Автоплатежи



Платежи
в приложениях



QR-оплата



Мобильный
терминал



ПЭИ не
только

Глобальные пересечения



устройства

идентификаторы

средства платежей

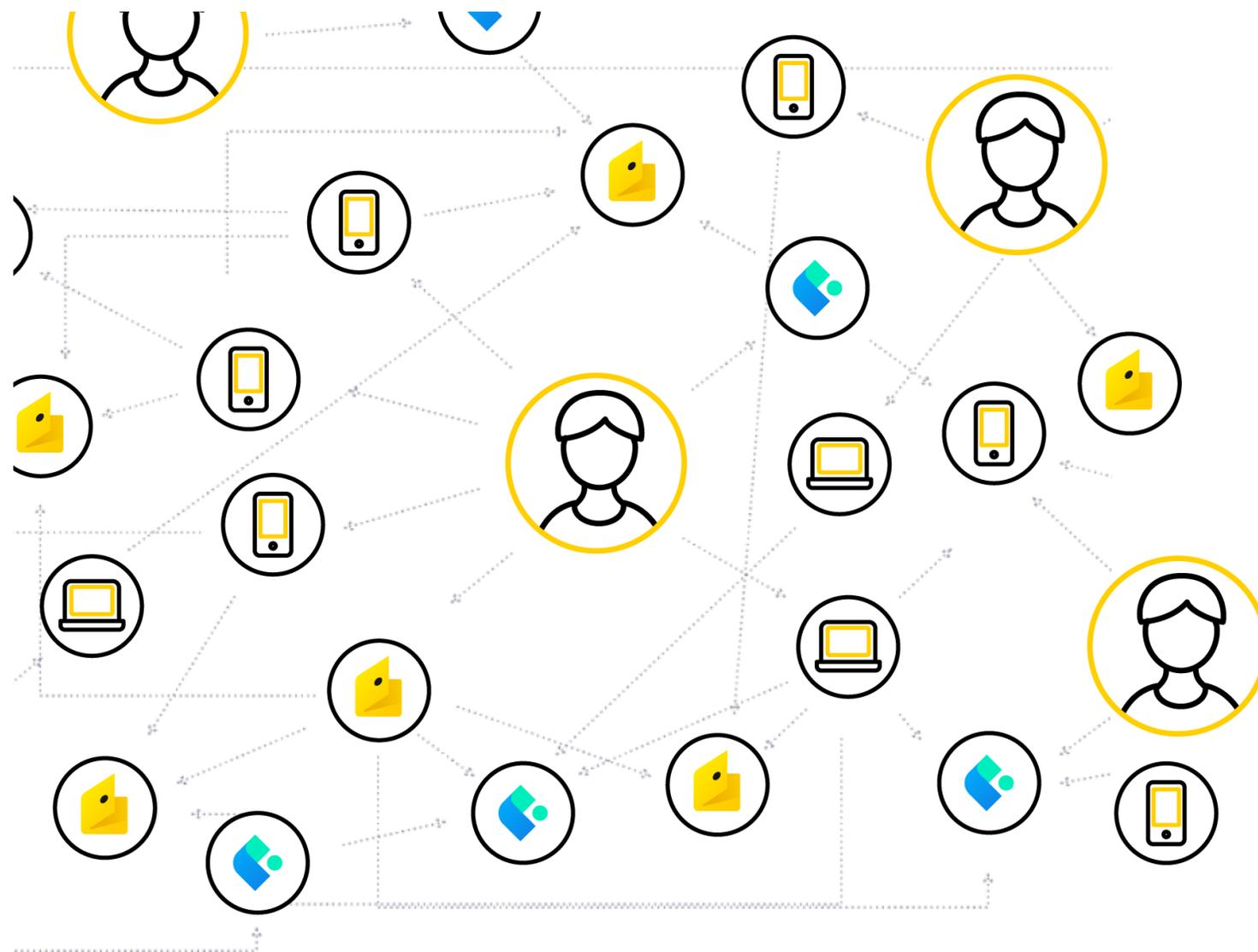
география

email

телефоны

IP, источники пополнений

...



Deep Learning vs Machine Learning

DL

-  Находит сложные зависимости
-  Умеет работать с последовательностями
-  Требуется много данных
-  Черный ящик

ML

-  Простые модели быстро учатся
-  В некотором случае, человеко-понятные
-  Нужно тщательное конструирование признаков специалистом
-  Не умеет искать сложные зависимости

Как это работает



Машинное обучение – это часть Data Science

Сбор и выбор данных – самая сложная часть



Обучающий набор (разметка)

Выбор модели и ее обучение



Тестирование и снова выбор и снова обучение

Применение на новых данных



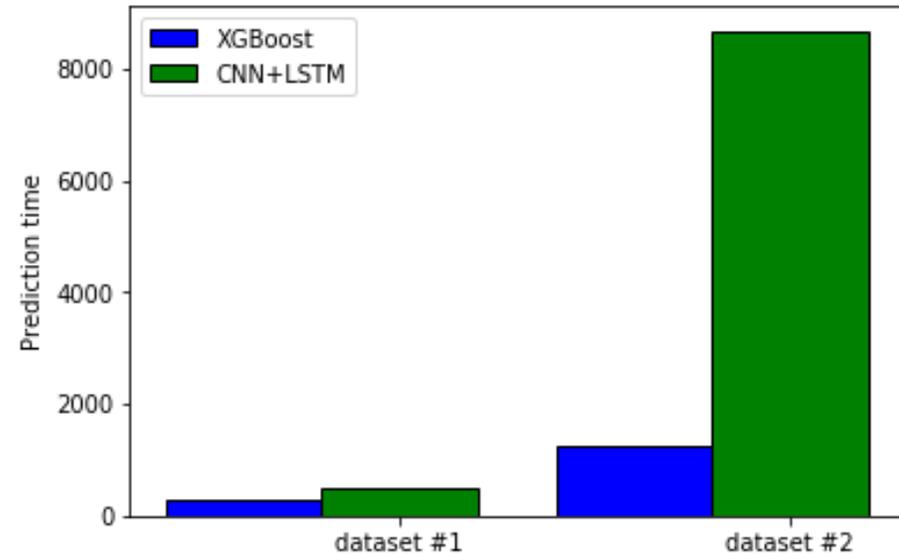
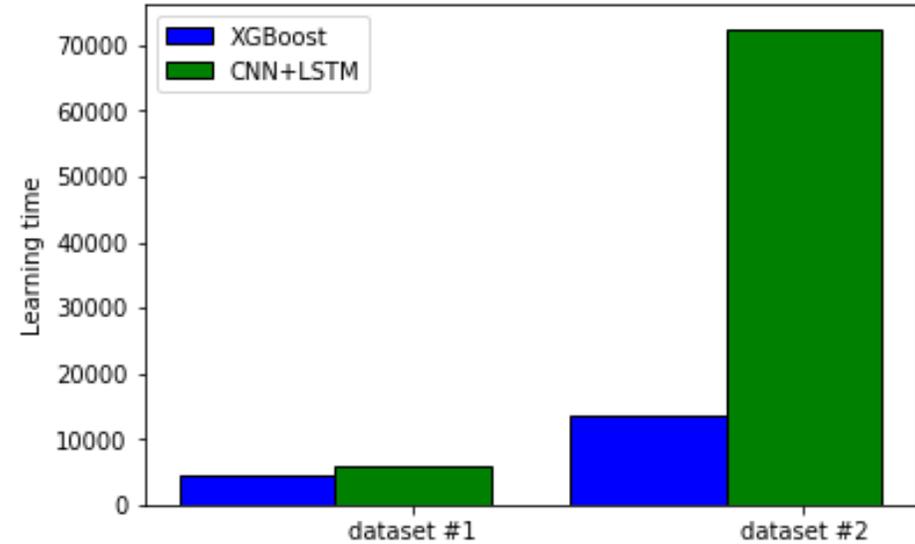
Скорость обучения и предсказания

-Dataset #1

Данные по платежам: 54
признаков, 522 910 объектов

-Dataset #2

Данные по платежам + данные по
устройствам: 2 000 признаков,
522 910 объектов (20/80)



Precision

Fraction of retrieved accounts that are relevant to the query

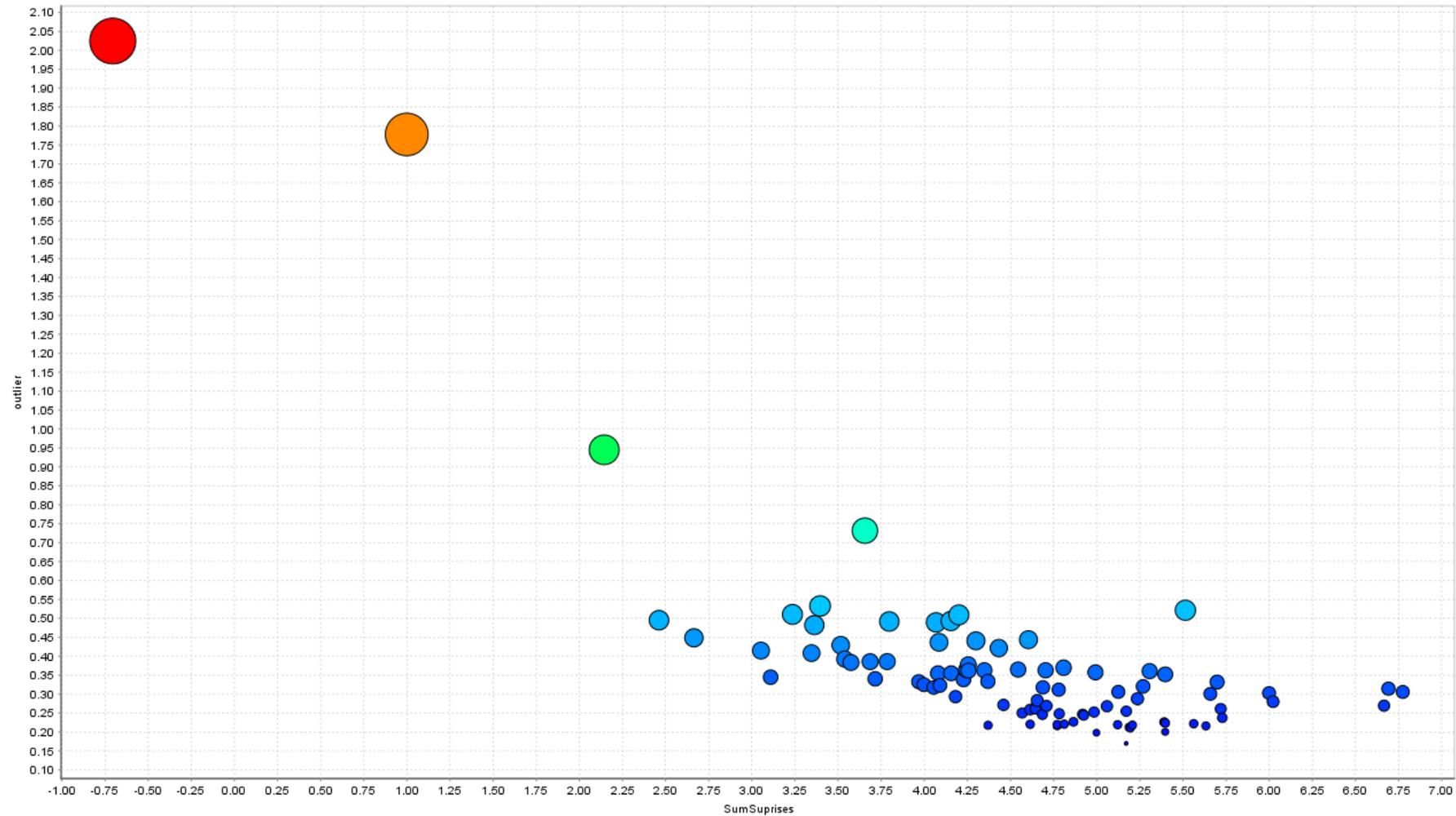
Metric: Precision	XGBoost	LSTM+CNN
Dataset #1	0.90795	0.94771
Dataset #2	0.91281	0.95831

Recall

Fraction of the relevant accounts that are successfully retrieved

Metric: Recall	XGBoost	LSTM+CNN
Dataset #1	0.96604	0.97891
Dataset #2	0.97234	0.98332

Подозрительная активность клиентов



Выводы

Машинное обучение не заменяет правила и не отменяет аналитиков

Можно использовать простые понятные модели, но нужно понимание особенностей своей работы

Anomaly detection не панацея, но иногда работает!=)

Ак Барс
Банк



27.09.2019

**Качественная идентификация как
инструмент предупреждения
противоправных операций**

Ак Барс Банк в системе ПОД/ФТ

присутствует в **27**
регионах страны
с головным
офисом в городе
Казани

Крупнейший
региональный
универсальный
банк с
государственным
участием
Республики
Татарстан

Располагает
всеми видами
существующих в
Российской
Федерации
банковских
лицензий

Обслуживает
более **4,3 млн.**
частных лиц и
свыше **50 тыс.**
корпоративных
клиентов

оказывает **более**
100 видов
банковских услуг
для
корпоративных и
частных клиентов

Перед Банком, как перед финансовой организацией стоит первостепенная задача по эффективному применению мер по борьбе с отмыванием денег, финансированием терроризма и финансированием распространения оружия массового уничтожения.

Входит в реестр
значимых
кредитных
организаций на
рынке платежных
услуг РФ

Член Совета
Комплаенс,
обладатель
множества грамот и
благодарственных
писем от Банка
России и
Росфинмониторинга
за работу в области
ПОД/ФТ

Грамотно выстроенная работа в части идентификации клиентов, их представителей и бенефициарных владельцев, по мнению Банка, является одним из важнейших аспектов в построении эффективной системы борьбы с отмыванием денег и финансированием терроризма.

Участник
совместного
пилотного проекта
ЦБ и ФСФМ по
выявлению
индикаторов ФТ

Определение бенефициарных владельцев и сложности их выявления

Ак Барс
Банк



Физическое лицо, которое прямо или косвенно владеет **минимальным процентом доли в собственности** юр лица

Физическое лицо, **осуществляющее управление** без права собственности за счет участия в финансировании предприятия

Физическое лицо, **осуществляющее управление** юридическим лицом иными способами: личные контакты с ответственными людьми

Физическое лицо, **ответственное за принятие стратегических решений**, которые оказывают решающее влияние на развитие

Физическое лицо, **осуществляющее исполнительный контроль** за ежедневной или регулярной деятельностью юридического лица с использованием позиции руководства высшего звена

Подход, учитывающий **преобладающее большинство акций**.
Акционеры, осуществляющие управление единолично или совместно с другими акционерами, включая какой-либо контракт, договоренность, взаимоотношения, посреднические отношения

Проблематика :

Сведения о бенефициарных владельцах могут быть не указаны в документах компаний или занижено их официальное участие

Затруднение выявления бенефициарных собственников в трастах и холдинговых структурах

Неразглашение информации о бенефициарах при использовании офшоров при оптимизации налогообложения и уклонения от уплаты налогов и при легализации средств, полученных криминальным путем

С целью максимального сокрытия сведений о личности бенефициарного владельца применяются всевозможные схемы оформления собственности и правоустанавливающей документации

Меры, принимаемые Банком, для установления владельцев бизнеса

Клиент



Клиентский менеджер



Сведения и документы по бенефициарному владельцу

Самостоятельное установление бенефициарных владельцев

на основании информации, получаемой Банком из внешних источников информации, доступной на законных основаниях (использование веб-сервиса Контур.Фокус, СПАРК-Интерфакс, средства массовой информации и пр.).

Обращение к комплаенс – офицеру в случае наличия затруднений при самостоятельном установлении бенефициарных владельцев



Бенефициарный владелец выявлен, информация Банка совпадает с информацией, представленной клиентом.



Бенефициарный владелец выявлен, информация Банка совпадает с информацией, представленной клиентом. Выявлена принадлежность бенефициарного владельца к категории ПДЛ. Присвоен высокий уровень риска.

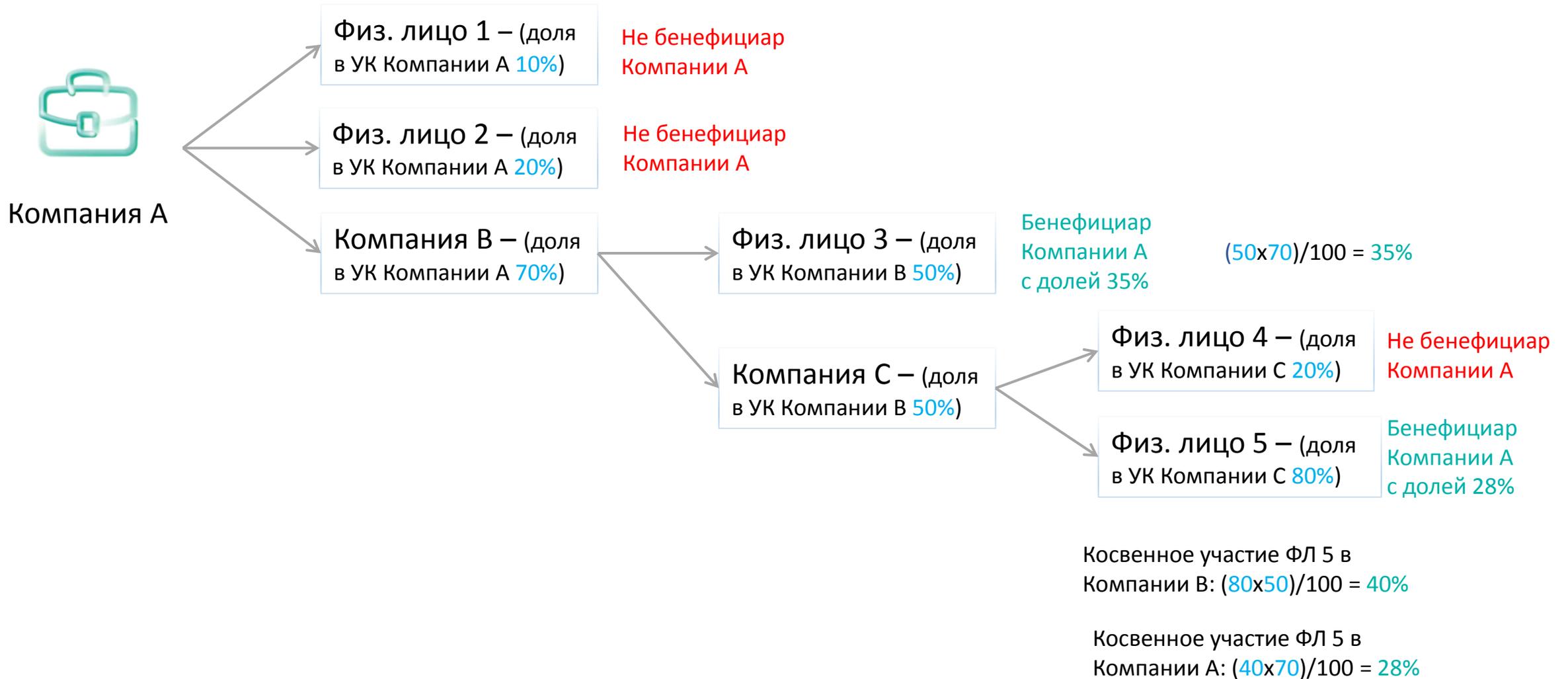


Отказ от заключения договорных отношений с клиентом в случае невозможности достоверно установить конечного бенефициарного владельца клиента (непрозрачная структура собственности, перекрестное (взаимное) владение, использование офшорных юрисдикций, трастов).

Кейс:

Банк рассматривал заявление юридического лица «М» на открытие расчетного счета. В сведениях о бенефициарных владельцах клиентом было указано физическое лицо, являющееся единственным учредителем компании. Из анализа представленных документов и информации, полученной из внешних источников, Банк пришел к выводу, что реальным собственником бизнеса является иное физическое лицо, отличное от указанного клиентом. Кроме того, юридическое лицо обладало признаками фирм-однодневок, а учредитель компании являлся учредителем 7 юридических лиц. Клиенту отказано в принятии на обслуживание на основании отсутствия прозрачности в отношении конечных собственников компании и наличия подозрений об осуществлении противоправной деятельности подконтрольными юридическими лицами с последующим репортигом по отказу от заключения договорных отношений.

Установление конечного бенефициара каскадным способом



Управление рисками ОД/ФТ при обслуживании лиц, связанных с ПДЛ

Установление факта принадлежности к окружению МПДЛ при идентификации клиента, определение степени родства

Верификация полученной информации с использованием сервиса X-compliance (Интерфакс)*

Заполнение клиентом вопросника установленной формы

Физическое лицо

Журавская Екатерина Всеволодна

Категория: Близкое окружение МПДЛ, Близкое окружение ID записи: 894831 Даты рождения: 1972-08-16 (); Дата смерти: Пол: Женский Дата обновления: 14.06.2019

Документы Адреса Альтернативные наименования Связанные лица Списки наблюдения Санкционные ограничения Доп. информация Биография

ФИО	Тип связи	Дата обновления	ID св. лица
Гуриев Сергей Маратович	супруг	2019-08-12 21:53:39	894829
Гуриев Марат Аликович	родитель супруга/супруги ребенка	2019-08-12 21:53:39	894830

*Пример интерфейса поисковика

✓ *Разрешение получено*

Получение разрешения на обслуживание Председателя Правления

Оценка риска представляемого продукта
Оценка уровня коррупционного риска должности ПДЛ
Получение информации из открытых источников данных

Продукт высокого риска – открытие счета с внесением наличных денежных средств с целью совершения перевода средств за рубеж. Информации негативного характера не выявлено.

Установление источника происхождения денежных средств

Источник происхождения денежных средств:

Фиксирование информации в АБС,
Присвоение высокого уровня риска

Уровень риска:

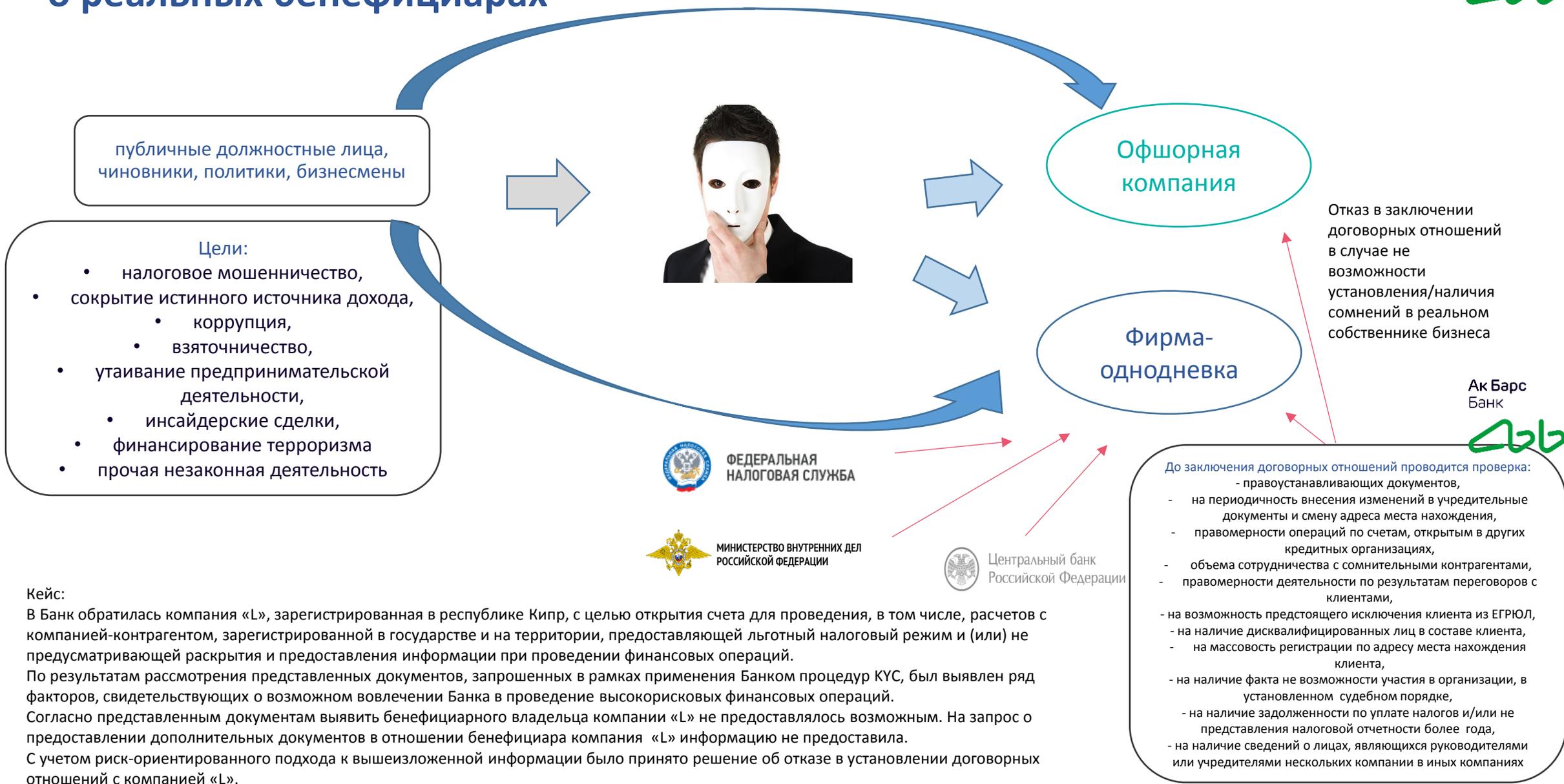
Мониторинг транзакционной активности клиента

Ежедневный автоматизированный отчет по операциям клиента

Направление сведений в Росфинмониторинг

Направлено ОЭС с кодом 6001 (1130) с указанием в поле DESCR информации о зачислении на счет близкого родственника МПДЛ крупной суммы денежных средств с последующим переводом на свой счет в иностранной кредитной организации

Подставные лица (frontiers) как инструмент сокрытия информации о реальных бенефициарах



Кейс:

В Банк обратилась компания «L», зарегистрированная в республике Кипр, с целью открытия счета для проведения, в том числе, расчетов с компанией-контрагентом, зарегистрированной в государстве и на территории, предоставляющей льготный налоговый режим и (или) не предусматривающей раскрытия и предоставления информации при проведении финансовых операций.

По результатам рассмотрения представленных документов, запрошенных в рамках применения Банком процедур КУС, был выявлен ряд факторов, свидетельствующих о возможном вовлечении Банка в проведение высокорисковых финансовых операций.

Согласно представленным документам выявить бенефициарного владельца компании «L» не предоставлялось возможным. На запрос о предоставлении дополнительных документов в отношении бенефициара компания «L» информацию не предоставила.

С учетом риск-ориентированного подхода к вышеизложенной информации было принято решение об отказе в установлении договорных отношений с компанией «L».

Механизмы выявления в Банке лиц, причастных к ПЭ/ФРОМУ

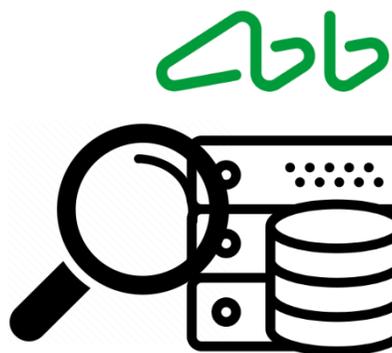
Ак Барс
Банк



- Своевременное получение перечней и их актуализация в АБС



- Проверка клиентов и связанных лиц, в том числе, по проводимым операциям и сделкам*



- ✓ Клиенты
- ✓ Бенефициары
- ✓ Представители
- ✓ Контрагенты

- ✓ Открытие расчетного счета
- ✓ Международный платеж
- ✓ Обмен валюты
- ✓ SWIFT перевод
- ✓ Выдача кредита
- ✓ Перевод без открытия счета

В случае выявления совпадения с ПЭ/ФРОМУ происходит эскалация в Комплаенс- подразделение



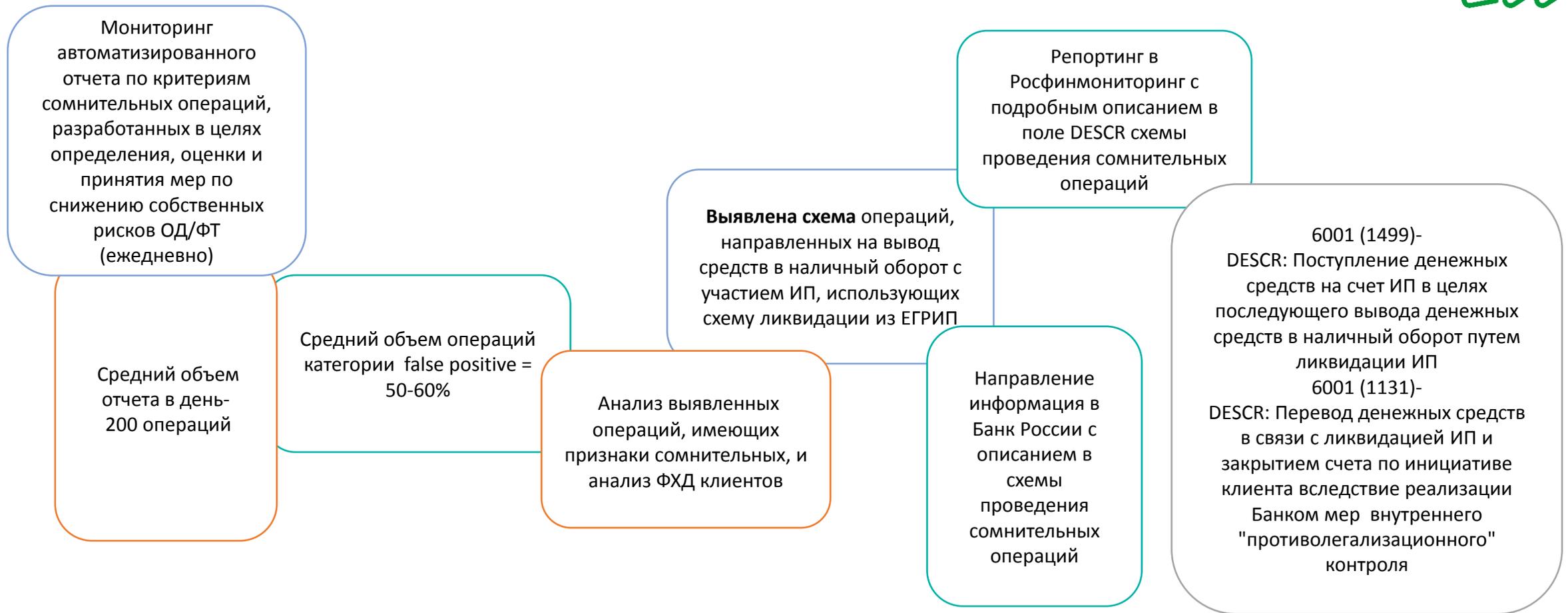
AML офицер

Незамедлительное применение мер в соответствии с установленным порядком

* Приведен примерный перечень операций.

Выявление новых типологий противозаконной деятельности клиентов

Ак Барс
Банк



За 8 месяцев 2019 года общее количество направленных в Росфинмониторинг сообщений, отвечающих признакам сомнительных с кодом 6001, составило - 18457 сообщений. В том числе операций с указанием признака необычной операции, как «иной» (ХХ99) – 8 304 сообщения (45%).

Ак Барс
Банк



www.akbars.ru

Использование технологии DeviceFingerprint
для целей выявления подозрительных
операций и клиентской активности

2019

Цели. Определение уязвимостей.

Основная цель – новые подходы к выявлению подозрительных операций и клиентской активности в зонах повышенного риска.

Основные уязвимые места:

- использование номинальных юридических лиц (юридические лица с признаками «фирм-однодневок»);
- возможность проводить финансовые операции по перемещению доходов, полученных преступным путем, скрывая при этом конечных выгодоприобретателей преступных схем за номинальными учредителями и директорами;
- для управления счетами организаций используется Интернет-банкинг.

Цели. Определение уязвимостей.

Риск наиболее характерен для совершения правонарушений в кредитно-финансовой сфере, бюджетной сфере, при совершении коррупционных преступлений.

Процесс хищения и отмыывания средств производится через цепочку подконтрольных, номинальных юридических лиц.

Большинству схем вывода денежных средств за рубеж, а также схем трансформации безналичных денежных средств в наличную форму предшествуют операции, которые, как правило носят транзитный характер.

Принимаемые меры по минимизации рисков.

Ориентирование на типологические признаки и схемы отмывания доходов с участием «фирм-однодневок».

Осуществляется комплекс мер по устранению номинальных юридических лиц: внедрены механизмы препятствования регистрации таких компаний и использованию для этого подставных физических лиц.

«Фирмы-однодневки» стараются быть похожими на обычные добросовестные организации.

Принимаемые меры по минимизации рисков.

В рамках реализации Правил внутреннего контроля – Программы управления риском легализации (отмывания) доходов, полученных преступным путем, фактором, влияющим на оценку риска клиента в категории «риск по типу клиента и (или) бенефициарного владельца», является:

- совпадение идентификатора устройства клиента, с использованием которого им осуществляется доступ к автоматизированной системе, программному обеспечению с целью осуществления переводов денежных средств, с идентификаторами устройств других клиентов, в том числе тех, в отношении операций которых принимались решения об их квалификации в качестве подозрительных.

Принимаемые меры: IP адреса.

IP адреса – точность, как следствие ценность информации не достаточно высока, тем более если говорить об автоматизации относительно выявления подозрительных операций и клиентской активности.

При реализации практика показала, что данные существенно «замусорены» совпадениями.

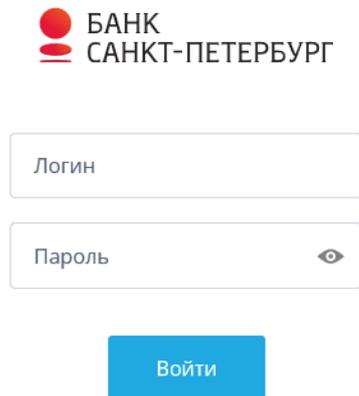
Дата	Время	IP-адрес	...
13.09.2019	13:04:18	95.16	126
13.09.2019	13:05:38	95.16	126
13.09.2019	16:30:38	95.16	126
11.09.2019	17:59:22	217.6	217
09.09.2019	18:24:30		
06.09.2019	17:41:24		
06.09.2019	17:43:11		
05.09.2019	14:28:49		
03.09.2019	13:05:06		
30.08.2019	18:06:59		
30.08.2019	02:01:30	95.16	26
29.08.2019	00:15:53	217.6	80
26.08.2019	19:48:11	95.16	26
23.08.2019	14:37:39	95.16	26
22.08.2019	08:04:14	95.16	26

Наименование клиента	Рег. номер к...	IP-адрес
		3 78
		3 78

Принимаемые меры: DeviceFingerprint.

Более точная модель для целей выявления подозрительных операций и клиентской активности может быть построена на технологии DeviceFingerprint (BrowserFingerprint).

DeviceFingerprint является способом опознавания пользователя и его устройства (присвоение идентификатора), на основе признаков, характеристик.



БАНК
САНКТ-ПЕТЕРБУРГ

Логин

Пароль 

Войти



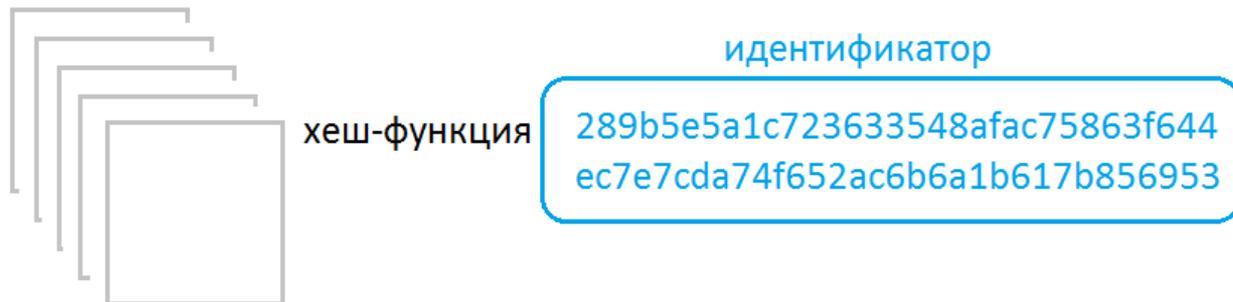
Принимаемые меры: DeviceFingerprint.

Примеры категорий данных, признаков, используемых для построения идентификатора устройства

Тип данных	Описание
Браузер	Информация, связанная с браузером, используемым конечного пользователя: тип, название, версия, список поддерживаемых языков, список установленных плагинов.
Шрифты	Названия шрифтов, установленных на компьютере конечного пользователя.
Экран	Информация, связанная с экраном пользователя. Разрешение монитора, разрешение рабочей зоны, глубина цвета монитора.

Массив данных будет отличаться практически на каждом устройстве.

Данные передаются в функцию хэширования и на выходе получается строка фиксированной длины, состоящая из букв и цифр – **идентификатор**.



DeviceFingerprint - инструмент.

DeviceFingerprint – не является целью, необходима логика вокруг него.

Элементы построения модели для целей реализации программы управления риском:

- аномалии – множество устройств у одного пользователя или множество пользователей у одного устройства;
- совпадение с устройствами пользователей, в отношении операций которых принимались решения об их квалификации в качестве подозрительных;
- ведение стоп-листа идентификаторов (правила обработки) для целей предиктивной аналитики в части клиентской активности, в том числе, как элемент системы on-line контроля.

DeviceFingerprint – инструмент (примеры).

Аномалии – множество устройств у одного пользователя или множество пользователей у одного устройства.

Множество устройств у одного пользователя

ID	Дата входа	Время в	IP-а	Hash	Тайм зона
1398697331	17.07.2019	16:43:25	94.2	32eb079dc91385f8dc4cdfdbe0924580ed82aeb80a6663d8a9c6d06602e7db2d	UTC+03:00
1398697331	22.07.2019	16:22:05	94.2	fe12ba83710 added90a899d2fc0d6acf6d97856bb1bef63bc43d30dca105ddbcc4	UTC+03:00
1398697331	01.08.2019	10:59:41	83.2	4 615cb32693f2e90177aa3ee4812cf83ae9ed83150b0dbec892499388dd806017	UTC+03:00
1398697331	22.08.2019	10:13:28	185	195 9f48137f316a6fdb6db8d38f0fa20de3e1cf9527c3a8678b0f3c30fbcf301dd5	UTC+03:00
1398697331	22.08.2019	13:02:15	185	195 9bd7af56123daf2c9dc6eb34d30575dd986448f7090d127ef0a886429d05ab	UTC+03:00
1398697331	22.08.2019	15:42:20	185	195 a94bb1089b24ebd782811aa41f71bc92daa3c076936a29fccd933021649c1e22	UTC+03:00
1398697331	22.08.2019	15:55:16	185	195 d561de9b1f3456cd90977ca0bf053f1fc64ffda8c97e14a742774e8a1020bba5	UTC+03:00
1398697331	22.08.2019	16:17:33	185	195 a7c34b7146b6aa449137e1111db64e7d4b463a010b8a007c6f95ab0808aec671b	UTC+03:00
1398697331	22.08.2019	18:13:50	185	195 243597df652c184407130e1b050996450fab5f6628641128c7c54b222305c4a	UTC+03:00

Использование на стороне пользователя средств самих браузеров (встроенные эмуляторы, «режим инкогнито» и т.п.) или сторонних утилит (программ), меняющих любые параметры браузера случайным образом.

DeviceFingerprint – инструмент (примеры).

Аномалии – множество устройств у одного пользователя или множество пользователей у одного устройства.

Множество пользователей у одного устройства

ID	Дата входа	Время входа	IP-адрес	Hash	Тайм зона
1375579473	20.09.2019	18:23:35	95.	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953	UTC+03:00
1326013649	20.09.2019	18:19:30	95.	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953	UTC+03:00
1389117974	20.09.2019	18:10:01	95.	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953	UTC+03:00
1396117101	20.09.2019	18:07:35	95.	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953	UTC+03:00
1354881404	20.09.2019	18:07:05	95.	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953	UTC+03:00
1390181672	20.09.2019	17:57:34	95.	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953	UTC+03:00
1389117974	20.09.2019	17:57:27	95.	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953	UTC+03:00
1390181672	20.09.2019	16:24:46	217.	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953	UTC+03:00
1389117974	20.09.2019	16:21:52	217.	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953	UTC+03:00
1392080980	20.09.2019	11:15:02	95.	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953	UTC+03:00

DeviceFingerprint – инструмент (примеры).

Совпадение с устройствами пользователей, в отношении операций которых принимались решения об их квалификации в качестве подозрительных.

ID	Дата входа	Время вход	IP-адрес	Hash	Тайм зона
1375579473	20.09.2019	18:23:35	95.	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953	UTC+03:00
1326013649	20.09.2019	18:19:30	95.	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953	UTC+03:00
1389117974	20.09.2019	18:10:01	95.	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953	UTC+03:00
1396117101	20.09.2019	18:07:35	95.	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953	UTC+03:00
1354881404	20.09.2019	18:07:05	95.	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953	UTC+03:00
1390181672	20.09.2019	17:57:34	95.	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953	UTC+03:00
1389117974	20.09.2019	17:57:27	95.	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953	UTC+03:00
1390181672	20.09.2019	16:24:46	217.	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953	UTC+03:00
1389117974	20.09.2019	16:21:52	217.	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953	UTC+03:00
1392080980	20.09.2019	11:15:02	95.	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953	UTC+03:00

Стоп-лист

289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
10912eb8fc868f9a268163c8e15c6529cc8f9dc405533bb51d133ed6f47fc6e6

ID	Дата входа	Время вход	IP-адрес	Имя устройства	Hash
1392080980	20.09.2019	11:15:02	95.	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1392080980	13.09.2019	13:04:18	95.	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1392080980	13.09.2019	16:30:38	95.	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1392080980	13.09.2019	13:05:38	95.	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1392080980	11.09.2019	17:59:22	217.	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1392080980	09.09.2019	18:24:30	217.	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1392080980	08.08.2019	17:22:48	176.	Mac OS X 10.13.6 Chrome 75.0.3770	10912eb8fc868f9a268163c8e15c6529cc8f9dc405533bb51d133ed6f47fc6e6
1392080980	16.07.2019	14:09:51	176.	Mac OS X 10.13.6 Chrome 75.0.3770	10912eb8fc868f9a268163c8e15c6529cc8f9dc405533bb51d133ed6f47fc6e6

DeviceFingerprint – инструмент (примеры).

Ведение стоп-листа идентификаторов для целей предиктивной аналитики в части клиентской активности, в том числе, как элемент системы on-line контроля.

ID	Дата входа	Время входа	IP-адрес	Имя устройства	Hash
1326013649	02.08.2019	18:13:20	95.1	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1326013649	30.07.2019	11:44:28	185	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1326013649	24.07.2019	12:29:54	185	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1326013649	24.07.2019	16:50:45	95.1	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1326013649	23.07.2019	14:23:09	185	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1326013649	18.07.2019	13:13:30	185	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1326013649	16.03.2019	10:27:38	37.1	Mac OS X 10.13.6 Chrome 72.0.3626	10912eb8fc868f9a268163c8e15c6529cc8f9dc405533bb51d133ed6f47fc6e6
1326013649	25.02.2019	11:11:32	78.1	Mac OS X 10.13.6 Chrome 71.0.3578	10912eb8fc868f9a268163c8e15c6529cc8f9dc405533bb51d133ed6f47fc6e6

ID	Дата входа	Время входа	IP-адрес	Имя устройства	Hash
1365766600	30.07.2019	12:26:16	185	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1365766600	29.07.2019	17:09:50	217	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1365766600	25.07.2019	14:45:06	95.1	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1365766600	23.07.2019	12:41:18	185	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1365766600	19.07.2019	13:27:53	185	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1365766600	27.05.2019	20:09:54	217	Mac OS X 10.13.6 Chrome 74.0.3729	10912eb8fc868f9a268163c8e15c6529cc8f9dc405533bb51d133ed6f47fc6e6

ID	Дата входа	Время входа	IP-адрес	Имя устройства	Hash
1392080980	20.09.2019	11:15:02	95.1	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1392080980	13.09.2019	13:04:18	95.1	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1392080980	13.09.2019	16:30:38	95.1	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1392080980	13.09.2019	13:05:38	95.1	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1392080980	11.09.2019	17:59:22	217	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1392080980	09.09.2019	18:24:30	217	Windows 10 IE 11.0	289b5e5a1c723633548afac75863f644ec7e7cda74f652ac6b6a1b617b856953
1392080980	08.08.2019	17:22:48	176	Mac OS X 10.13.6 Chrome 75.0.3770	10912eb8fc868f9a268163c8e15c6529cc8f9dc405533bb51d133ed6f47fc6e6
1392080980	16.07.2019	14:09:51	176	Mac OS X 10.13.6 Chrome 75.0.3770	10912eb8fc868f9a268163c8e15c6529cc8f9dc405533bb51d133ed6f47fc6e6

DeviceFingerprint – выводы.

Включая технологию DeviceFingerprint в контур системы управления рисками кредитной организации в части выявления подозрительных операций и клиентской активности (в том числе в части противодействия использованию номинальных юридических лиц):

- повышается «точность» и скорость выявления клиентов – юридических лиц с признаками «фирм-однодневок»;
- повышается «точность» в процессе установления цепочек подконтрольных, номинальных юридических лиц (включая категорию «регистраторы»);
- появляется возможность построения системы для целей предиктивной аналитики в части клиентской активности;
- как следствие, повышается качество сообщений о подозрительных операциях (СПО);
- система on-line контроля дополняется рядом сценариев (работа с новым инициирующим триггером).



БАНК
САНКТ-ПЕТЕРБУРГ



Оценка ПОД/ФТ рисков в проектах ЕБРР

ЕАГ/МУМЦФМ Семинар, Казань, 26-27 Сентября
2019



European Bank
for Reconstruction and Development

Руководящие Принципы проверки благонадежности клиентов

Основной документ, определяющий приемлемые стандарты благонадежности и принципы, на которых основывается процедура проверки благонадежности клиентов.

Документ предусматривает

Ответственность за первоначальную проверку и оценку рисков лежит на команде банкиров. Команда банкиров лучше всего может добиться выполнения этой задачи строго придерживаясь процедур проверки, которые описывают роли всех участников процесса проверки.

Общие Процедуры проверки

Дополняют Руководящие Принципы и детально описывают необходимые шаги в процессе проведения проверки во всех проектах.

Документ предусматривает

ПОД/ФТ проверочный лист должен быть заполнен Командой банкиров для всех проектов с участием финансовых, и приравняемых к ним, институтов, в отражении специфического риска, который они представляют. К приравняемым к финансовым институтам относятся фонды прямых инвестиций, а также любые другие организации, где капиталы собираются в единый пул для последующего инвестирования.

ПОД/ФТ Процедуры

Описывают необходимые шаги, выполняемые сотрудниками Банка, проводящими проверку благонадежности клиентов для всех проектов с участием финансовых, и приравняемых к ним, институтов.

Команда банкиров обязана

- Оценить риск отмывания денег или финансирования терроризма в процессе проведения проверки всех проектов с нефинансовыми учреждениями.
- Для всех проектов с участием финансовых, и приравняемых к ним, институтов заполнить ПОД/ФТ проверочный лист.

Документ предусматривает

- ✓ Банк не будет осуществлять проект, если не известен его конечный бенефициар.
- ✓ Банк не будет устанавливать отношения с любыми лицами, которые были осуждены за совершенное преступление или находящимися под следствием за совершенное преступление.
- ✓ Банк не будет устанавливать отношения с любыми лицами, которые в настоящий момент числятся в международном черном списке.
- ✓ Банк не будет осуществлять проект, если есть доказательства связей с организованной преступностью или участия в преступной деятельности.
- ✓ Отношения с ПЗЛ, высоко рисковыми клиентами, и проекты в определенных высоко рисковых секторах, требуют усиленных проверок.



- ✓ Международные санкции.
- ✓ Уход от налогов и использование оффшорных компаний.
- ✓ Финансирование терроризма и отмывание преступных доходов.



Банк, в лице Комплаенс Отдела, имеет статус наблюдателя в ФАТФ, МАНИВЭЛ и ЕАГ, участвует в их Пленарных заседаниях, учитывает их решения и применяет рекомендации для усиления своих процедур проверки.

- ✓ Для всех проектов с участием финансовых, и приравняваемых к ним, институтов заполнить ПОД/ФТ проверочный лист.
- ✓ По всем остальным проектам только общий проверочный лист. Но в нем ответить ПОД/ФТ вопросы.
- ✓ Фокус на эффективность служб контроля финансовых, и приравняваемых к ним, институтов, а не просто их наличие.
- ✓ Предоплаты кредитов, а также оплата третьими лицами требует усиленной проверки.
- ✓ Если есть сомнения или вопросы следует обращаться в Комплаенс Отдел.



- ✓ Проверка клиента
- ✓ 'Знай своего клиента/контекст'
- ✓ Усиленная проверка в отношении ПЗЛ, и банков-корреспондентов
- ✓ Мониторинг счетов и сообщение о подозрительных операциях
- ✓ Хранение документов / Тренинг персонала
- ✓ Использование международного финансирования
- ✓ Назначение Комплаенс Официера
- ✓ Эффективность



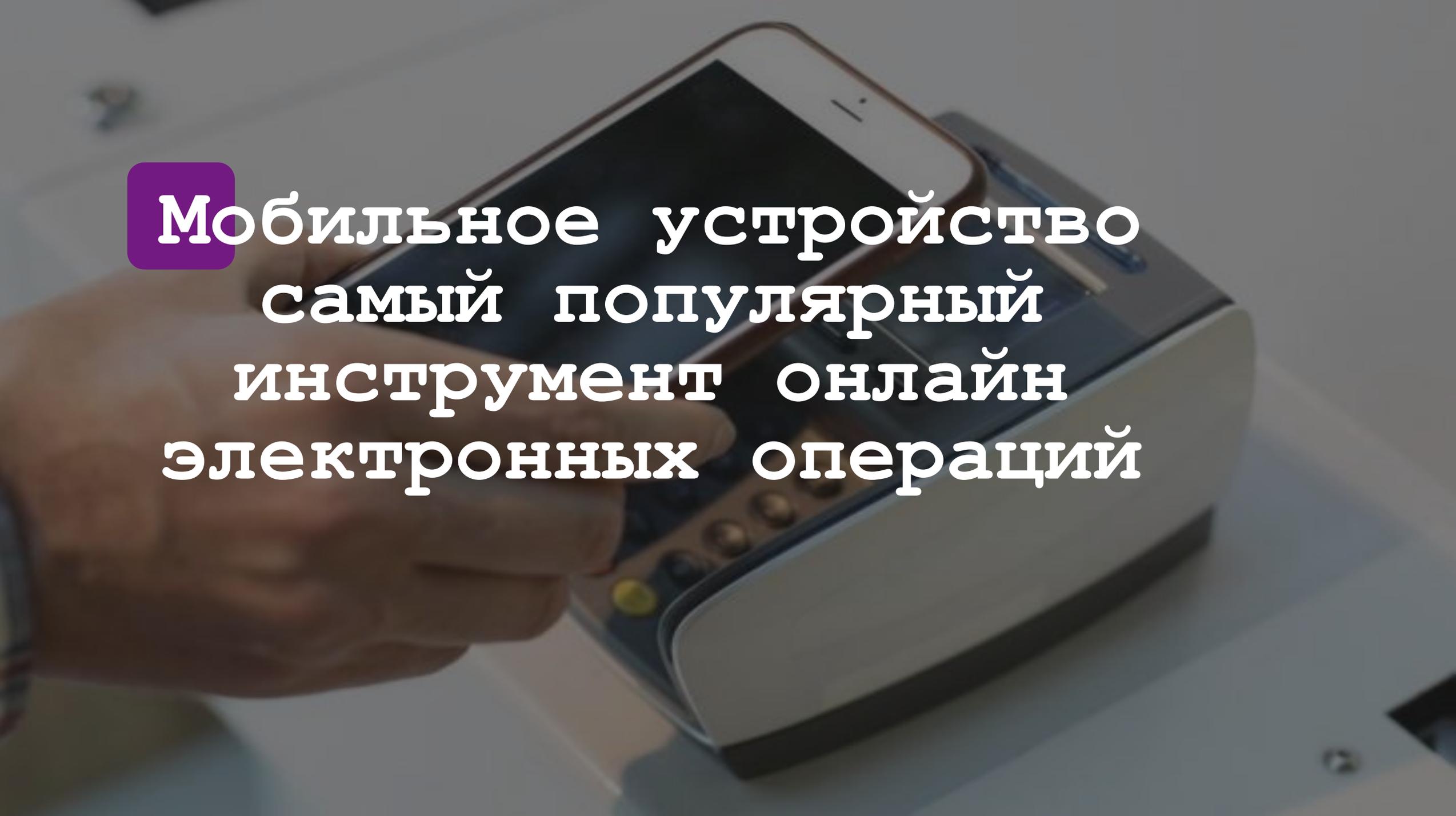
- ✓ Резолюции Совбеза ООН и Рекомендации ФАТАФ
- ✓ Проверка имен/деятельности по спискам ООН
- ✓ Запрет на предоставление финансирования любым лицам, находящимся в списке ООН



Risk. It isn't always
where you expect it to be.

An aerial night photograph of a city, featuring a prominent, brightly lit skyscraper with a distinctive spire. The surrounding urban landscape is visible with various buildings and streets, some of which are illuminated. The overall scene is dark, with the city lights providing the primary illumination.

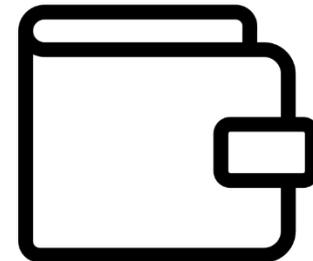
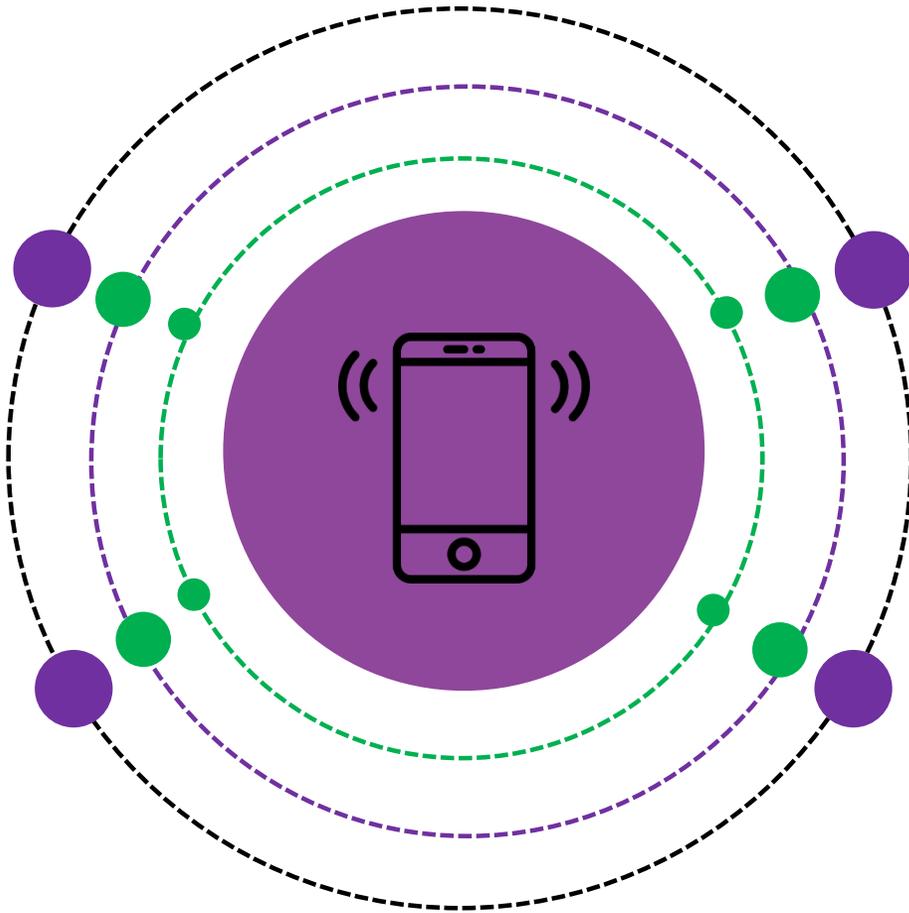
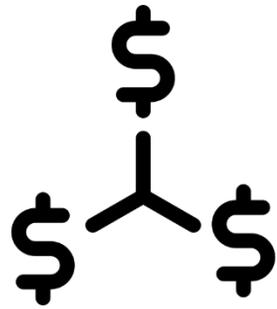
**Финансовый мониторинг и
выявление подозрительной
активности клиентов
телекоммуникационными
компаниями**

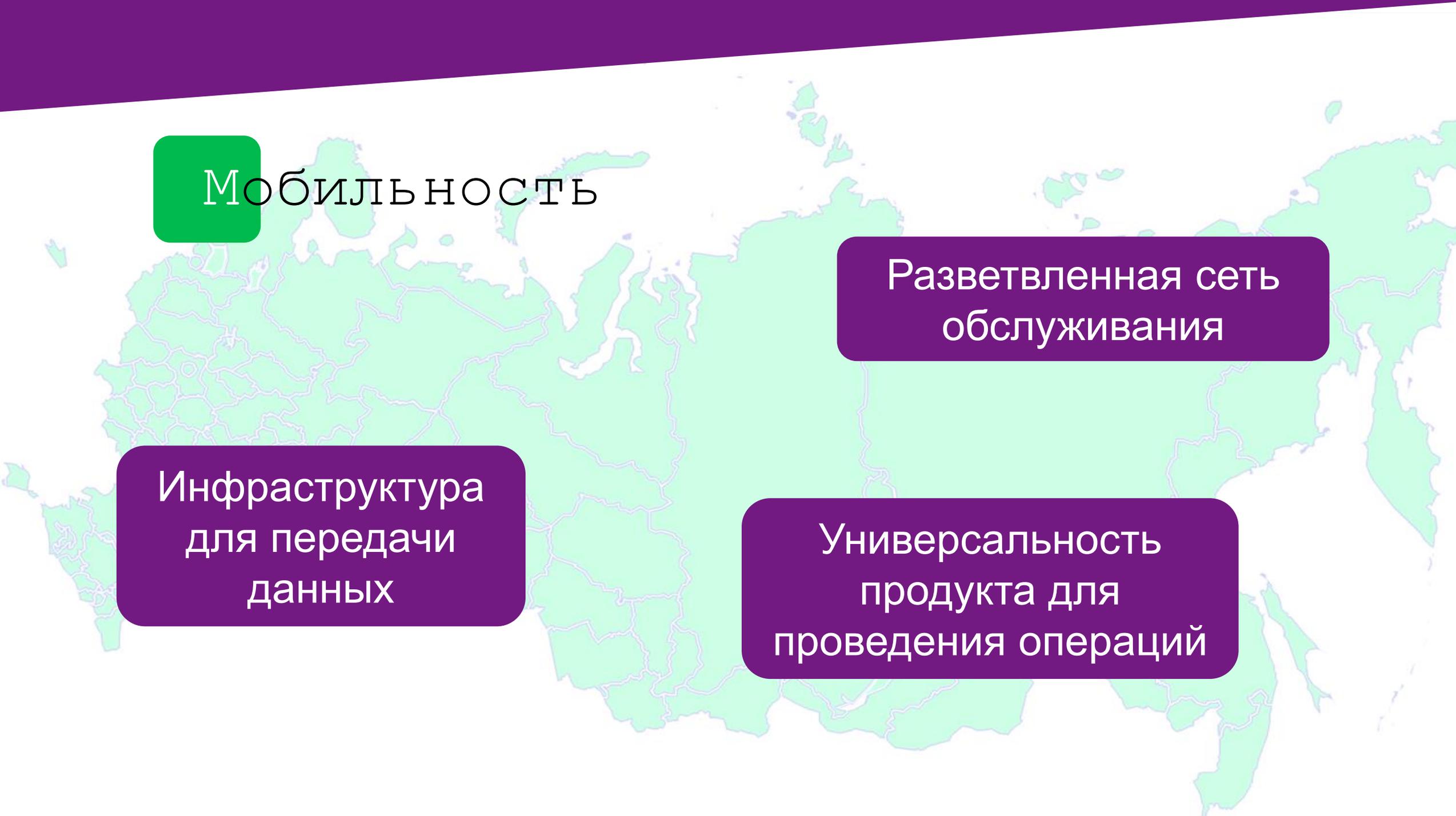
A hand is holding a smartphone over a payment terminal. The terminal has a screen and several buttons. The background is a light-colored surface.

Мобильное устройство
самый популярный
инструмент онлайн
электронных операций



Преимущества мобильного оператора



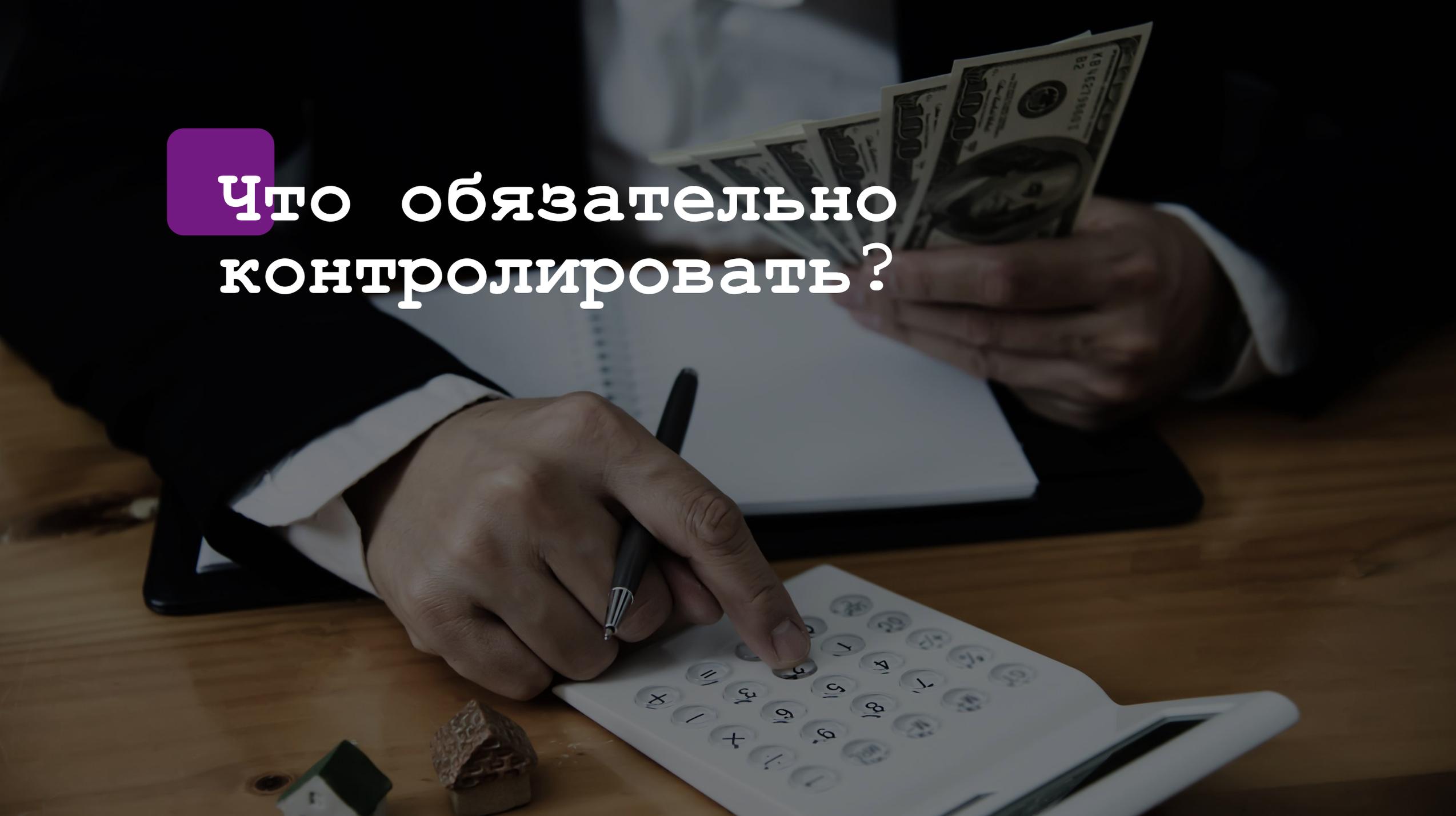


МОБИЛЬНОСТЬ

Разветвленная сеть
обслуживания

Инфраструктура
для передачи
данных

Универсальность
продукта для
проведения операций

A person in a dark suit and white shirt is seated at a wooden desk. Their right hand is holding a stack of US dollar bills, including several 100-dollar bills, and they appear to be counting them. Their left hand is holding a silver pen and is pointing at a white calculator. The calculator is open and shows various numbers and symbols on its keypad. The background is dark and out of focus, emphasizing the person's hands and the financial activity. The text "Что обязательно контролировать?" is overlaid on the image in white, with the word "Что" inside a purple square.

**Что обязательно
контролировать?**

Внимание №1

К операциям с денежными средствами в наличной форме: снятие или зачисление на лицевой счет ЮЛ денежных средств в наличной форме





Внимание №2

К зачислению денежных средств на лицевой счет или списанию денежных средств с лицевого счета ЮЛ, период деятельности которого не превышает трех месяцев со дня его регистрации

Либо те же действия, если операции по указанному лицевому счету не производились с момента его открытия

Внимание №3

К зачислению или переводу на лицевой счет денежных средств, если участник операции имеет регистрацию, место жительства, место нахождения в Республике Иран и КНДР



Banking

Что еще
обязательно
контролировать?

Balance

Monthly

Annual

A man in a dark suit and white shirt is shown from the chest up. A hand-drawn diagram in green dashed lines with six green circular nodes is centered on his chest. The diagram contains the text 'Необычный характер сделки (признаки)'. Surrounding this central text are six text blocks, each connected to a node of the diagram. The background is dark and slightly blurred.

Необычный характер сделки (признаки)

Неоднократное совершение операций, которые могут подлежать обязательному контролю

Зачисление физическому лицу денежных средств от юридического лица

Отказ клиента от совершения разовой операции, в отношении которой возникают подозрения, что она осуществляется в целях ОД/ФТ и ФРОМУ

Перечисление денежных средств в течении короткого промежутка времени на счет отличный от счета с которого данные денежные средства были ранее зачислены

Запутанный или необычный характер операции, не имеющей очевидного экономического смысла или законной цели

Иные обстоятельства, дающие основания полагать, что операции осуществляются в целях ОД/ФТ и ФРОМУ

Осуществление переоформления абонентского номера с переносом денежных средств с ЮЛ физическому лицу

Профиль сомнительной операции

- Аналитика нехарактерных операций
- Взаимодействие с Compliance по формированию типологий сомнительных операций
- Координация Росфинмониторингом применения новых критериев необычных операций

Тенденции



Отказ от использования наличных денег в пользу электронных средств платежа



Вовлечение в сомнительные схемы социально незащищенных слоев населения



Формирование географических локаций

Аналитика нехарактерных операций

Взаимодействие с Compliance по формированию типологий сомнительных операций

Координация Росфинмониторингом применения новых критериев необычных операций

Compliance



Изучение нехарактерных операций



Определение типовых признаков операций

Взаимодействие со всеми субъектами рынка



Рассмотрение полного цикла движения денежных средств



Формирование типологии по выявлению сомнительных операций

Аналитика нехарактерных операций

Взаимодействие с Compliance по формированию типологии сомнительных операций

Координация Росфинмониторингом применения новых критериев необычных операций

Росфинмониторинг

Личный кабинет

Актуальные типологии и признаки сомнительных операций

Новые виды рисков возникновения сомнительных операций

Секторальная оценка рисков

Оценка качества внутреннего контроля

Аналитика нехарактерных операций

Взаимодействие с Compliance по формированию типологий сомнительных операций

Координация Росфинмониторингом применения новых критериев необычных операций

Международное партнерство





Обмен лучшими практиками



Региональные особенности



Миграционная направленность



Трансграничность платежей