

The logo for EAG, consisting of the letters 'EAG' in a bold, white, sans-serif font, set against a dark blue background that is part of a larger graphic design with curved, overlapping shapes in shades of blue and white.

МЕЖДУНАРОДНЫЙ УЧЕБНО-МЕТОДИЧЕСКИЙ ЦЕНТР
МУМЦФМ
ФИНАНСОВОГО МОНИТОРИНГА

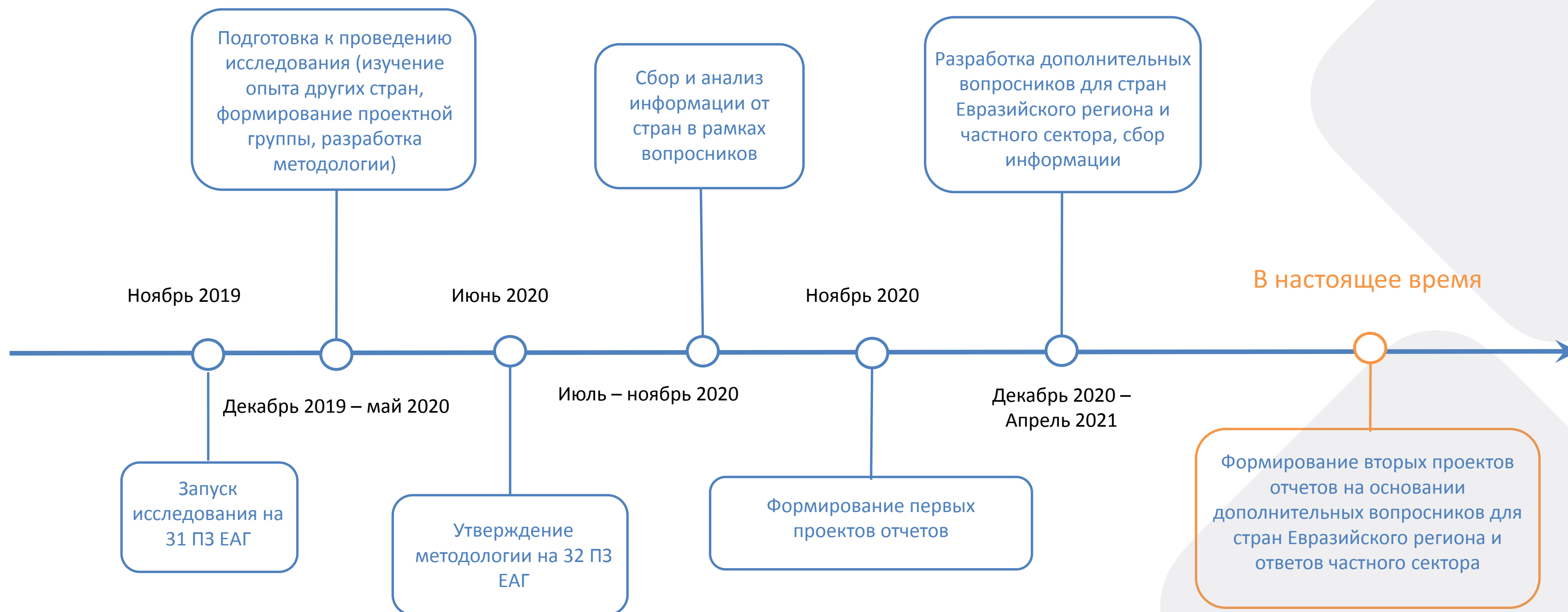
ЗАСЕДАНИЕ МЕЖДУНАРОДНОГО СОВЕТА
КОМПЛАЕНС

СБОРНИК ПРЕЗЕНТАЦИЙ

28-29 апреля 2021 г.

A decorative graphic at the bottom of the page consisting of overlapping, curved shapes in shades of blue and white, mirroring the design at the top.

Методология проведения оценки рисков ОД/ФТ в Евразийском регионе



Методология проведения региональной оценки рисков



ВЫЯВЛЕНИЕ РИСКОВ



Вопросник по наблюдаемым схемам ОД/ФТ

- Перечень схем / методов
- Частота их проявления
- Страны, вовлеченные в схемы

ПОНИМАНИЕ РИСКОВ



Вопросники по факторам угроз и уязвимостей

- Использование способов и инструментов в целях ОД/ФТ
- Определение характера угроз
- Частота совершения преступлений в составе организованных преступных групп
- Определение характера уязвимостей: риск-контекст и организационные факторы

Структура отчетов о проведении региональной оценки рисков ЕАГ

Отчеты по каждому из четырех субрегионов

- ✓ Ключевые угрозы в субрегионе
- ✓ Ключевые уязвимости в субрегионе
- ✓ Риски регионального уровня

Расчет уровня риска регионального уровня

1

ЧАСТОТА
РАЗМЕР СРЕДСТВ

Сводные значения по каждой схеме на основании заполненных странами вопросников

2

ОПРЕДЕЛЕНИЕ РИСКА как совокупности схем с учетом их проявления в рамках совершения различных видов преступлений. Расчет сводных значений частоты и размера средств по каждому риску.

3

РИСК

=

$$\sqrt{\text{ЧАСТОТА}^2 + \text{РАЗМЕР СРЕДСТВ}^2}$$

Расчет рейтингов рисков и их визуализация на тепловой карте

РЕГИОНАЛЬНЫЕ РИСКИ, ТРЕБУЮЩИЕ ЗНАЧИТЕЛЬНОГО ВНИМАНИЯ И ПОВЫШЕННЫХ МЕР К ИХ СНИЖЕНИЮ (ОТ 2-Х ДО 3-Х БАЛЛОВ ВКЛЮЧИТЕЛЬНО)

1.1.	Использование фиктивных и (или) подконтрольных компаний
1.2.	Проведение операций, связанных с обналичиванием, включая покупку наличной выручки
1.3.	Проведение «транзитных» операций по банковским счетам
1.4.	Приобретение движимого/недвижимого имущества на территории/за пределами государства (этап интеграции)
1.5.	Использование электронных средств платежа и криптовалют
1.6.	Инвестирование преступного дохода в создание предприятий либо внесение средств в уставной капитал юридических лиц, в том числе находящихся в третьих странах (этап интеграции)
1.7.	Использование офшорных компаний
1.8.	Использование фиктивных юридических лиц и индивидуальных предпринимателей

РЕГИОНАЛЬНЫЕ РИСКИ, ТРЕБУЮЩИЕ ПОСТОЯННОГО КОНТРОЛЯ И УСИЛЕННЫХ МЕР К ИХ СНИЖЕНИЮ (ОТ 1-ГО ДО 2-Х БАЛЛОВ ВКЛЮЧИТЕЛЬНО)

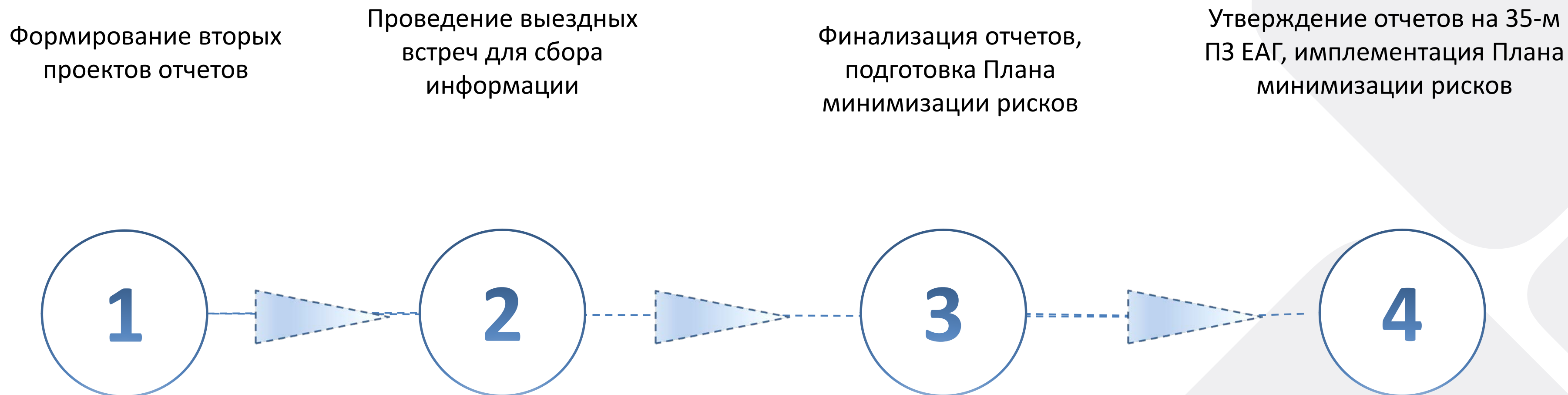
2.1.	Использование доверительных управляющих, трастов, адвокатов и иных лиц, оказывающих услуги по управлению активами
2.2.	Вывод полученных преступным путем денежных средств за пределы субрегиона с последующим возвратом в страны субрегиона в виде инвестиций в законную коммерческую деятельность. (этап интеграции)
2.3.	Легализация похищенных путем совершения кибератак денежных средств
2.4.	Путем использования благотворительных фондов
2.5.	Использование туроператоров
2.6.	Использование невещественных активов

РЕГИОНАЛЬНЫЕ РИСКИ, ТРЕБУЮЩИЕ ПРИНЯТИЯ СТАНДАРТНЫХ МЕР К ИХ СНИЖЕНИЮ (ОТ 0 ДО 1 БАЛЛА ВКЛЮЧИТЕЛЬНО)

3.1.	Использование систем денежных переводов без открытия счета
3.2.	Проведение операций, связанных с приобретением товаров, контента и услуг в сети Интернет
3.3.	Вывод денежных средств за рубеж с использованием инструментов принудительного взыскания
3.4.	Использование курьеров наличных
3.5.	Использование ценных бумаг банков в целях конвертации денег в иностранную валюту, их вывода и обналичивания

Тепловая карта рисков ОД





Спасибо за внимание!

Ак Барс
Банк

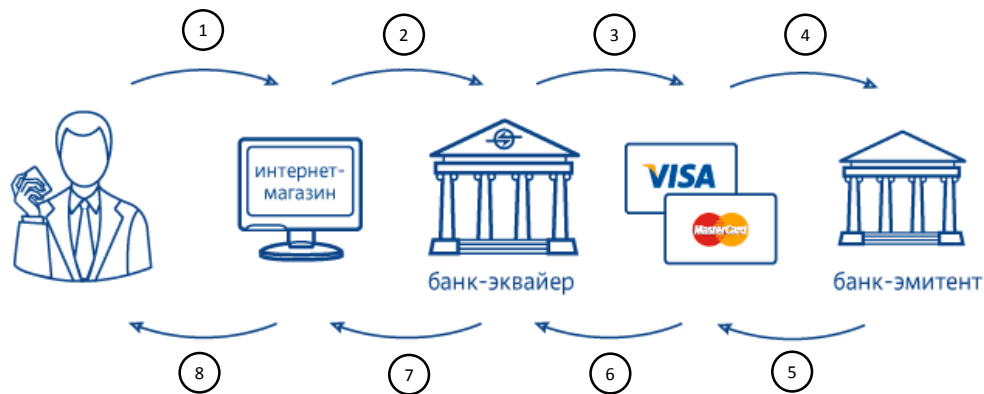


ТАИССР
1920-2020



AML риски в области интернет-эквайринга и способы их минимизации

Интернет эквайринг – общий термин, которым обозначается прием платежей по пластиковым и виртуальным картам через Интернет с использованием специально разработанного web-интерфейса.



1. Клиент совершает покупку в Интернет-магазине.
2. После проведения аутентификации Провайдер направляет информацию для авторизационного запроса Банку эквайеру.
3. Эквайер направляет запрос на авторизацию операции в международную платежную систему.
4. МПС формирует запрос Банку эмитенту

5. Банк эмитент формирует ответ на запрос МПС
6. МПС передает данный ответ Банку эквайеру.
7. Банк эквайер переводит возмещение по совершенным операциям на счет Интернет-магазина и передает информацию о статусе оплаты интернет-магазину.
8. Пользователь получает результаты заказа.

Заключение договора напрямую между Банком и ТСП



- Прямое заключение договора между Банком и ТСП
- Проведение процедур проверки и идентификации ТСП
- Возможно привлечение провайдера для предоставления доп. услуг при приеме платежей (личный кабинет, отчеты и т.д.)

С привлечением платежного фасилитатора



- Банк не заключает договор с ТСП.
- Распределение денежных средств между ТСП осуществляет платежный фасилитатор.
- Банк взаимодействует только с платежным фасилитатором.

Риски в интернет эквайринге связаны в первую очередь с качеством **мерчантов**, которым предоставляется услуга.

Финансовые риски:

- убытки по оспоренным операциям (чарджбэкам);
- комиссии и штрафы от международных платежных систем (МПС) за превышение уровня фрода, запрещенную деятельность, нарушение правил работы;
- штрафы Банка России за несоответствие требованиям законодательства.

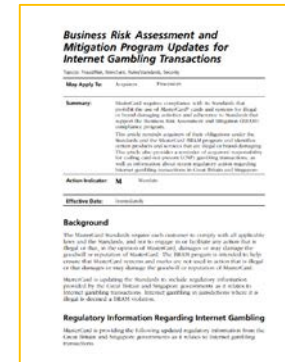
Правовые и репутационные риски:

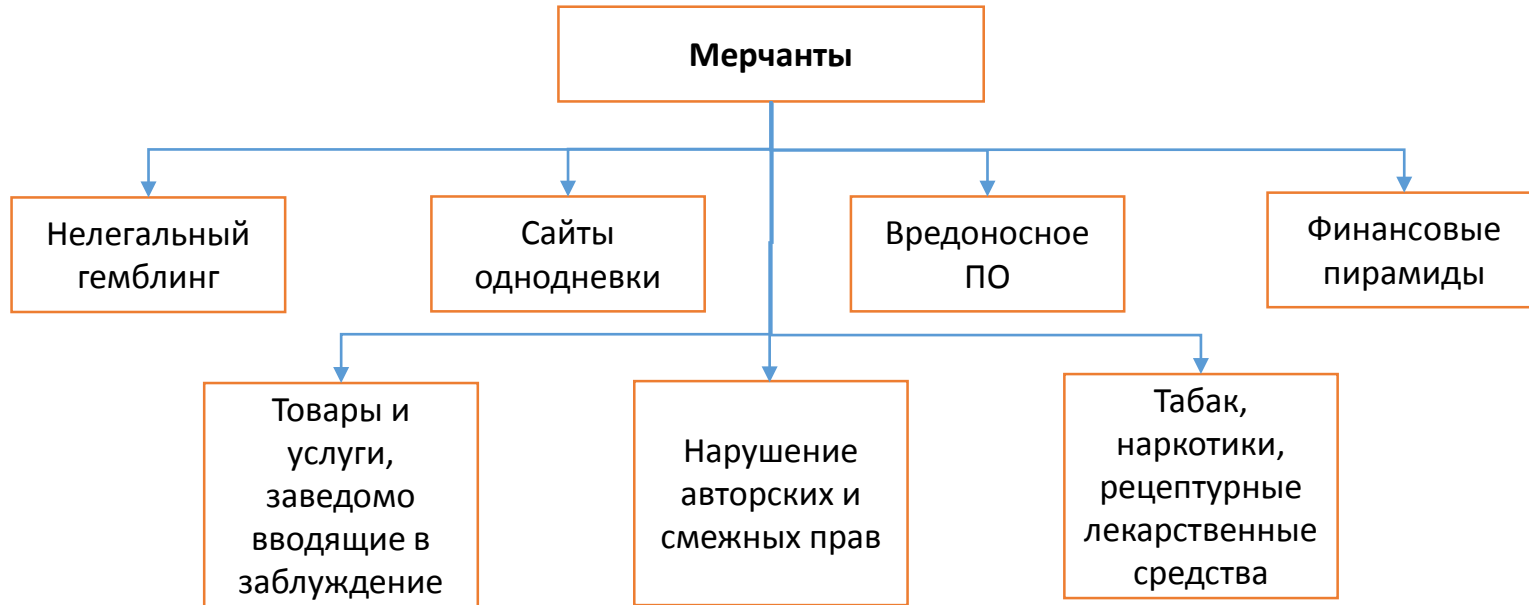
- потеря банком деловой репутации;
- прекращение сотрудничества с клиентами и партнерами;
- последствия от судебных исков со стороны держателей карт.

** известны случаи, когда кардхолдеры специально ищут в работе банков нарушения действующего законодательства (особенно часто в области противодействия отмыванию доходов, полученных преступным путем, и финансированию терроризма), пишут жалобы в ЦБ, Росфинмониторинг и правоохранительные органы.*

Риски, связанные с эквайрингом подробно описаны в документах МПС:

Правила и меры по защите бренда Visa описаны в Global Brand Protection Program (GBPP), аналогичная программа MasterCard называется Business Risk Assessment and Mitigation (BRAM).





Чтобы заниматься интернет-эквайрингом и не попадать под санкции и штрафы, банкам приходится тщательно контролировать своих эквайринговых клиентов.

При работе через фасилитаторов это становится значительно сложнее, так как во многом уровень риска зависит от благонадежности партнера

Причем тут AML?

Для снижения рисков в работе в области интернет эквайринга банки должны обладать определенной зрелостью в части **реализации принципа «Знай своего клиента» (KYC)**



Мискодинг (miscoding) – это отдельный вид мошенничества в банковской эквайринговой сети, которое заключается в подмене назначения платежа.

- Чаще всего к мискодингу прибегают нелегальные онлайн казино и букмекеры. Нелегальному игорному бизнесу, на фоне законодательного запрета на проводимую деятельность, жизненно необходимо обеспечить прием ставок с банковских карт и пополнение игровых аккаунтов.
- Также такую схему используют криптообменники и онлайн-мошенники для прямого обмана потребителей.
- Законно получить эквайринговый терминал с мерчант кодом MCC 7995 Betting / Casino Gambling могут только те компании, которые имеют соответствующие разрешения на ведение гемблинговой деятельности. Обычно это строго регламентируется и проверяется платежными системами Visa и MasterCard и банком-эквайером.
- Благодаря мискодингу недобросовестным участникам рынка удастся обманным путем проходить первичную проверку финансового мониторинга банка, где зарегистрирован их терминал. Для этого заявляется любая другая деятельность – прием платежей ЖКХ, обучение, онлайн кинотеатры, торговля и услуги и пр., а сайт меняет свое наполнение. Эту теневую схему можно считать классическим примером отмывания денег.
- Банк-эквайер должен идентифицировать все такие сделки, а банк-эмитент карточек – знать характер этих операций. Подмена и использования фейковых MCC-кодов является грубым нарушением правил МПС.

MCC код: 0000, 0763, 1799, 2791, 2842, 4214, 4225, 4813, 4815, 4829, 4900, 5044, 5046, 5047, 5051, 5169, 5199, 5271, 5551, 5935, 5960, 5962, 6010, 6011, 6012, 6022, 6023, 6025, 6026, 6028, 6050, 6051, 6211, 6381, 6399, 6513, 6529, 6530, 6531, 6532, 6533, 6534, 6535, 6536, 6537, 6538, 6540, 6611, 6760, 7012, 7273, 7276, 7277, 7279, 7280, 7311, 7321, 7322, 7372, 7389, 7392, 7393, 7511, 7995, 8111, 8211, 8220, 8241, 8244, 8249, 8299, 8398, 8641, 8651, 8661, 8675, 8699, 8734, 8911, 8931, 9211, 9222, 9223, 9311, 9399, 9401, 9402, 9405, 9411, 9702, 9753, 9950

Как усилить внутренний контроль в интернет-эквайринге

- Зачастую в Банках присутствуют **недостатки внутреннего контроля** на следующих этапах процесса:
- привлечение на обслуживание, предварительный отсев высокорисковых мерчантов;
 - проверка интернет-магазинов, анализ деятельности клиента и актуализация информации;
 - формирование профиля интернет-магазина (средние обороты, средний чек и т.д.) и отслеживание изменений в поведении и профиле клиента;
 - регистрация терминалов и присвоение МСС кода (риск мискодинга);
 - контроль за использованием терминалов, установление ключевых индикаторов риска;
 - мониторинг фрода и реагирование на него;
 - контрольные механизмы банков в области интернет эквайринга не описаны в их ПВК.



Правоохранительные органы в некоторых странах используют как один из механизмов выявления нарушений в сфере интернет-эквайринга **контрольные закупки**.

Аналогичные инструменты могли бы существенно повысить эффективность системы внутреннего контроля кредитной организации

Ак Барс
Банк



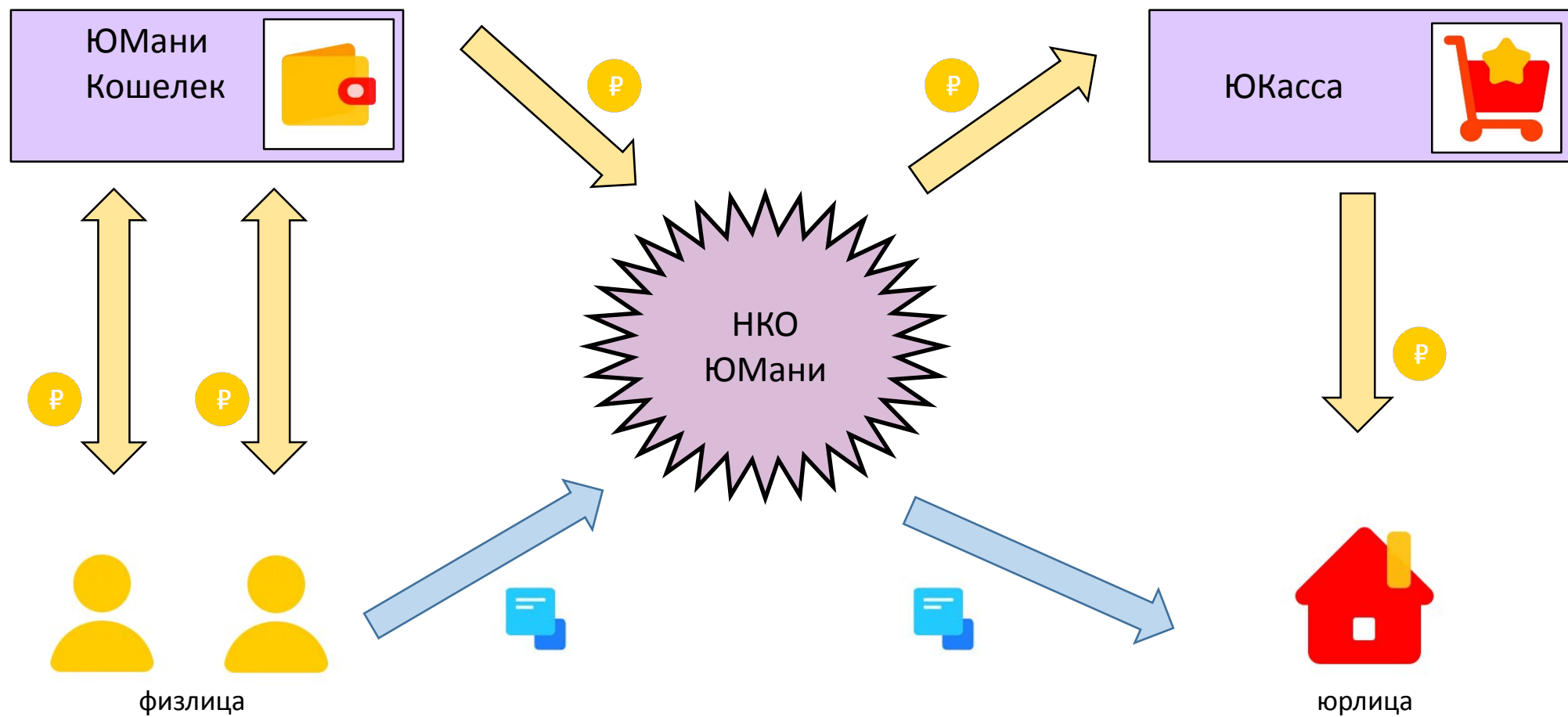
Благодарю за внимание



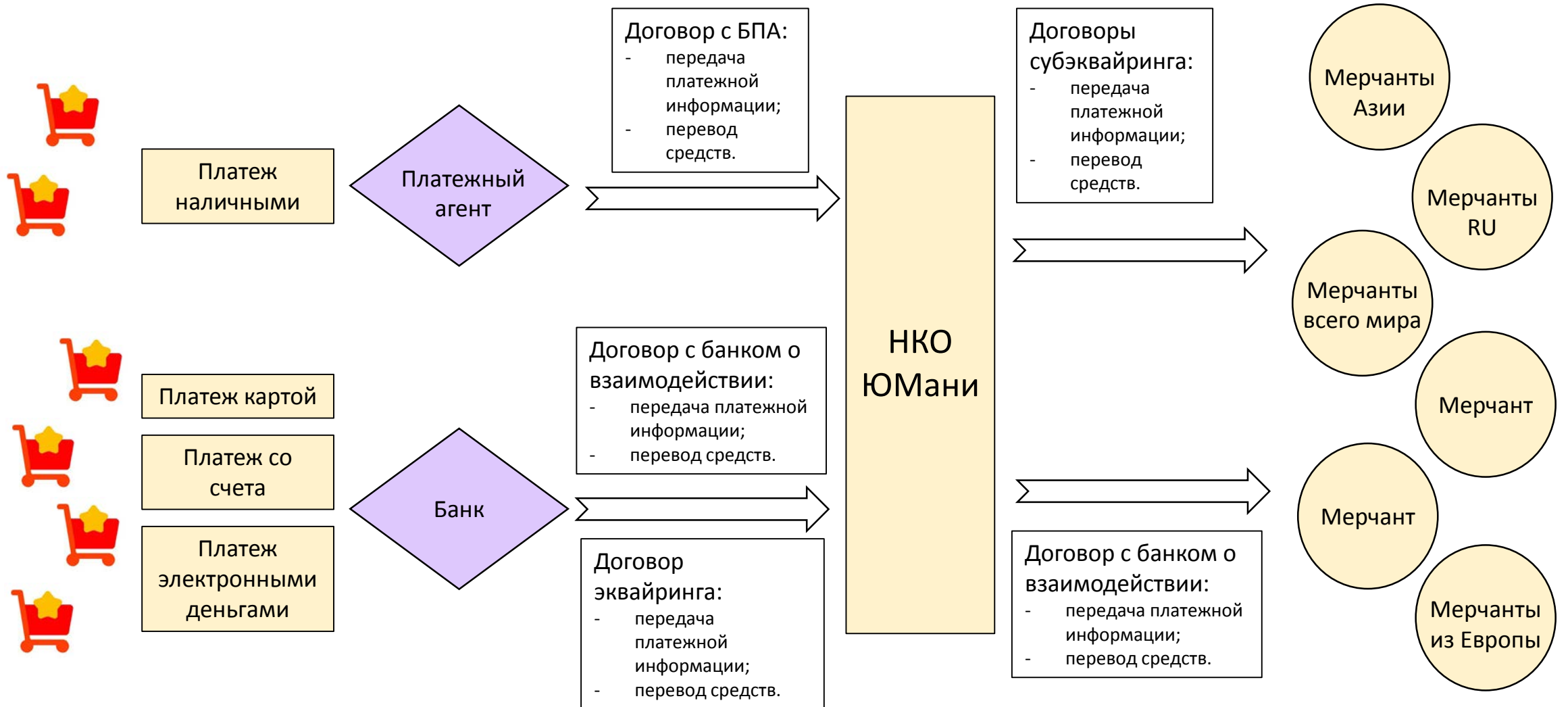
Противоправные типологии в сервисе электронных денег и автоматизированные средства их выявления

Дмитрий Гронин,
Руководитель службы внутреннего контроля

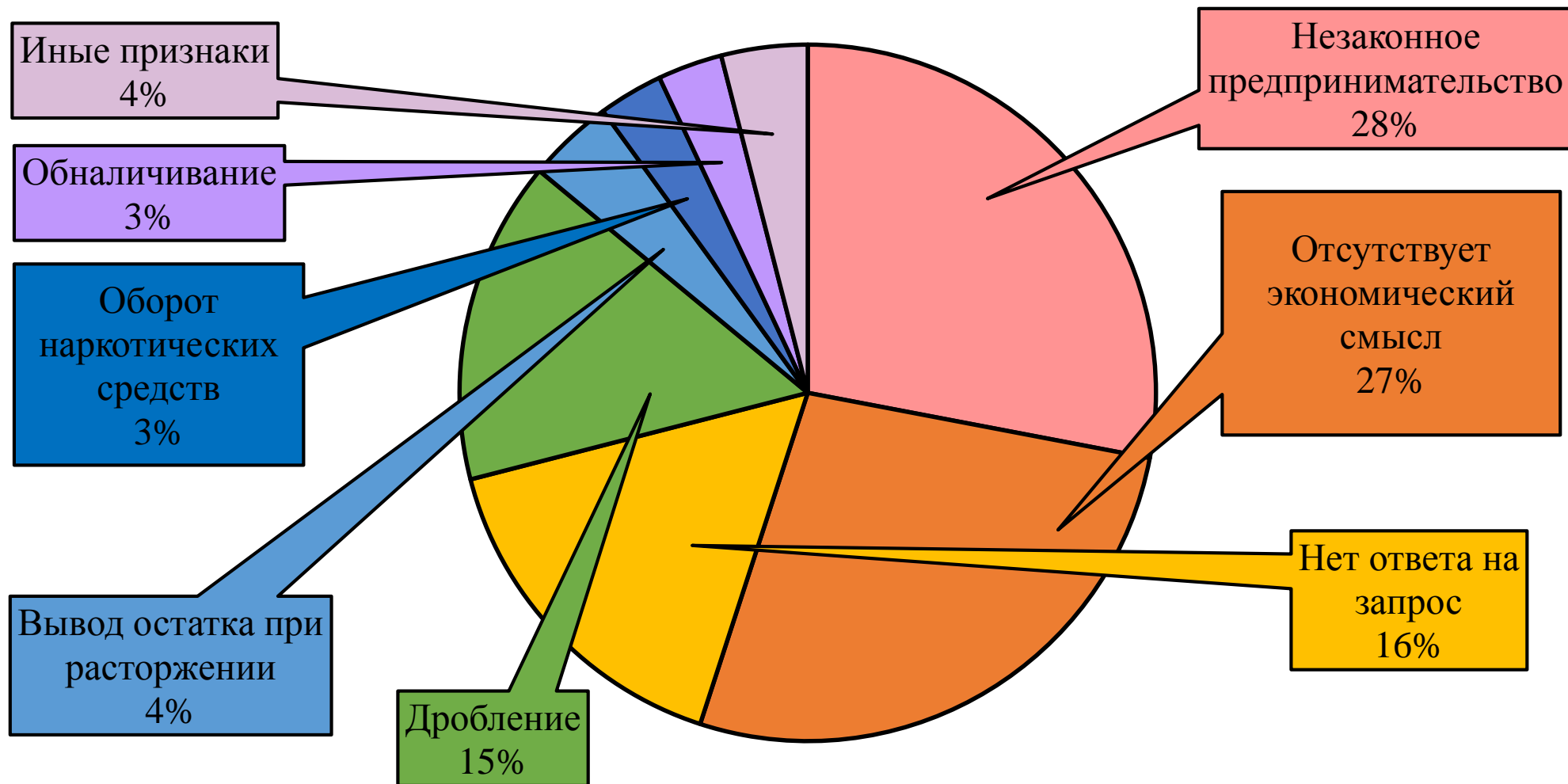
Наши основные сервисы



ЮКасса

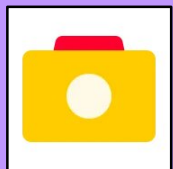


Структура основных направлений репортинга-2020



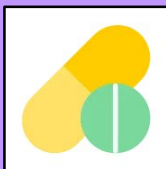
Противоправные типологии

Незаконное предпринимательство



- Продажа товаров/услуг;
- Платный доступ к контенту;
- Криптообменники;
- Валютные обменники;
- Системы переводов;
- Сбор инвестиций/пирамиды.

Оборот запрещенной продукции



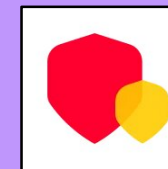
- Наркотики;
- Оружие;
- Химически активные и взрывчатые вещества;
- Оборот виртуальных ценностей (контрафакт).

Обналичивание через «дропов»



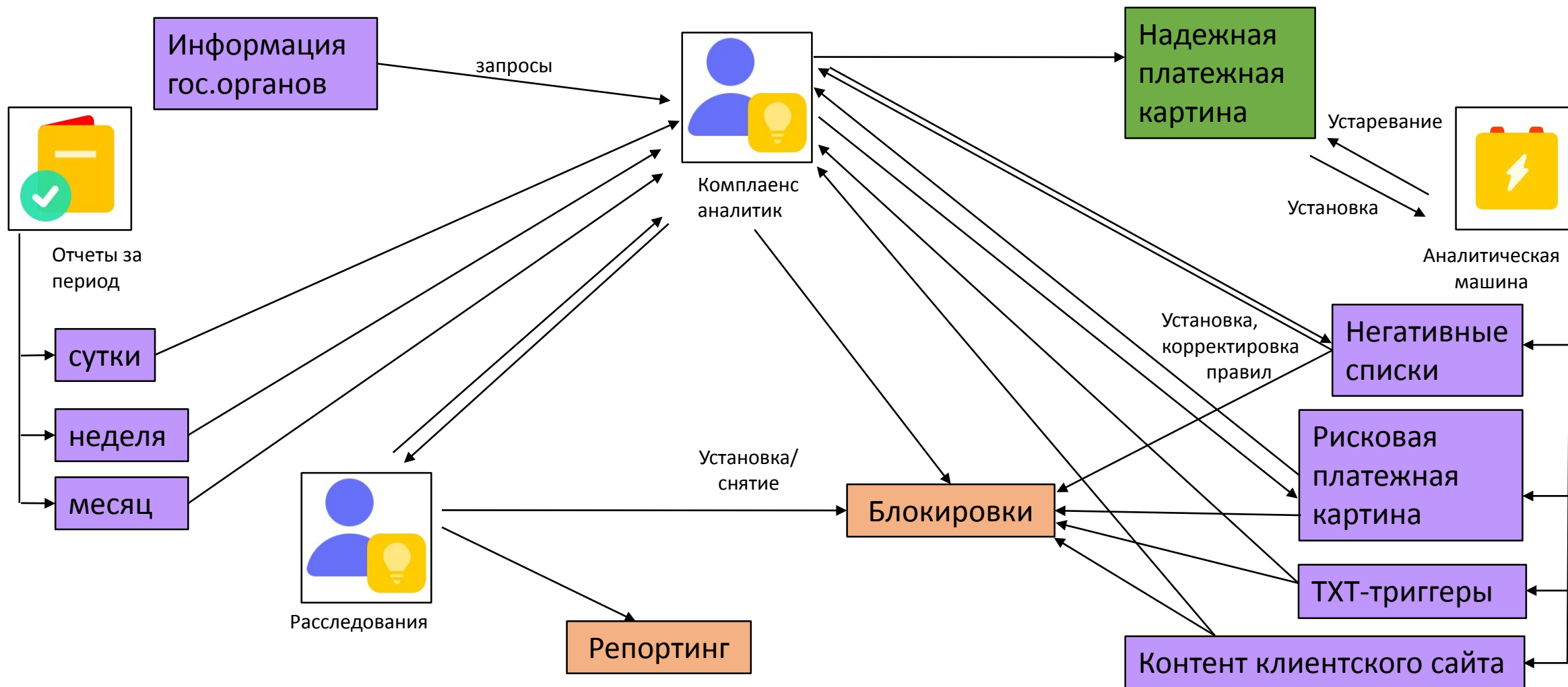
- Соккрытие от налогов;
- Бюджетные нарушения;
- Формирование взяточной массы;
- Хищения;
- Вброс фальшивых купюр;
- Мошенничество.

НСД и прочее



- Технический взлом аккаунта;
- Социальная инженерия;
- Подделка нотариальных и иных документов;
- «Схема» с фиктивными исполнительными документами.

Мониторинг потоков электронных денег





Глобальные пересечения

устройства, cookie
идентификаторы
средства платежей
география
email
телефоны
IP, источники пополнений
...



Искусственный интеллект (аналитическая машина)

- Самообучаемая модель проверки сайтов мерчантов;
- Модели выявления НДС;
- Выявление платежных аномалий на кошельках;
- Модели выявления аномальных и недобросовестных продаж (с учетом мониторинга цен и отзывов в сети);
- Выявление роботизированного управления кошельком.

Региональные способы отмывания денег. Презентация результатов предварительного опроса частного сектора

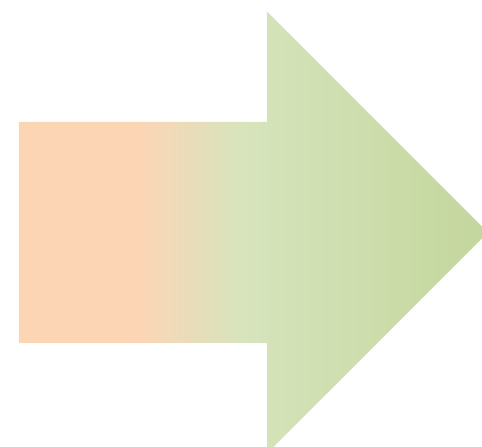
1 Со счетов номинальных компаний

Способ ОД	Среднее значение	Страны						
		Казахстан	Кыргызстан	Таджикистан	Узбекистан	Россия	Китай	Туркменистан
<i>внутри страны</i>								
с последующим переводом на счета юридических лиц, обладающих признаками фирм-однодневок;	1,57	1,28	1,37	1,30	2,50	3,00	2,00	0,00
с последующим переводом на счета индивидуальных предпринимателей;	1,42	1,42	1,00	1,20	1,50	2,60	2,00	0,00
с последующим переводом на счета физических лиц.	1,40	1,35	0,75	1,20	1,50	3,00	2,00	0,00
<i>с последующим переводом в офшорные юрисдикции</i>								
на счета иностранных юридических лиц, обладающих признаками фирм-однодневок;	1,35	1,35	1,25	1,20	1,50	2,20	1,00	0,00
на счета иностранных юридических образований;	1,14	1,50	1,25	0,90	0,50	1,40	0,00	0,00
<i>с последующим переводом в страны Евразийского региона</i>								
на счета иностранных юридических лиц, обладающих признаками фирм-однодневок;	1,19	1,07	1,00	1,40	1,00	1,80	1,00	0,00
на счета иностранных юридических образований;	1,00	1,00	1,25	1,10	0,50	1,20	0,00	0,00
<i>с последующим переводом в иные страны</i>								
на счета иностранных юридических лиц, обладающих признаками фирм-однодневок;	1,23	1,14	1,25	1,20	1,00	2,00	1,00	0,00
на счета иностранных юридических образований.	1,07	1,35	1,25	0,90	0,50	1,20	0,00	0,00

Риск ОД из промежуточного отчета по субрегиону «Использование фиктивных и подконтрольных компаний»

Тенденции использования юридических лиц в схемах ОД

«Классические»
НОМИНАЛЬНЫЕ
КОМПАНИИ



Реально
действующие
КОМПАНИИ

Использование различных типов лиц в операциях, связанных с ОД

Тип лица	Среднее значение	Страны						
		Казахстан	Кыргызстан	Таджикистан	Узбекистан	Россия	Китай	Туркменистан
Общества (товарищества) с ограниченной ответственностью	1,75	1,85	1,66	1,33	2,50	2,75	1,50	0,00
Физические лица	1,70	1,85	1,44	1,55	2,00	2,75	1,00	0,00
Индивидуальные предприниматели	1,61	1,78	1,30	1,55	1,50	2,00	2,00	1,00
Фонды	1,25	1,28	1,12	1,44	1,00	1,75	0,50	0,00
Акционерные общества	1,04	0,78	1,11	1,33	2,00	0,75	1,50	0,00
Юридические образования	0,97	1,08	1,42	0,87	0,50	1,00	0,00	0,00
Потребительские кооперативы	0,92	1,30	0,44	1,11	0,50	1,25	0,00	0,00

2 С использованием банковских счетов и карт физических лиц

Способ ОД	Среднее значение	Страны						
		Казахстан	Кыргызстан	Таджикистан	Узбекистан	Россия	Китай	Туркменистан
С использованием банковских счетов и карт физических лиц	1,47	1,21	1,25	1,30	1,00	2,80	3,00	0,00

Риск ОД из промежуточного отчета по субрегиону «Отмывание доходов с использованием банковских платежных карт и банковских счетов»

Способ ОД	Среднее значение	Страны						
		Казахстан	Кыргызстан	Таджикистан	Узбекистан	Россия	Китай	Туркменистан
<i>перемещение средств с использованием нерегулируемых субъектов</i>								
виртуальных валют;	0,85	0,78	0,37	1,20	0,50	1,80	0,00	0,00
неформальных систем денежных переводов (хавала и пр.).	0,76	0,35	0,50	0,80	1,00	1,60	2,00	1,00
платежных систем, обеспечивающих передачу между пользователями неких титульных знаков, позволяющих оплачивать ими товары и услуги;	0,64	0,57	0,25	0,90	1,00	1,20	0,00	0,00

Риски ОД из промежуточного отчета по субрегиону «Использование электронных средств платежа и криптовалют», «Использование курьеров наличных»

Перевод средств из безналичной формы в наличную

Способ ОД	Среднее значение	Страны						
		Казахстан	Кыргызстан	Таджикистан	Узбекистан	Россия	Китай	Туркменистан
Снятие с банковских карт физических лиц	1,78	1,71	2,00	1,40	1,50	2,80	2,00	0,00
Снятие с корпоративных банковских карт фирм-однодневок	1,33	1,64	0,50	1,20	1,00	3,00	0,00	0,00
Покупка наличной иностранной валюты	1,52	1,50	1,62	1,60	1,00	2,00	1,00	0,00

Риск ОД из промежуточного отчета по субрегиону «Проведение операций, связанных с обналичиванием, включая покупку наличной выручки»

Перевод средств из наличной формы в безналичную

Способ ОД	Среднее значение	Страны						
		Казахстан	Кыргызстан	Таджикистан	Узбекистан	Россия	Китай	Туркменистан
На банковские счета физических лиц	1,69	1,64	2,25	1,20	1,50	2,20	2,00	0,00
На счета организаций, ведущих реальную финансово-хозяйственную деятельность	1,23	1,14	2,12	1,10	0,50	0,80	1,00	1,00
Через кассу организаций, обладающих признаками фирм-однодневок	1,00	0,85	0,75	1,10	1,50	2,00	0,00	0,00
Приобретение векселей	0,47	0,07	0,5	0,50	0,00	2,00	0,00	0,00

Риски ОД из промежуточного отчета по субрегиону:

- ❑ «Использование фиктивных юридических лиц и индивидуальных предпринимателей»;
- ❑ «ОД с использованием банковских платежных карт и банковских счетов»

Способ ОД	Среднее значение	Страны						
		Казахстан	Кыргызстан	Таджикистан	Узбекистан	Россия	Китай	Туркменистан
Купля-продажа наличной иностранной валюты	1,75	1,71	2,75	1,80	1,50	0,75	1,00	0,00
<i>переводы без открытия банковского счета</i>								
с физическими лицами на территории страны;	1,57	1,21	2,50	1,30	1,50	1,60	2,00	1,00
с физическими лицами в других странах	1,54	1,07	2,25	1,70	1,50	2,00	1,00	0,00
с физическими лицами в странах с повышенным уровнем наркотрафика	1,30	1,00	1,00	1,60	2,00	1,80	2,00	0,00

Риск ОД из промежуточного отчета по субрегиону «Использование систем денежных переводов без открытия счета», «использование курьеров наличных»

1 Размещение денежных средств на банковских счетах/вкладах

Способ ОД	Среднее значение	Страны						
		Казахстан	Кыргызстан	Таджикистан	Узбекистан	Россия	Китай	Туркменистан
Размещение денежных средств на банковских счетах/вкладах	1,69	1,42	2,37	1,50	1,00	2,00	2,00	1,00

Риск ОД из отчета субрегиона «Отмывание доходов с использованием банковских платежных карт и банковских счетов»

2 Сделки с недвижимым имуществом

Способ ОД	Среднее значение	Страны						
		Казахстан	Кыргызстан	Таджикистан	Узбекистан	Россия	Китай	Туркменистан
<i>за наличный расчет</i>								
внутри страны;	1,48	1,57	2,14	1,10	2,00	1,40	0,00	2,00
в странах Евразийского региона;	0,89	0,85	1,20	1,22	0,50	0,80	0,00	0,00
в офшорных юрисдикциях;	0,89	1,00	0,60	1,33	0,50	0,80	0,00	0,00
в иных странах.	0,76	0,71	0,60	1,33	0,50	0,60	0,00	0,00
<i>за безналичный расчет</i>								
внутри страны;	1,30	1,50	1,75	0,70	0,50	1,40	2,00	1,00
в странах Евразийского региона;	1,00	0,92	1,71	0,80	0,50	1,00	1,00	0,00
в иных странах;	0,97	0,78	1,42	1,00	1,00	1,00	1,00	0,00
в офшорных юрисдикциях.	0,92	1,07	0,57	1,10	0,50	1,00	1,00	0,00

Риск ОД из промежуточного отчета по субрегиону «Приобретение недвижимого имущества на территории/за пределами государства»

3) Иные способы

Способ ОД	Среднее значение	Страны						
		Казахстан	Кыргызстан	Таджикистан	Узбекистан	Россия	Китай	Туркменистан
Погашение ранее оформленных кредитов	1,20	1,14	1,57	1,33	0,00	1,40	1,00	0,00
Оплата юридических услуг	1,02	1,21	1,37	0,80	0,00	1,40	0,00	0,00
Приобретение драгоценных металлов, драгоценных камней и ювелирных изделий	1,02	0,71	1,12	1,10	1,00	1,40	1,00	2,00
Оплата нотариальных услуг	0,83	1,00	1,37	0,40	0,00	1,20	0,00	0,00
Передача денежных средств в доверительное управление иностранным юридическим образованиям	0,80	0,64	0,71	0,90	0,00	1,60	1,00	0,00
Оплата аудиторских услуг	0,75	0,85	1,00	0,60	0,00	1,20	0,00	0,00
Приобретение векселей	0,65	0,21	1,14	0,70	0,00	1,80	0,00	0,00

Риск ОД из промежуточного отчета по субрегиону «Использование доверительных управляющих, трастов, адвокатов и иных лиц, оказывающих услуги по управлению активами»

Спасибо за внимание!

Тема: Субъекты повышенного внимания.
Портрет высокорискового клиента, его
финансовое поведение (клиенты -
юридические лица).

Акционерно-коммерчески банк “Узпромстройбанк”

Введение: актуальность вопроса

- стандарты ФАТФ и национальное законодательство Узбекистана;
- система ПОД/ФТ/ФРОМУ Узбекистана
- кризис 2008 года, COVID-19;
- Технологические и современные аспекты рисков ПОД/ФТ/ФРОМУ.

Роль регуляторов в совершенствовании механизмов НПК: методология

- Практика банков и других организаций + обновление;
- Передача рекомендаций банкам;
- Хаб информации по новым реализуемым технологиям;
- Статистическая информация по фрод-инцидентам банков;
- Соавтор нормативных и рекомендательных документов по ПОД/ФТ/ФРОМУ.

Роль регуляторов в совершенствовании механизмов НПК: практические кейсы

- Соответствие операций виду деятельности, результаты изучения места деятельности порождает сомнение;
- Внезапный крупный оборот;
- Вторичные и последующие счета;
- Несоответствие места деятельности и регистрации клиентов;
- Крупные обороты корпоративных карт клиентов;
- Источниками поступлений юридического лица являются кредитные ресурсы;
- Крупные наличные поступления (в качестве экспортной выручки, вклада в уставный фонд).

Роль ПФР в совершенствовании механизмов НПК: методология

- Хотя ПФР более ориентировано на финансово-экономические преступления, практика ПФР связана и с уголовными преступлениями;
- Источник информации по международным валютным схемам операций;
- Единственный источник информации по трансграничным наличным перевозкам;
- Самый широкий доступ к международным и базам данных по физическим/юридическим лицам;
- Подозрительные операции всех организаций, аккумулируются в ПФР
- Концентратор практических схем и способов незаконных операций, в том числе направленных на ОД/ФТ;
- У ПФР имеется набор учебно-методических материалов по профилям высокорискованных юридических лиц, в том числе преступных групп.

Роль ПФР в совершенствовании механизмов НПК: практические кейсы

Кейс А. Лицензируемые виды деятельности:

- Одна или несколько входящих операций клиента по деталям платежа и целям договоров являются обязательными к лицензированию, но у клиента нет лицензии на такую деятельность вообще;
- Одна или несколько входящих операций клиента по деталям платежа и целям договоров являются обязательными к лицензированию, у клиента есть лицензия, но она предназначена для другого типа деятельности;
- Рекомендованные со стороны ПФР меры:
- Мониторинг операций юридических лиц, проверка лицензий и их верификация.

Роль ПФР в совершенствовании механизмов НК: практические кейсы

Кейс Б. Операции по импорту товаров или услуг, в осуществление которых вовлечены разные стороны:

- Резидент РУз осуществляет импорт;
- Сумма достаточно крупная, по крайней мере речь идет сотни тысяч долларов;
- Контракт клиента введен в Единую электронную информационную систему внешнеторговых операций (государственная система);
- Но если посмотреть контракт, то Производитель находится в стране А, поставка будет осуществлена компанией, находящейся в стране Б, банк контрагента находится в стране В, а грузоотправитель находится в стране Г.
- Рекомендованные со стороны ПФР меры:
- Мониторинг операций юридических лиц, представление сомнительной операции.

Роль ПФР в совершенствовании механизмов НПК: практические кейсы

Кейс В. *Операции по поручительству крупных юридических лиц:*

- Компания А и Компания Б заключают сделку о возвратном займе;
- Компания А является получателем займа и как гарантия для Компании Б даёт поручительства более крупной Компании В (может быть и с государственной долей);
- Так как эта схема проработана в результате сговора между представителями 3-х компаний, Компания А не возвращает средства Компании Б, а Компания Б естественно подаёт в суд Компанию А по невозврату средств;
- На основании договора поручительства, суд решает в перечислить от компании В средства компании Б, и Компания Б очень быстро перечисляет средства разным юридическим или физическим лицам, то есть происходит искусственное получение средств за счёт убытков Компании В.
- Рекомендованные со стороны ПФР меры:
- Мониторинг операций юридических лиц, обращение особого внимания операциям, связанным с договорами поручительства или уступки права требования.

Региональные угрозы и факторы уязвимостей по линии отмывания денег

Евразийская группа по противодействию легализации
преступных доходов и финансированию терроризма (ЕАГ)

Докладчик: Назерке Жампейис (Секретариат ЕАГ)

Угрозы - источники преступного дохода первой степени

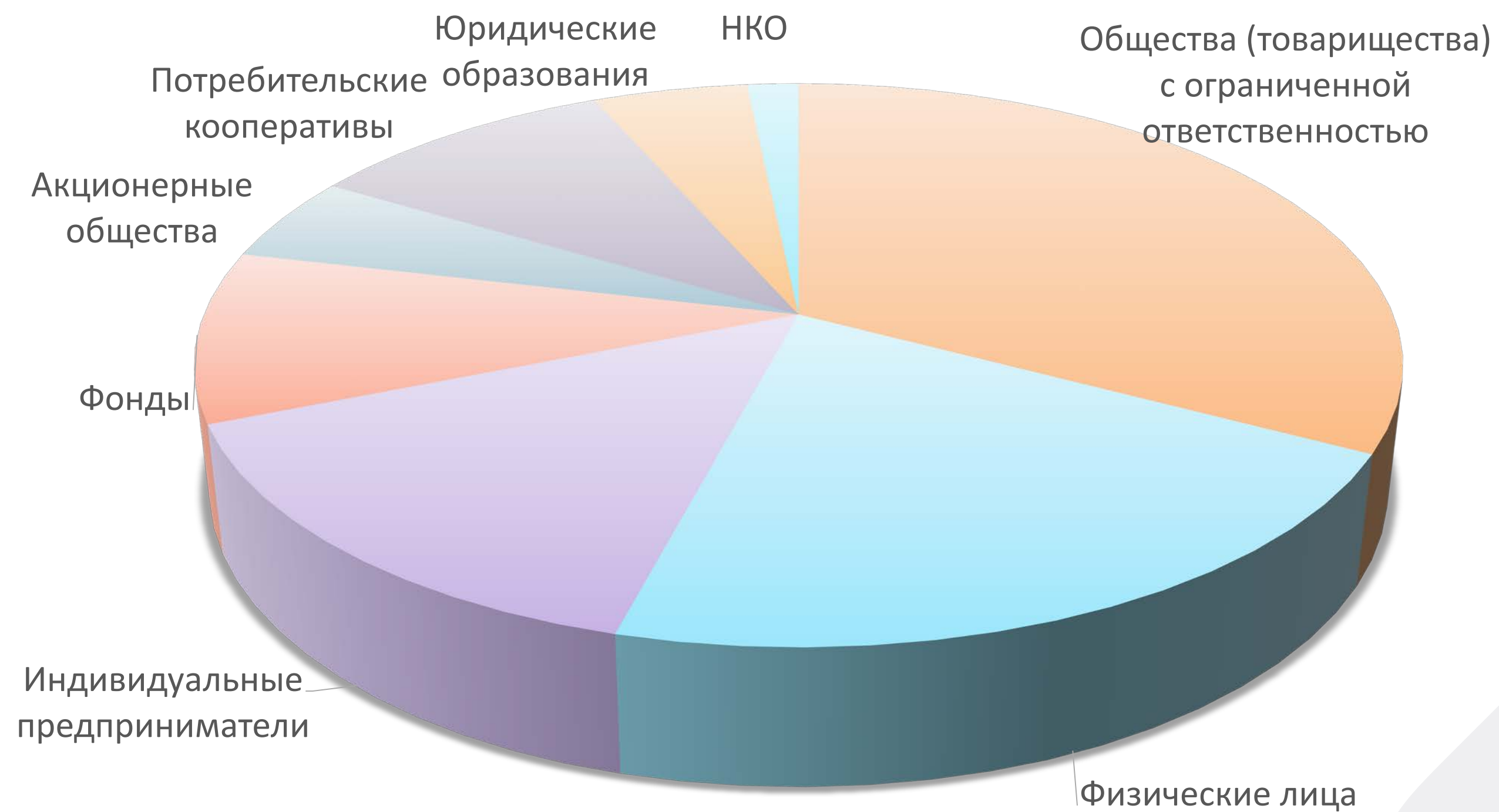


Угрозы – источники преступного дохода второй степени



Угрозы – источники преступного дохода третьей степени





ФИНАНСОВЫЙ СЕКТОР

(банки и небанковские кредитно-финансовые организации)



VS

СЕКТОР УНФПП

(бухгалтеры, казино, дилеры по драгоценным металлам и камням, организаторы азартных игр, юристы, нотариусы, риэлторы)



Уязвимости – риск контекст



Заинтересованность в незаконном выводе средств за рубеж



Высокий уровень расчетов наличными деньгами



Пробелы в регулировании и осуществлении государственного контроля

- за новыми финансовыми продуктами и услугами, включая электронные денежные средства (электронные кошельки, криптовалюты)
- за теневым сектором экономики



Возможность использования номинальных юридических лиц



Внедрение новых продуктов и технологий в финансовой сфере



Пробелы в регулировании и организации внутреннего контроля в сфере УНФПП и финансовой сфере





По итогам проекта ROP включить в планы технического содействия проведение обучений для УНФПП и обучений для всех подотчетных организаций по ознакомлению с типологиями, по работе с санкционными списками и по иным темам, определенным по итогам анкетирования



Привлечение ЕАГ при проведении обучений



Направление ПФР и иными компетентными органами в адрес частного сектора информационных сообщений об актуальных типологиях ОД



Разработка единой методологии квалификации операций



Формирование перечня должностей или перечня НПДЛ.

Разработка Руководства по разъяснению требований Р.12 (предложение представителя Таджикистана)



Разработка методологии выявления бенефициарных владельцев на основе типовых схем собственности и контроля



Повышение осведомленности населения о требованиях законодательства в сфере ПОД/ФТ



Иные предложения?

**Спасибо за
внимание!**

Проекты технического содействия Российской Федерации в контексте региональной оценки рисков ОД/ФТ

Иванов Олег Алексеевич - первый заместитель генерального директора МУМЦФМ

Применение результатов региональной оценки рисков

Региональная оценка рисков



Корректировка программ ТС в сфере ПОД/ФТ



Тренинги

РОП в деятельности ФУ, УНФПП
и надзорных органов



Электронные сервисы в сфере
ПОД/ФТ

Доступны в тестовом режиме на
платформе МУМЦФМ с
01.07.2021

Электронные сервисы в сфере ПОД/ФТ



- Национальный центр оценки рисков ОД/ФТ



- Личный кабинет организации



- Личный кабинет надзорного органа



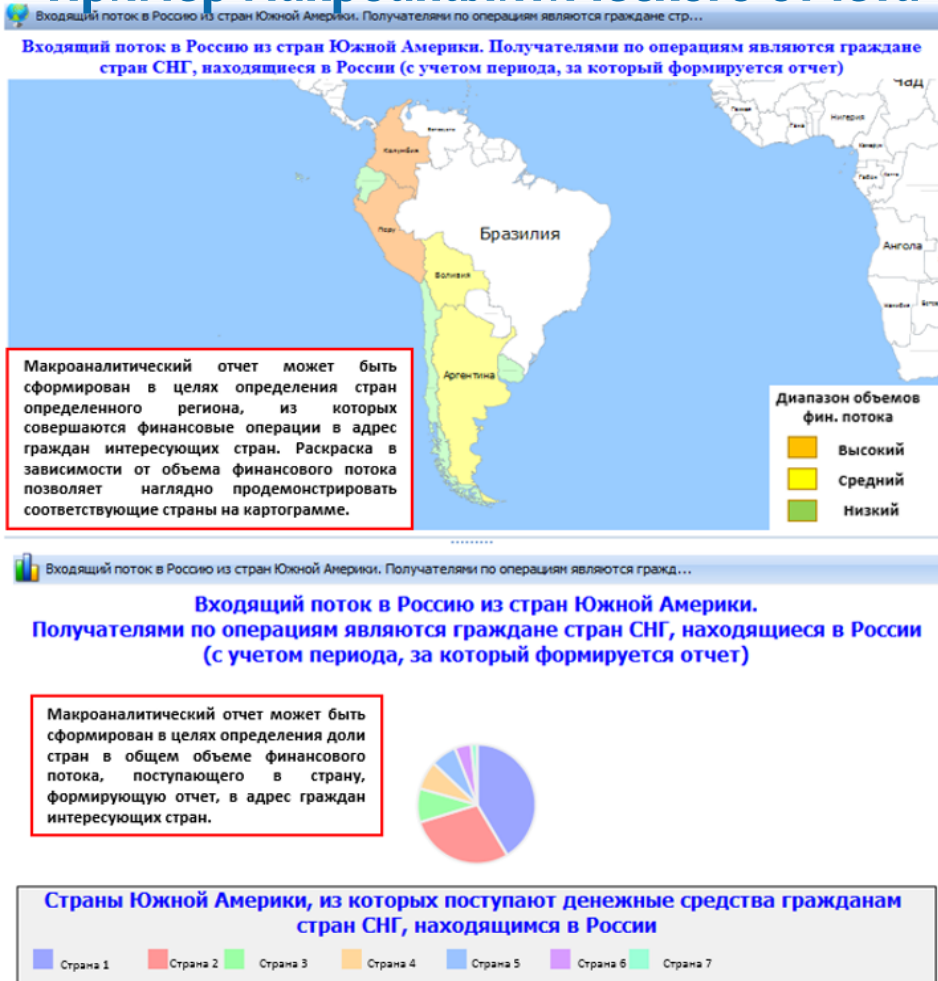
- Прозрачный блокчейн



- Система «Графус»

Национальный центр оценки рисков ОД/ФТ

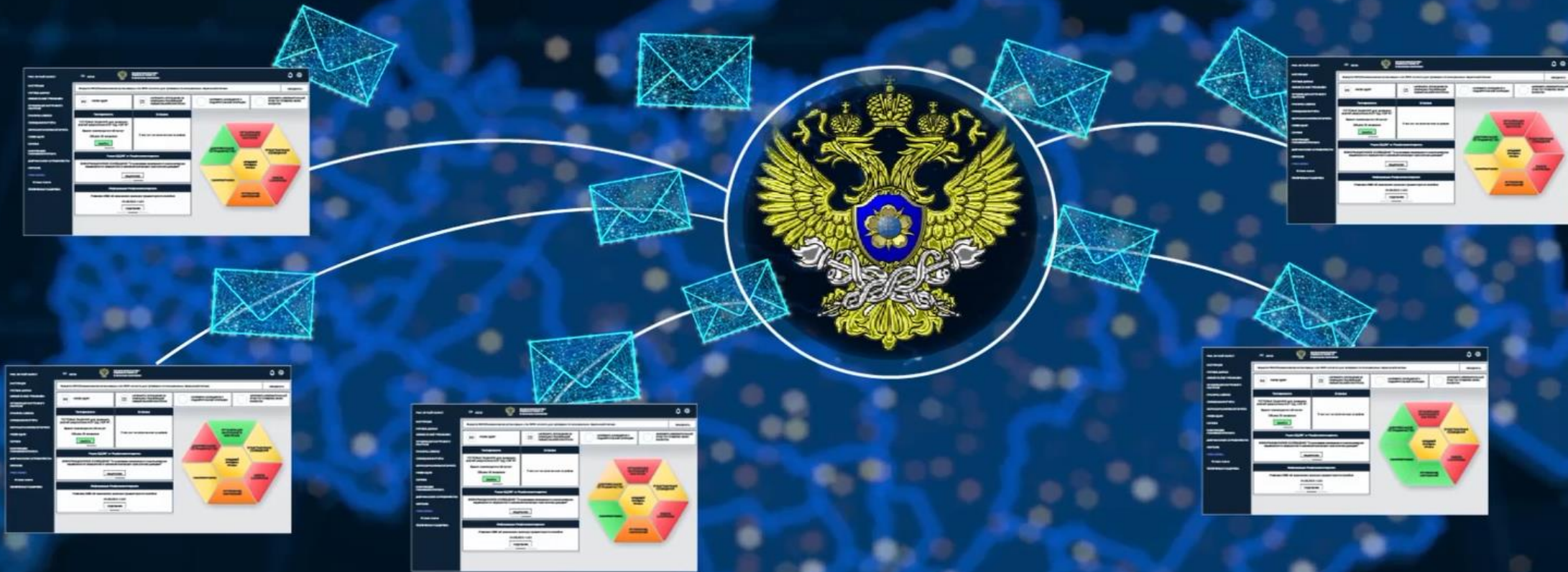
Пример макроаналитического отчета



Возможности НЦОР

- Проведение многофакторного стратегического анализа данных
- Выявление тенденций и аномалий
- Основания проведения финансовых расследований

Личный кабинет организации



Личный кабинет организации



Личный кабинет организации



РИСКИ ОД/ФТ



АКТУАЛЬНЫЕ ТИПОЛОГИИ

РОСФИНИММОНИТОРИНГ
Федеральная служба
по финансовому мониторингу

Введите ИНН/наименование организации или ФИО клиента для проверки по санкционным перечням/спискам ПРОВЕРИТЬ

РИСКИ ОД/ФТ	НАПРАВИТЬ СООБЩЕНИЕ ОБ ОПЕРАЦИИ, ПОДЛЕЖАЩЕЙ ОБЯЗАТЕЛЬНОМУ КОНТРОЛЮ	НАПРАВИТЬ СООБЩЕНИЕ О ПОДОЗРИТЕЛЬНОЙ ОПЕРАЦИИ	НАПРАВИТЬ ЕЖЕКВАРТАЛЬНЫЙ ОТЧЕТ ПО ПРОВЕРКЕ СВОИХ КЛИЕНТОВ
-------------	--	---	---

Тестирование	Штрафы
ТЕСТОВЫЕ ЗАДАНИЯ для проверки знаний результатов НОР ОД, НОР ФТ Время прохождения: 60 минут Объем: 18 вопросов ПРОЙТИ	У вас нет не оплаченных штрафов

Риски ОД/ФТ от Росфинмониторинга

ИНФОРМАЦИОННОЕ СООБЩЕНИЕ "О признаках возможного использования недвижимого имущества в схемах легализации преступных доходов"
ПОДРОБНЕЕ

Информация Росфинмониторинга

Решение МВК об изменении размера гуманитарного пособия
04.08.2020 15:23
ПОДРОБНЕЕ



ИНДИКАТОРАХ ПОДОЗРИТЕЛЬНЫХ ОПЕРАЦИЙ



- ОЦЕНКА ЗАКОНОПОСЛУШНОСТИ
- РЕЕСТР ПОДНАДЗОРНЫХ СУБЪЕКТОВ
- РЕЕСТР СУБЪЕКТОВ, ПРОШЕДШИХ ОБУЧЕНИЕ В МУМЦФМ
- РЕЕСТР СУБЪЕКТОВ НАПРАВИВШИХ СООБЩЕНИЯ С НАРУШЕНИЕМ СРОКА ОБУЧЕНИЕ

СВЕДЕНИЯ О ТИПОЛОГИЯХ И РИСКАХ

ПРЕДСТАВИТЬ ИНФОРМАЦИЮ В РОСФИНАММОНИТОРИНГ

ИНФОРМАЦИОННЫЕ ПИСЬМА (СООБЩЕНИЯ) РОСФИНАММОНИТОРИНГА

ЗАПРОСЫ/ОТВЕТЫ

ПЕРЕЧНИ И ИНФОРМАЦИЯ ДЛЯ ПРИМЕНЕНИЯ ЗАГРАДИТЕЛЬНЫХ МЕР

ЗАКОНОДАТЕЛЬСТВО В СФЕРЕ ПОД/ФТ

- 140, Организация, оказывающая посреднические услуги при осуществлении сделок купли-продажи недвижимого имущества
- 160, Оператор по приему платежей
- 170, Коммерческая организация, заключающая договоры финансирования под уступку денежного требования в качестве финансового агента
- 999, Иная
- 998, Вид деятельности не определен
- 141, Индивидуальный предприниматель, оказывающий посреднические услуги при осуществлении сделок купли-продажи недвижимого имущества



РЕЕСТР ОРГАНИЗАЦИЙ

РИСКИ ПОД/ФТ



ИНФОРМАЦИЯ РОСФИНАММОНИТОРИНГА

ОБЯЗАТЕЛЬНЫЕ ТРЕБОВАНИЯ

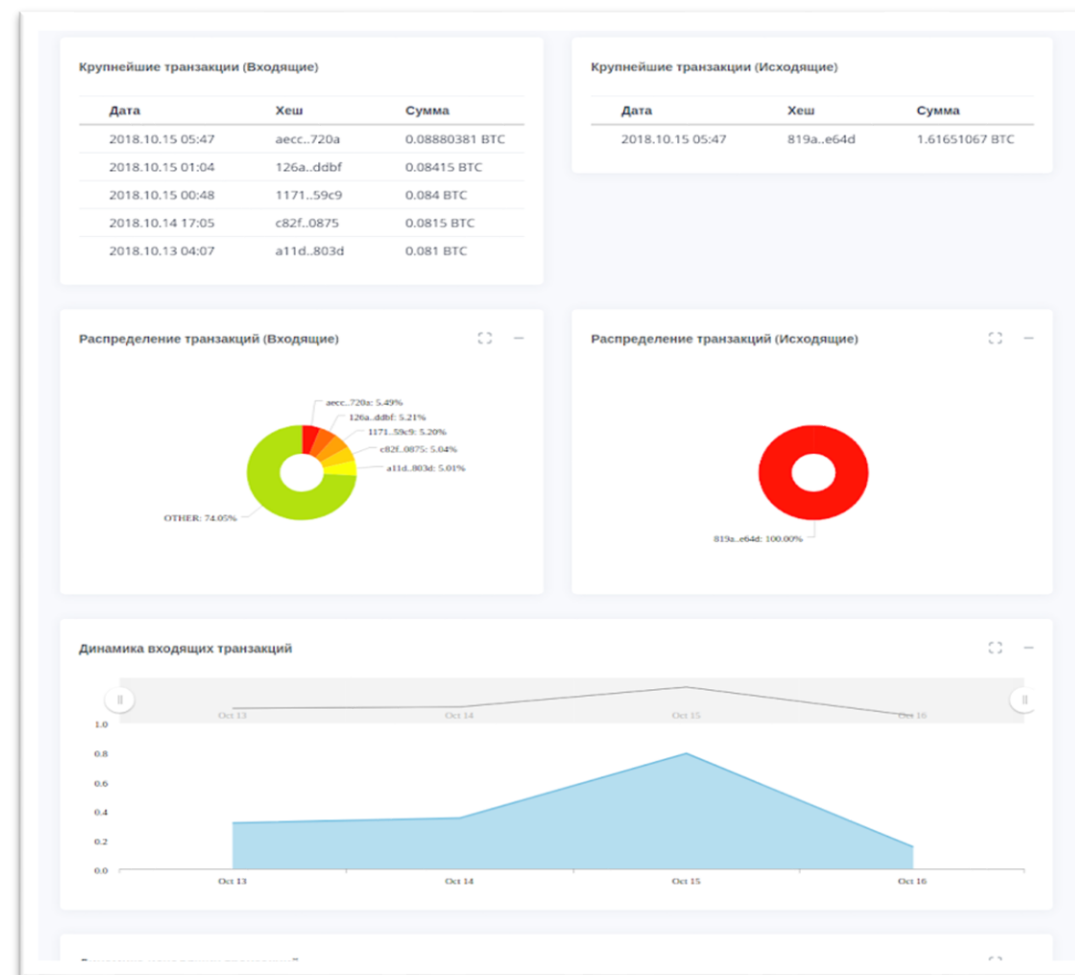
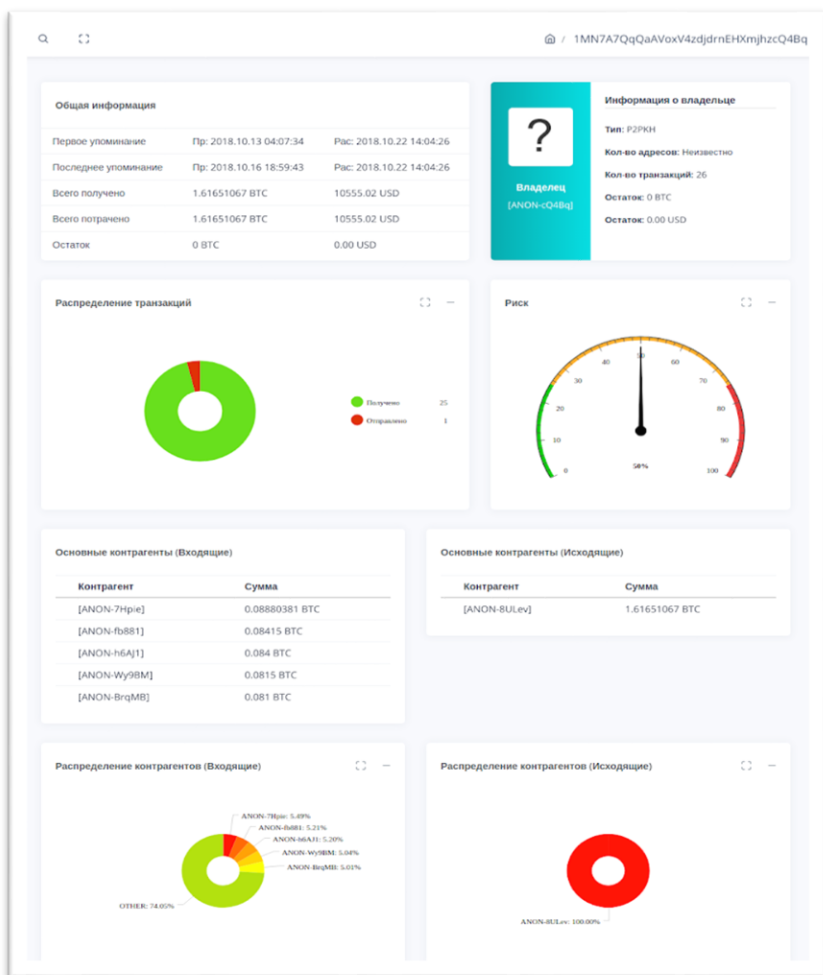


ПЕРЕЧНИ

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

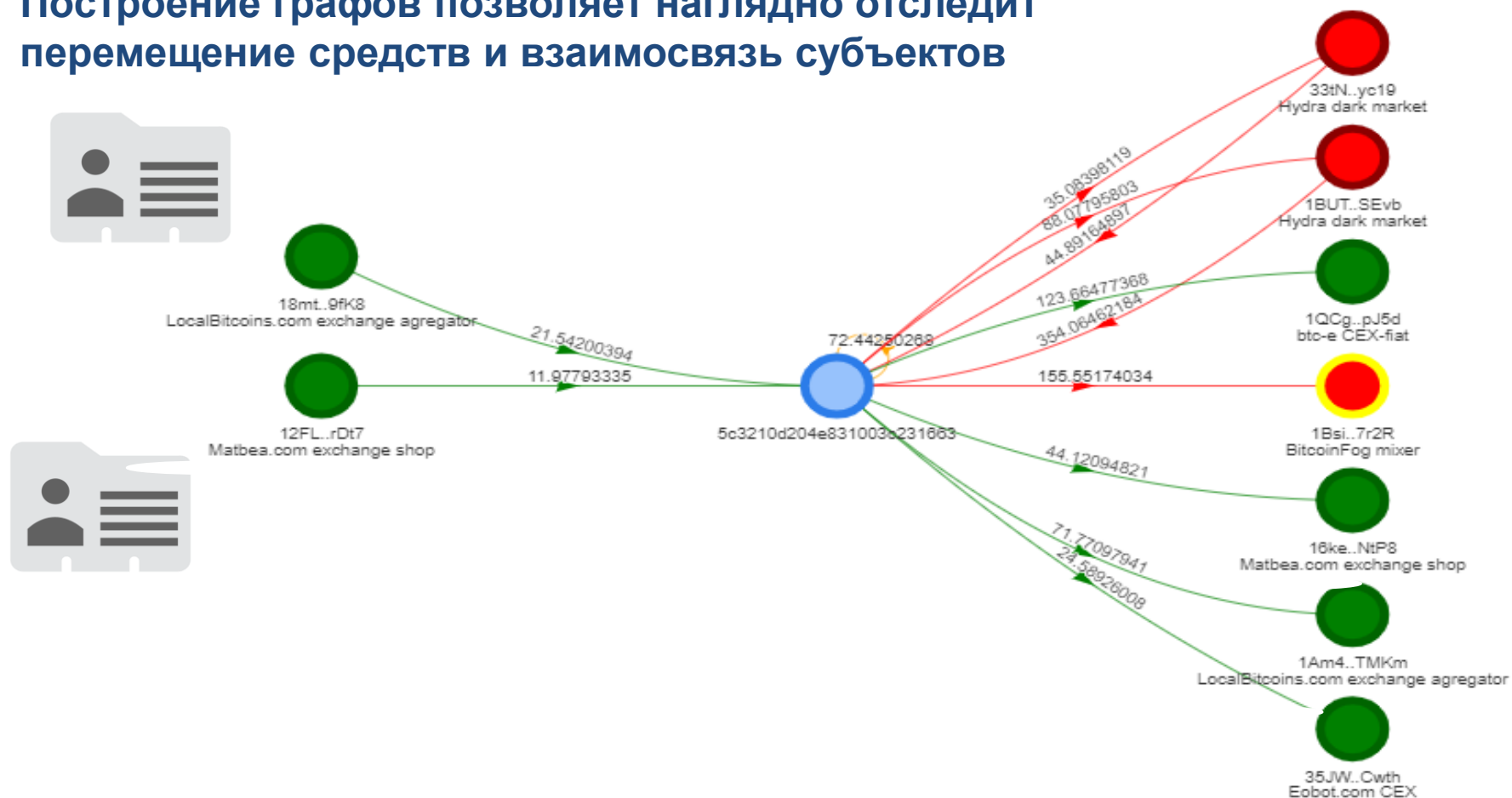


Интерфейс системы «Прозрачный блокчейн»



Пример расследования

Построение графов позволяет наглядно отследит перемещение средств и взаимосвязь субъектов



«Графус» - Система для дистанционного обучения проведению финансовых расследований в сфере ПОД/ФТ

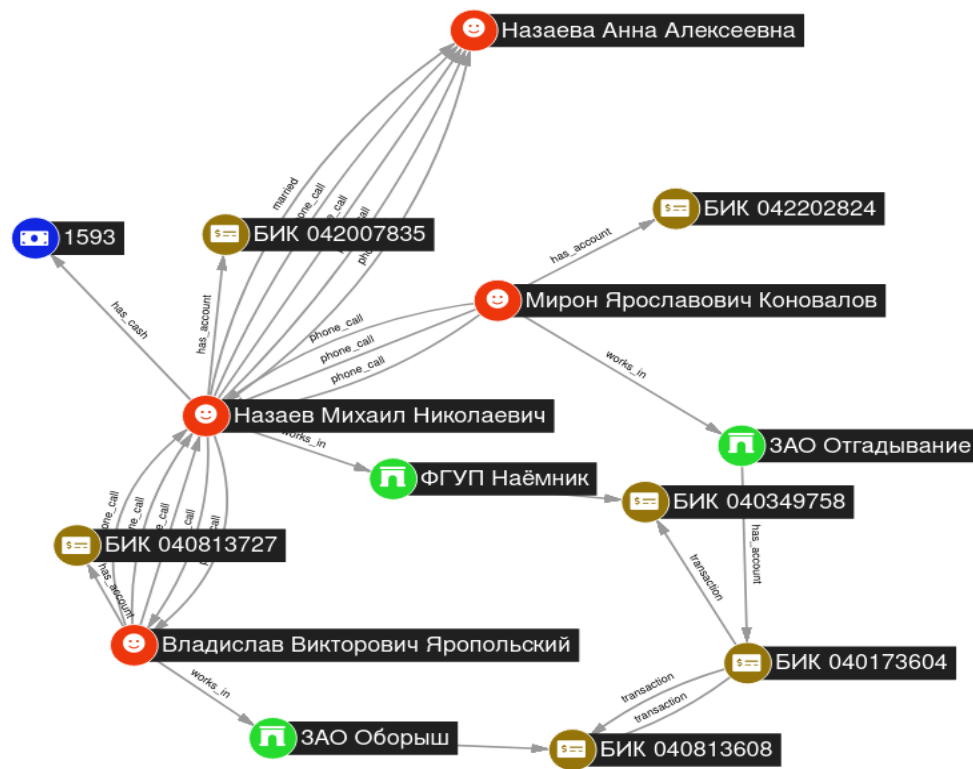


Транзакции сговорщиков и лн

Подграфы Граф

Organization (3) account (6) person (4) cash (1)
has_account (6) works_in (3) transaction (3) has_cash (1) phone_call (12) married (1)

Force Сброс Показать все надписи



МЕЖДУНАРОДНАЯ ОЛИМПИАДА ПО ФИНАНСОВОЙ БЕЗОПАСНОСТИ



повышение общей информационной, финансовой и правовой грамотности молодежи, выявление талантливых школьников и студентов в области финансовой безопасности



создание условий для индивидуальной образовательной траектории, содействие профессиональной ориентации школьников и студентов



стимулирование учебно-познавательной и научно-исследовательской деятельности школьников и студентов, развитие научных знаний в области финансовой безопасности

МАРШРУТ ОЛИМПИАДЫ

Всероссийский урок по финансовой безопасности

I этап Олимпиады (отборочный)

II этап Олимпиады (финальный)

I этап Олимпиады

**проводится на площадках вузов – участников
Международного сетевого института в сфере ПОД/ФТ**

**участники – обучающиеся 8-10 классов и студенты
вузов**

срок проведения – с 17 по 21 мая 2021 года

победители получают право участия во II этапе

Олимпиады

II этап Олимпиады

**проводится на федеральной территории
«Сириус» (г. Сочи, Россия)**

**срок проведения – с 3 по 9 октября 2021
года**

Благодарю за внимание!

Использование Regtech-платформ для многоуровневой оценке рисков ОД/ФТ



Методология национальной оценки рисков



«...частный сектор может оказаться **наилучшим источником информации** по многим вопросам. Участниками из числа представителей частного сектора, способными оказать **существенное содействие** в процессе проведения оценки рисков ОД/ФТ на национальном уровне, могут быть самые разные учреждения, организации и субъекты...».

Анкетирование с использованием возможностей Личного кабинета



Вопросы, предполагающий выбор одного из предложенных ответов

Каковы масштабы деятельности Вашей организации?

Каковы, по Вашему мнению, перспективы посреднической деятельности на рынке недвижимости в среднесрочной перспективе?

Как Вы считаете, будет ли преступник использовать услуги риелтора для того чтобы приобрести / продать объекты недвижимого имущества?

Анкетирование с использованием возможностей Личного кабинета



Вопросы, предполагающий выбор одного из предложенных ответов

Каков порядок Ваших действий, если наблюдается нестандартное поведение клиента, которое можно связать с высокими рисками соответствующей сделки?

Что препятствует Вам более активно информировать Росфинмониторинг о подозрительных операциях (сделках) своих клиентов?

Каков порядок Ваших действий, если наблюдаются попытки клиента скрыть личность истинного участника сделки (собственника), лица, реально руководящего проведением сделки, не являющегося официальной стороной сделки (или представителем одной из сторон сделки)?

Анкетирование с использованием возможностей Личного кабинета



Вопросы, предполагающие ранжирование ответов по степени значимости по 5-балльной шкале

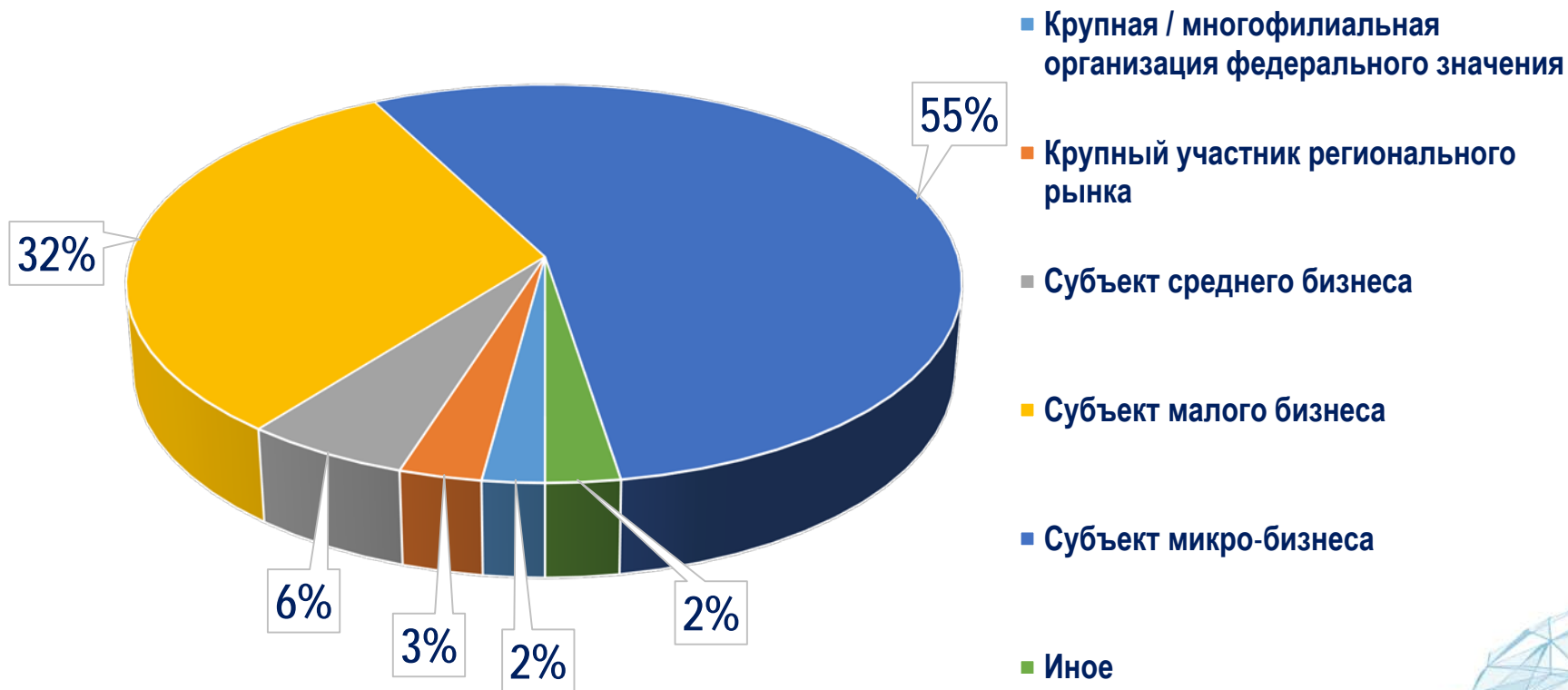
В связи с чем, по Вашему мнению, сделки с недвижимым имуществом привлекательны для целей легализации преступных доходов?

	Укажите ранг:
Возможность расчетов наличными денежными средствами	
Дороговизна и одновременно высокая ликвидность	
Возможность получения текущего дохода (например, от сдачи в аренду)	
Возможности манипулирования ценой объекта	
Возможность регистрации объекта недвижимого имущества на подставное лицо	

Анкетирование риелторов с использованием Личного кабинета на сайте Росфинмониторинга



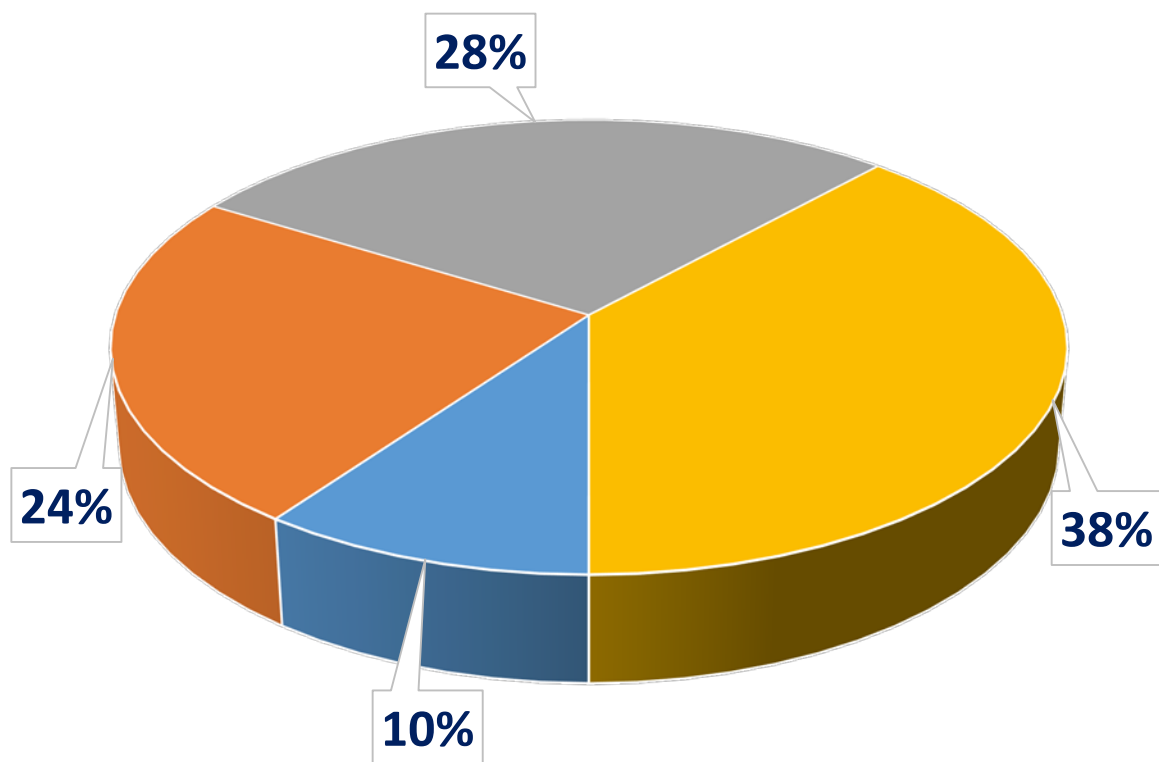
В опросе приняло участие порядка 1 тыс. респондентов



Ответы на вопросы анкеты для риелторов



Как Вы оцениваете тенденции в секторе посредников на рынке недвижимого имущества в связи с пандемией:

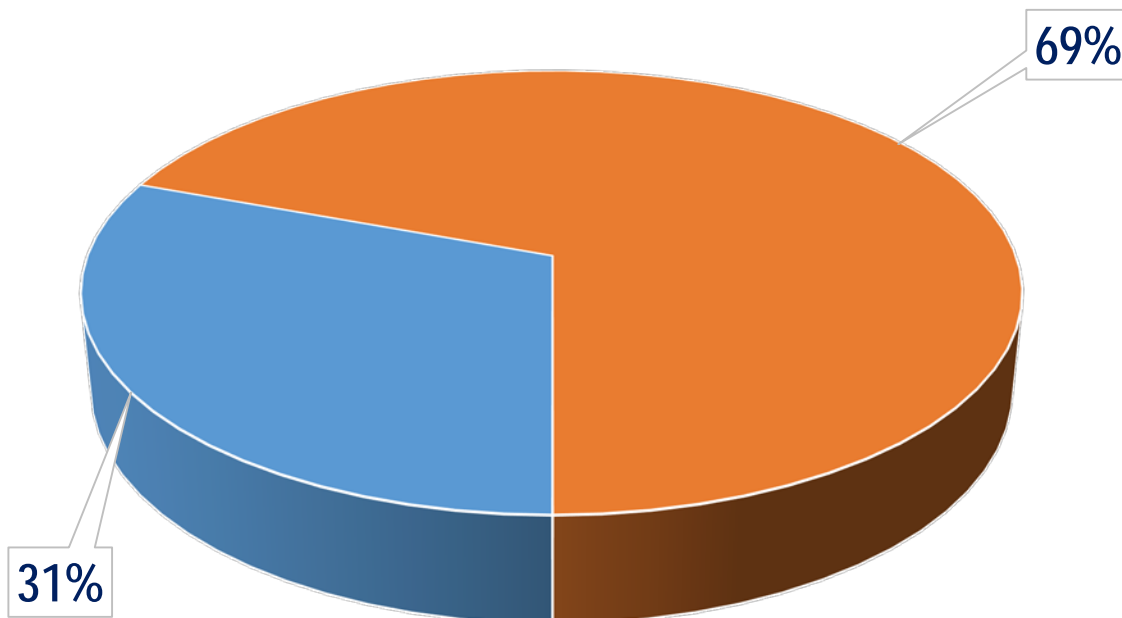


- Наблюдается существенный рост спроса на посреднические услуги на рынке недвижимого имущества
- Наблюдается незначительный рост спроса на посреднические услуги на рынке недвижимого имущества
- Спрос на услуги сохраняется на докризисном уровне
- Наблюдается сокращение спроса на посреднические услуги на рынке недвижимого имущества

Ответы на вопросы анкеты для риелторов



Каковы, по Вашему мнению, перспективы посреднической деятельности на рынке недвижимости в среднесрочной перспективе?

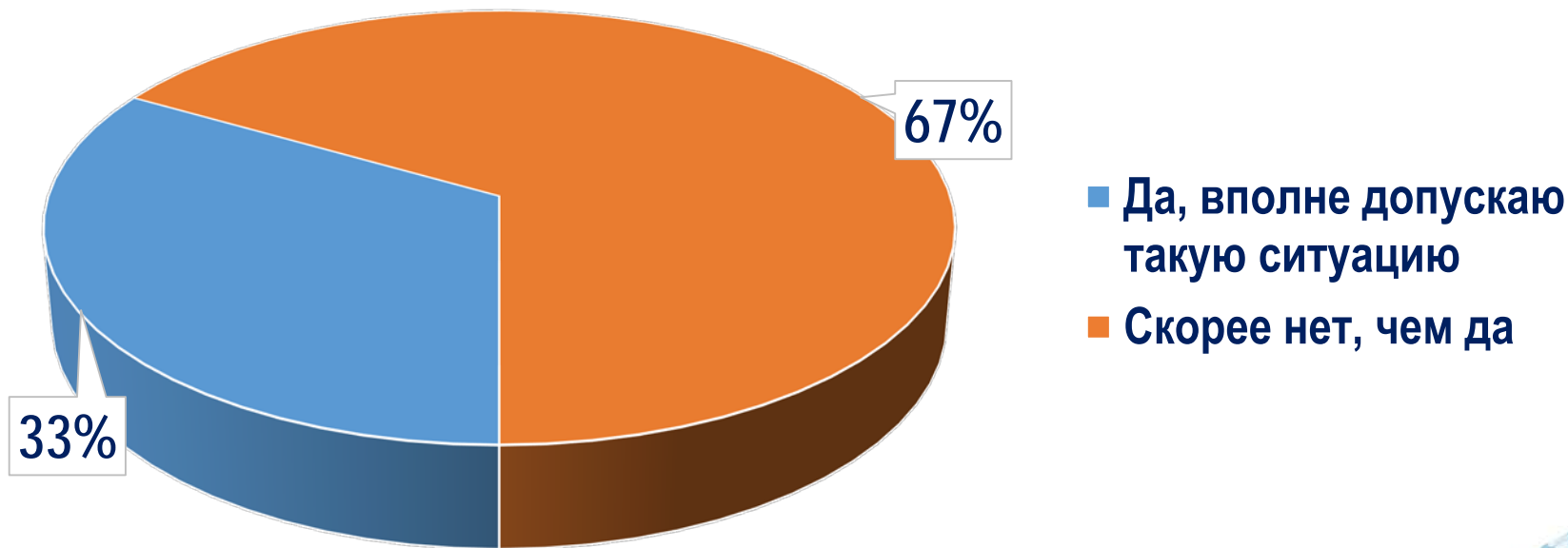


- Традиционные услуги риелтора будут постепенно замещаться онлайн сервисами (маркетплейсами), в том числе организованными банками, предоставляющими ипотечные продукты
- Услуги риелтора останутся востребованными

Ответы на вопросы анкеты для риелторов



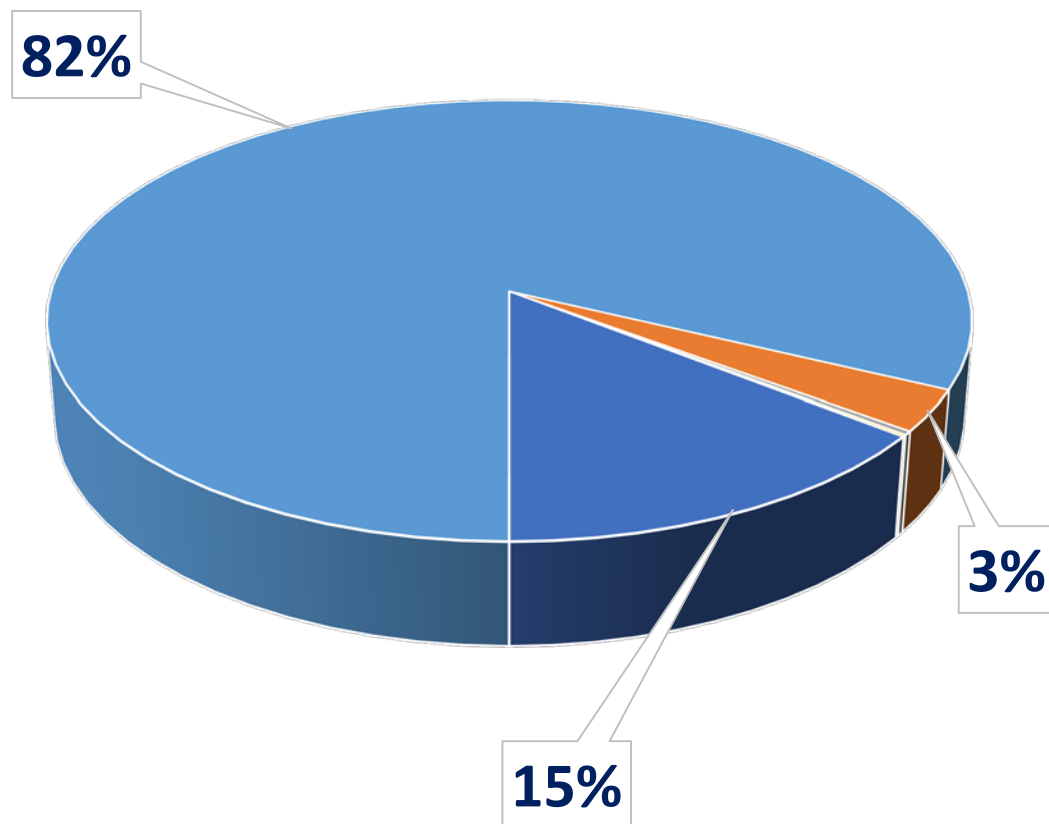
Как Вы считаете, будет ли преступник использовать услуги риелтора для того чтобы приобрести / продать объекты недвижимого имущества?



Ответы на вопросы анкеты для риелторов



Каков порядок Ваших действий, если наблюдаются попытки клиента скрыть личность истинного участника сделки (собственника), лица, реально руководящего проведением сделки, не являющегося официальной стороной сделки

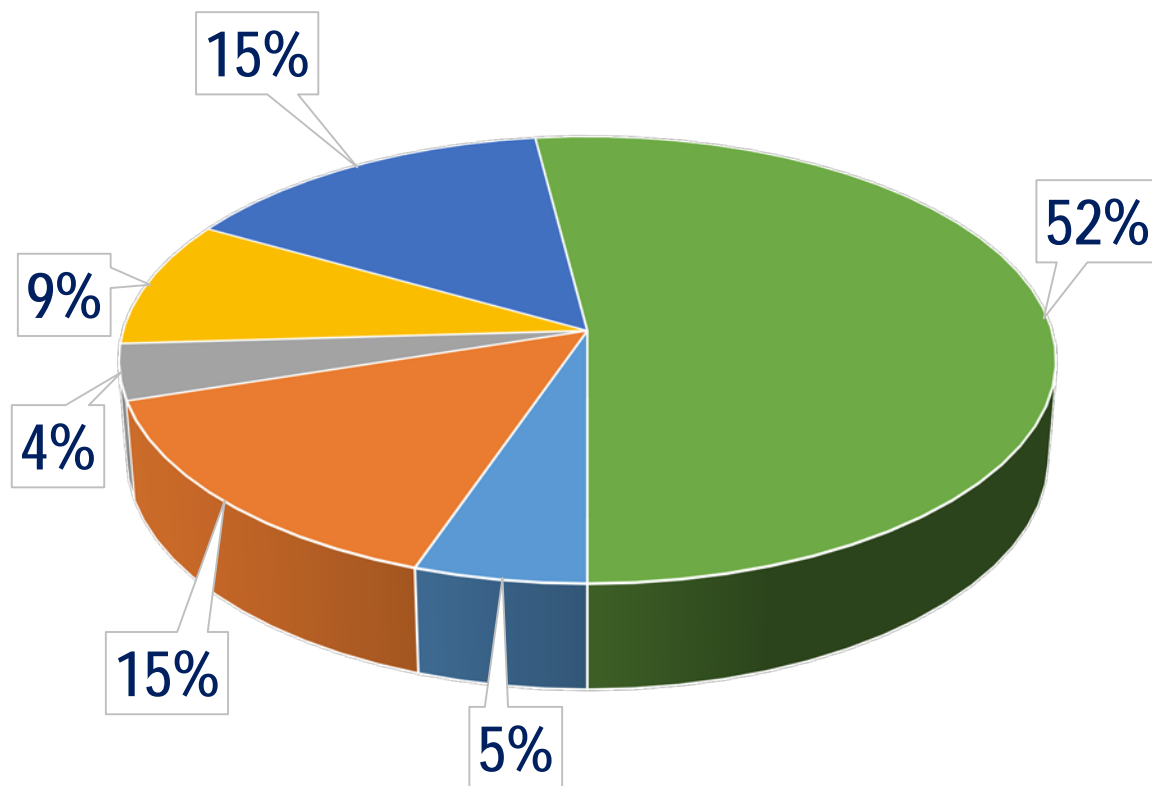


- Такого рода ситуации возникают, и они служат основанием для запроса дополнительных документов по сделке и направления СПО
- Такого рода ситуации возникают, но они не служат основанием для присвоения клиенту высокого уровня риска
- Как правило, не обращаем внимание на поведение клиента при его обслуживании
- Не принимаем никаких мер, поскольку запрос дополнительной информации может привести к потере клиента
- Иное (таких ситуаций не возникало)

Ответы на вопросы анкеты для риелторов



Что препятствует риелтору активно информировать о подозрительных операциях своих клиентов

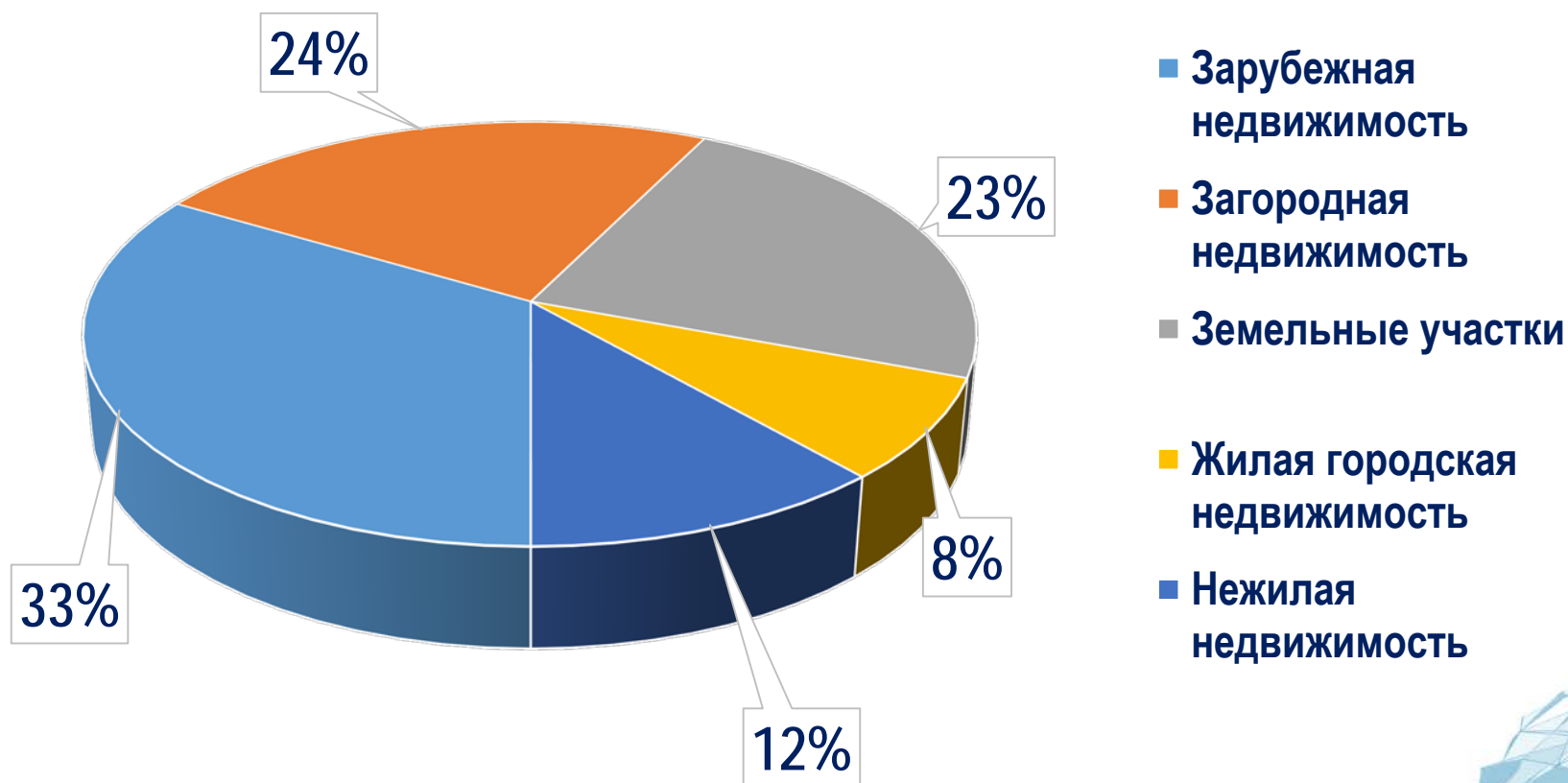


- Направление такого рода сведений может негативно сказаться на бизнесе
- Недостаточно методик и рекомендаций по выявлению подозрительных сделок и операций
- Отсутствие необходимых знаний и навыков по формированию и отправке сведений
- Недостаточно информации для формирования и отправки сведений
- Сложность оформления и отправки электронного сообщения
- Серьезные препятствия отсутствуют

Ответы на вопросы анкеты для риелторов



Какие объекты недвижимого имущества, по Вашему мнению, являются наиболее привлекательными для инвестирования преступных доходов



Использование результатов анкетирования



- Проведение секторальной и национальной оценки рисков ОД/ФТ;
- Ориентирование риелторов на риски и уязвимости (обратная связь);
- Разработка плана мероприятий по снижению рисков в секторе;
- Подготовка учебных материалов для ВУЗов Международного сетевого института в сфере ПОД/ФТ

Благодарю за внимание !



О ситуации в государствах ЕАГ в области ПОД/ФТ в связи с COVID-19 и мерах по минимизации рисков ОД/ФТ

Евразийская группа по противодействию
легализации преступных доходов и финансированию
терроризма (ЕАГ)

Общая ситуация в регионе, вызванная пандемией

Неравномерное воздействие пандемии на государства региона ЕАГ

Отсутствие единой политики

Страны с различными режимами ограничений и без них

Введенные ограничения:

- Трансграничные перемещения / массовые скопления людей
- Предпринимательская деятельность
- Предоставление части финансовых услуг

Динамика предикатных преступлений

Положительные тенденции

- Снижение общественно опасных деяний и преступлений против собственности

Негативные тенденции

- Рост фактов мошенничества, в том числе с использованием высоких технологий и в инвестиционной сфере
- Киберпреступления (фишинг, взлом, программы вымогатели)
- Продажа/предоставление нелегальных медицинских товаров и услуг
- Сговор и манипуляция ценами на медицинские товары и услуги
- Коррупционные преступления
- Преступления в сфере государственных закупок

Динамика предикатных преступлений

Мошенничество

- Продажа СИЗ/ лекарств
- Возврат средств за билеты
- Анализы, медосмотр, тесты на COVID-19
- Продажа уникальных товаров
- Инвестиционное мошенничество /финансовые пирамиды /фирмы однодневки
- Возврат (возмещение) налогов
- Получение пособий / льгот / выплат
- Пропуска для передвижения в условиях ограничений
- Перевод средств на лечение
- Имитация рассылок от имени Всемирной организации здравоохранения / имитация рассылок от благотворительных организаций, благотворительных кампаний Всемирного банка или МВФ

Новые уязвимости из-за COVID-19

рост зависимости клиента от операций, осуществляемых по онлайн-каналам

выделение правительствами средств на поддержку/кредитование на основании ошибочных/ложных целей

периодического ухудшения профиля клиентов в связи с ограничением физического присутствия

увеличение объема операций с наличными денежными средствами

ограничения по проведению проверок ПОД/ФТ

ухудшение экономической ситуации в стране

Принимаемые ответные меры в регионе EAG

в области нормативно-правового регулирования

в деятельности подразделений финансовой разведки

в правоохранительной деятельности

в деятельности надзорных органов

в деятельности финансовых учреждений

Ответные меры в области нормативно-правового регулирования

Формирование нормативно-правовой базы для дистанционного получения государственных услуг

Формирование нормативно-правовой базы для дистанционного обслуживания в финансовых учреждениях

Расширение требований базовых законов о ПОД/ФТ

Информирование подотчетных субъектов

Ответные меры в деятельности подразделений финансовой разведки

информирование со стороны ПФР представителей частного сектора об угрозе COVID, соответствующих рисках и типологиях

мониторинг открытых источников на предмет выявления схем мошенничества, связанных с COVID-19

дополнительный мониторинг медицинской сферы

дополнительный анализ СПО с характерными признаками

Ответные меры в правоохранительной деятельности

информирование о соответствующих рисках и схемах мошенничества

работа со СМИ

выстраивание системы дистанционного обращения граждан

проводится постоянный мониторинг расходования бюджетных средств, выделяемых на предотвращение последствий распространения COVID-19

проводится постоянный мониторинг государственных контрактов, связанных с коронавирусом

Ответные меры в деятельности надзорных органов

изменения формата проведения проверок и формата взаимодействия с частным сектором

оперативное доведение информации о типологиях и рисках, связанных с эпидемической ситуацией, признаках (индикаторах) подозрительных операций

введение отдельного индикатора СПО, связанного с коронавирусом

меры по стимулированию онлайн платежей

ослабление нормативных требований

Спасибо за внимание

UKNF

URZĄD
KOMISJI
NADZORU
FINANSOWEGO

POLISH FINANCIAL SUPERVISION AUTHORITY

Павел Палушиньский

Отдел комплаенс

29.04.2021

**Надзорные инициативы,
предпринятые Управлением
финансового надзора
Польши для снижения риска
отмывания денег и
финансирования терроризма
в Польше во время
пандемии COVID-19**

Управление финансового надзора Польши

Управление финансового надзора Польши (UKNF) было создано в сентябре 2006 года.

Миссия UKNF — обеспечение стабильности и безопасного развития финансового рынка.

UKNF — независимый орган, задачами которого являются ограничение чрезмерного риска, связанного с деятельностью поднадзорных учреждений (не только рисков, связанных с отмыванием денег и финансированием терроризма — ОД/ФТ), и повышение прозрачности финансового рынка.

UKNF осуществляет надзор за:

- банковским сектором;
- рынком капитала;
- страховым рынком;
- платежными учреждениями и офисами операторов платежных систем;
- операторами электронных денег;
- сектором кооперативных кредитных союзов.

Новые риски, связанные с пандемией COVID-19

Пандемия коронавируса (COVID-19) создала новые проблемы как для финансовых учреждений, так и для органов власти, ответственных за борьбу с отмыванием денег и финансированием терроризма.

Среди выявленных новых рисков и тенденций наиболее значимыми являются:

- установление деловых отношений без физического присутствия клиента — «удаленная» идентификация и проверка клиента, обычно через Интернет;
- новые схемы мошенничества, такие как:
 - мошенничество с использованием медикаментов или средств индивидуальной защиты;
 - мошенничество в социальных сетях и телефонные звонки с целью мошеннических попыток получить пожертвования для незаконных благотворительных организаций;
 - телефонные звонки людей, выдающих себя за государственных служащих, с просьбой предоставить личную информацию или информацию о банковском счете;
 - фиктивные инвестиционные фирмы, обещающие высокую прибыль (в последнее время в Польше значительно увеличился объем мошенничества такого типа).

Инициативы, предпринятые Управлением финансового надзора Польши для снижения риска

UKNF предприняло меры для снижения новых видов рисков, а также для повышения безопасности финансового рынка Польши. Основные инициативы следующие:

- В 2019 году UKNF опубликовало официальное заявление о проверке личности клиентов средствами видеоверификации. В этом документе изложены передовые практики, связанные с проверкой личности клиентов, которые физически не присутствуют при идентификации.
- В 2020 году UKNF опубликовало анкету для банков о платежных учреждениях. Основная цель этой анкеты — обеспечение безопасности финансовых операций и надлежащего выполнения поднадзорными учреждениями требований Закона Польши о ПОД/ФТ.

Инициативы Управления финансового надзора Польши

- В 2020 году UKNF выпустило руководство для поднадзорных учреждений по самостоятельной оценке рисков отмывания денег и финансирования терроризма, проведение которой является одним из обязательств в соответствии с Законом Польши о ПОД/ФТ и Директивой (ЕС) 2015/849 Европейского парламента и Совета Европейского союза — так называемой 4-й Директивой о ПОД.
- UKNF обеспокоено новыми тенденциями, связанными с мошенничеством, в особенности, поддельными инвестиционными схемами, доля которых значительно увеличилась в Польше за последнее время.

Удаленная идентификация и проверка

Невозможность очной встречи с клиентом может повлиять на способность финансового учреждения надлежащим образом идентифицировать и проверять своих клиентов и, следовательно, проводить эффективную оценку рисков клиентов. Ключевые факторы риска, связанные с установлением деловых отношений «удаленно», заключаются в следующем.

- До пандемии в рамках процедуры «Знай своего клиента» (ЗСК) обычно требовалось, чтобы клиент подтвердил свою личность «физически» в филиале финансового учреждения. Новые обстоятельства вынудили финансовые учреждения быстро изменить свой подход и ввести новые каналы распространения (Интернет) без проведения надлежащей оценки рисков и без применения соответствующих инструментов или процедур.
- Затраты на специализированные инструменты, которые можно использовать для установления деловых отношений удаленно, чрезмерны для небольших учреждений (например, для офисов операторов платежных систем).
- В процессе проверки личности часто используются ксерокопии удостоверений личности, которые предоставляют потенциальные клиенты, что значительно затрудняет проверку подлинности документов.

Указанные выше факторы часто приводят к чрезмерному упрощению процессов ЗСК и, как следствие, к применению неадекватных мер надлежащей проверки в отношении «удаленных» клиентов.

Платежные учреждения

Платежные счета, предлагаемые платежными учреждениями, часто используются преступниками для совершения мошеннических действий или деятельности по отмыванию денег. Основные причины этого следующие:

- недостаточная осведомленность о потенциальных рисках ОД/ФТ;
- отсутствие специализированных инструментов, поддерживающих процессы ПОД/ФТ;
- относительно высокий уровень рисков ОД/ФТ, которые готовы взять на себя платежные учреждения;
- чрезмерно упрощенные процессы и процедуры ЗСК;
- тесные связи с биржами криптовалют.

Для обеспечения безопасности финансовых операций UKNF предприняло меры, направленные на укрепление сотрудничества между банками и сектором платежных услуг. На основе опросов и опыта, полученного в ходе проверок, была подготовлена анкета на базе исследования, проведенного Вольфсбергской группой.

- Предполагается, что эта анкета позволит банкам получить информацию о клиенте из сектора платежных услуг.
- На основе информации, предоставленной платежными учреждениями в анкете, банки смогут быстрее определить риск ОД/ФТ, возникающий в результате конкретных деловых отношений, и применить соответствующие меры надлежащей проверки клиентов для снижения этого риска.

Самостоятельная оценка риска ОД/ФТ подотчетными учреждениями (1)

Требование о проведении оценки рисков организации изложено в Законе Польши о ПОД/ФТ и вытекает из положений 4-й Директивы о ПОД.

Самостоятельная оценка рисков представляет собой основной документ, который определяет меры, принимаемые финансовыми учреждениями в целях противодействия отмыванию денег и финансированию терроризма, и служит отправной точкой для разработки внутренних процессов ПОД/ФТ.

Кроме того, самостоятельная оценка рисков существенно влияет на:

- осведомленность подотчетного учреждения о своей подверженности риску и, следовательно, о своей готовности к принятию риска;
- форму внутренних документов, регулирующих сферу ПОД/ФТ в подотчетном учреждении;
- объем и метод применения мер финансовой безопасности к клиентам подотчетного учреждения;
- практический подход к выполнению подотчетным учреждением требований в сфере ПОД/ФТ;
- меры, принимаемые подотчетным учреждением для снижения рисков в различных сферах своей деятельности, которые особенно подвержены рискам отмывания денег и финансирования терроризма.

Самостоятельная оценка риска ОД/ФТ подотчетными учреждениями (2)

Финансовые учреждения должны обновлять свою самостоятельную оценку рисков в случае изменений факторов риска, связанных с клиентами, странами или географическими регионами, продуктами, услугами, операциями или каналами сбыта. UKNF ожидает, что подотчетные учреждения также рассмотрят возможность обновления оценки рисков в случае существенных долгосрочных изменений в деловой среде, способных оказать существенное влияние на текущую деятельность учреждения, а также на способы использования его продуктов и услуг.

Важным примером вышеупомянутого обстоятельства является эпидемия, которая оказывает долгосрочное влияние на:

- подверженность финансовых учреждений рискам ОД/ФТ;
- подверженность рискам ОД/ФТ всего финансового сектора как в Польше, так и во всем мире.

Самостоятельная оценка рисков ОД/ФТ должна служить отправной точкой при принятии стратегических бизнес-решений в области ПОД/ФТ и при определении готовности к риску ОД/ФТ.

Таким образом, для правильного понимания и снижения рисков ОД/ФТ финансовым учреждениям жизненно важно оценивать новые факторы, такие как эпидемия или появление новых каналов распределения, и соответствующим образом обновлять самостоятельные оценки рисков.

Новые мошеннические схемы

В последнее время мошенническая активность в Польше значительно усилилась. Основные причины следующие:

- Пандемия вынуждала людей выполнять операции удаленно (например, через Интернет), что ограничивало возможность взаимодействия с клиентом и информирования его/ее о потенциальных рисках, связанных с его/ее операциями.
- Экономическая среда (относительно высокий уровень инфляции, низкие процентные ставки) может склонять инвесторов к более высокому риску при поисках новых типов инвестиций и возможностей.
- В настоящее время наиболее популярными схемами мошенничества в Польше являются инвестиционные виды мошенничества. Агенты фиктивных инвестиционных фирм напрямую связываются со своими жертвами и предлагают чрезвычайно выгодные инвестиции, которые можно осуществить только через их компании. Они часто пытаются убедить своих «клиентов» раскрыть информацию о банковских счетах или установить сторонние приложения, позволяющие им получать доступ к банковским счетам жертв. Инвестированные средства быстро перемещаются через несколько банковских или платежных счетов и в конечном итоге переводятся на анонимные криптовалютные кошельки и исчезают.

Повышение информированности о финансовом рынке

UKNF ежегодно проводит образовательные мероприятия в рамках цикла встреч с представителями финансового рынка Образовательного центра для участников рынка (CEDUR).

Тема предотвращения отмывания денег и финансирования терроризма является неизменным элементом учебных занятий, в ходе которых обсуждаются вопросы, связанные с риском ОД/ФТ, а также представляются результаты проверок и связанные с ними рыночные практики.

Семинары CEDUR — прекрасная возможность для обсуждения новых рисков и выявленных тенденций, а также для обмена опытом между финансовыми учреждениями и представителями UKNF.

Учебные мероприятия приносят непосредственные результаты: во время проверок подотчетных учреждений, которые участвовали в семинарах CEDUR, эти учреждения часто демонстрируют, что ими уже были предприняты меры с целью выполнения обязательств, связанных с ПОД/ФТ, в соответствии с полученной информацией на семинарах.

Спасибо!

Павел Палушиньский

Отдел комплаенс

pawel.paluszynski@knf.gov.pl

г. Варшава, улица Пиекна 20, 00-549

www.knf.gov.pl

Построение процедур «Знай своего клиента» в условиях пандемии и цифровой трансформации услуг

2021 год

halykbank.kz



facebook.com/halykbank



Дистанционное установление деловых отношений



В связи с пандемией, вызванной COVID-19, банки второго уровня (далее – БВУ) в 2020 году направили ресурсы на реализацию продуктов, позволяющих осуществлять установление деловых отношений и обслуживание клиентов в дистанционном формате.

Законодательная база РК с учетом изменений, внесенных в Закон РК О ПОД/ФТ* и в подзаконные НПА РК**, позволяет устанавливать деловые отношения в дистанционном формате.

С учетом государственных баз, доступ к которым был получен посредством Центра обмена идентификационными данными (ЦОИД), Государственной базы данных «Физические лица», сервиса Egov у БВУ появилась возможность осуществлять сверку идентификационных данных клиентов.

В рамках обстоятельств, связанных с пандемией, и открывшихся технических/законодательных возможностей, АО «Народный Банк Казахстан» (далее – Банк) в 2020 году реализовал проект по дистанционному открытию счетов индивидуальным предпринимателям.

Процедуры дистанционного установления отношений Банком были реализованы с учетом всех требований законодательства РК по ПОД/ФТ и полным исполнением процедур «Знай своего клиента».

* Закон Республики Казахстан «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

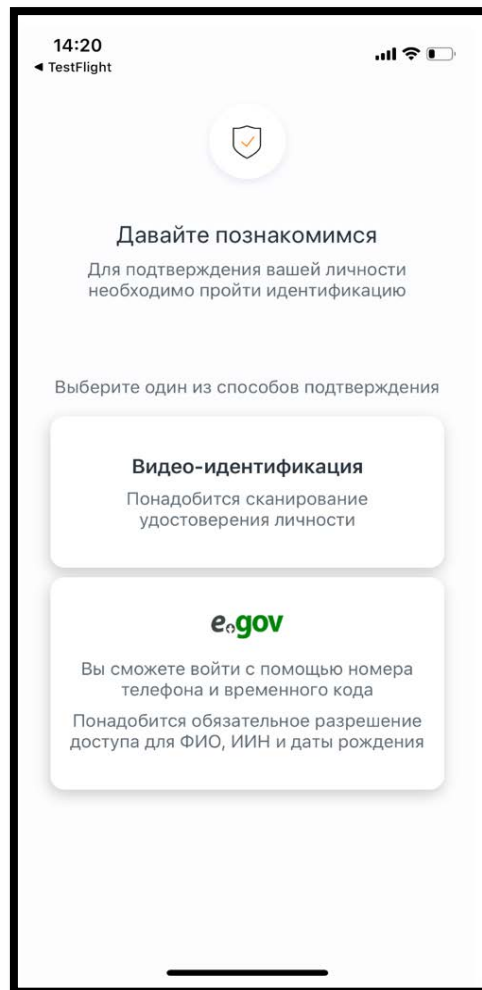
** Постановление Правления НБ РК от 29.06.2018 года №140 «Об утверждении Требований к надлежащей проверке клиентов в случае дистанционного установления деловых отношений субъектами финансового мониторинга».

Идентификация клиента и подтверждение личности клиента через биометрию

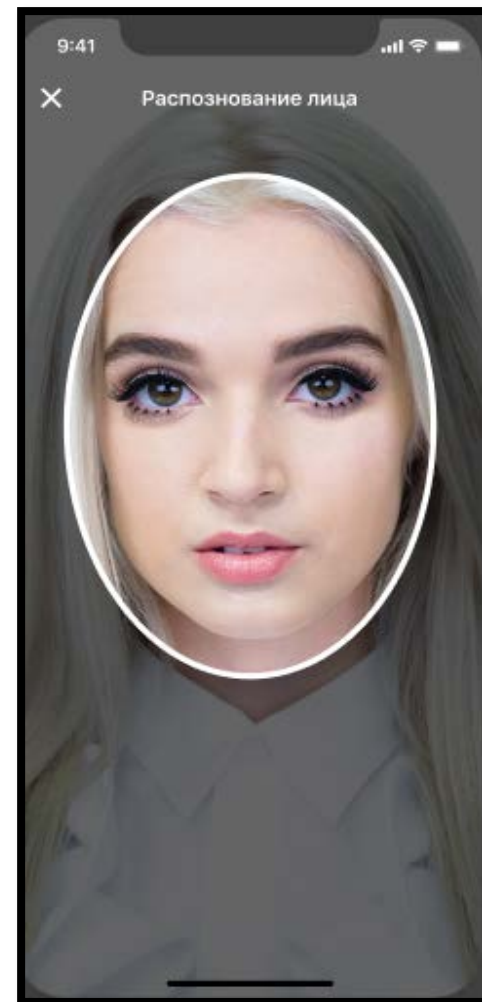
При идентификации и аутентификации клиентов в дистанционном канале «Onlinebank» используются средства биометрической идентификации

- ✓ В целях прохождения процедур КУС Клиенту необходимо подтвердить свою личность (пройти идентификацию)/
- ✓ На данном этапе клиент может выбрать идентификацию :
 - через портал государственных услуг EGOV
 - через видео-идентификацию (нужно подготовить удостоверение личности)

Таким образом, у клиентов имеется две возможности идентификации посредством государственного портала, либо путем непосредственной идентификации в системе Банка.



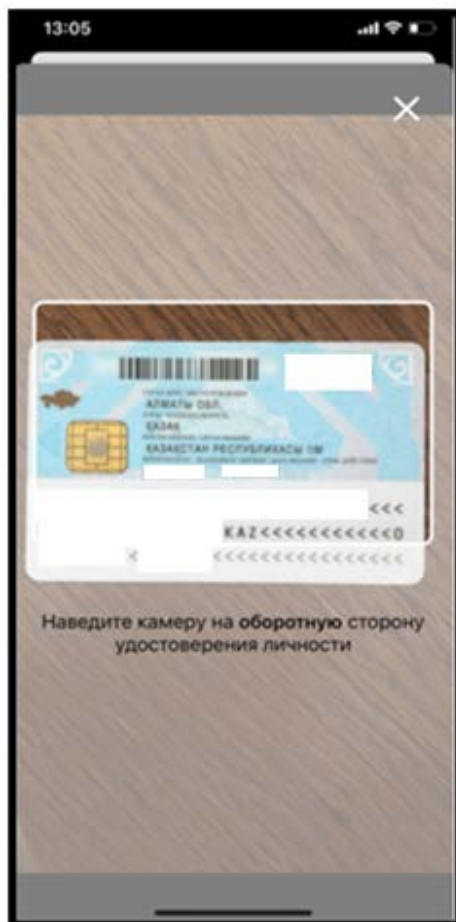
- ✓ В случае прохождения видеоидентификации в системах Банка осуществляется сверка биометрических данных клиента с данными, имеющимися в Банке и ЦОИД. С учетом установленных параметров осуществляется проверка личности клиента посредством государственной базы данных.
- ✓ Видеоидентификацию должен проходить именно тот человек на кого открывается счет.



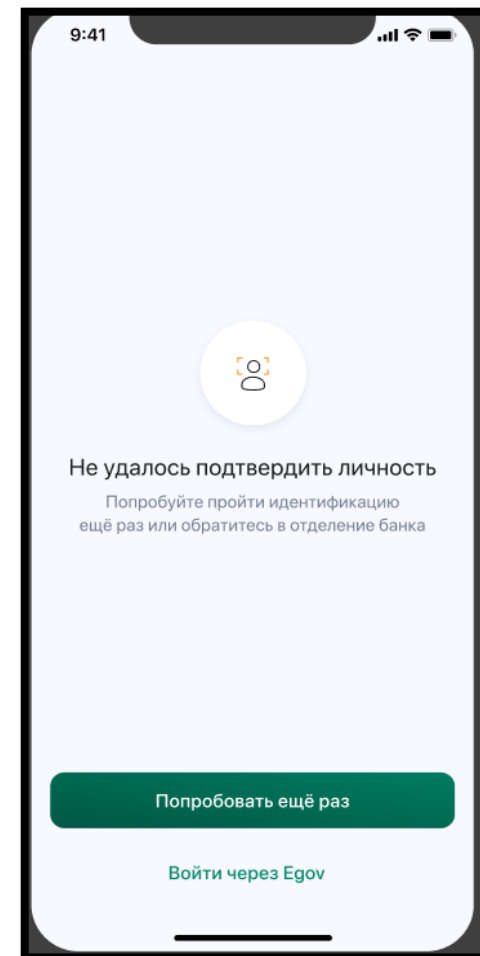
Идентификация клиента и подтверждение личности клиента через биометрию

При идентификации и аутентификации клиентов осуществляется подтверждение личности физического лица путем сверки с государственными базами данных

- ✓ Кроме того, с учетом видео-подтверждения личности клиента с помощью государственной базы данных (ГБДФЛ) осуществляется сверка идентификационных данных клиента, с учетом сканированного удостоверения личности.
- ✓ С учетом видеоидентификации и сверки параметров документа, удостоверяющего личность с данными государственных баз осуществляется подтверждение личности клиента.



- ✓ С учетом установленных проверок для подтверждения личности и прохождения идентификации должны сработать все необходимые контроли.
- ✓ При не прохождении по каким-либо причинам проверок и не подтверждения личности у клиентов имеется возможность повторить видео-подтверждение или попробовать пройти идентификацию через портал EGOV.



Дополнительно необходимо отметить, что помимо данных, удостоверяющих личность, Банком осуществляется также сверка сведений непосредственно ИП/КХ, в рамках которого происходит открытие счета и установление деловых отношений с клиентом. Регистрационные параметры ИП/КХ также проходят проверку.

Ограничения при дистанционном установлении деловых отношений

Банк устанавливает деловые отношения дистанционным способом исключительно с клиентами, соответствующими следующим требованиям:

- 1) физическое лицо, которому присвоен идентификационный номер;
- 2) клиент не является лицом, включенным в перечень организаций и лиц, связанных с финансированием терроризма и экстремизма;
- 3) клиент не является установленным лицом или организацией, в отношении которых применяются международные санкции (эмбарго) в соответствии с резолюциями Совета Безопасности Организации Объединенных Наций;
- 4) клиент не является лицом, которому присвоен уровень риска, требующий применения усиленных мер надлежащей проверки в соответствии с пунктом 7 статьи 5 Закона о ПОДФТ и правилами внутреннего контроля.

Банк принимает решение о дистанционном установлении деловых отношений с клиентами самостоятельно с учетом оценки степени риска ОД/ФТ по типу клиента, странового (географического) риска, риска услуги (продукта) и (или) способа ее (его) предоставления.

Банк отказывает в установлении деловых отношений дистанционным способом и (или) в проведении операции в случае:

- 1) несоответствия клиента вышеуказанным требованиям;
- 2) невыполнения условий, о наличии согласия клиента-физического лица на сбор, обработку, хранение и предоставление, в том числе при необходимости третьим лицам, его персональных данных, подтвержденного посредством идентификационного средства, при отсутствии исполнения условий: ввода клиентом в системе удаленного доступа своего индивидуального номера, идентификации и аутентификации клиента, и фиксации сведений по клиенту;
- 3) при наличии подозрений у Банка о совершении клиентом операции в целях ОД/ФТ;
- 4) по иным основаниям, предусмотренным Кодексом РК «О налогах и других обязательных платежах в бюджет» Законом о ПОДФТ, Законом РК «О платежах и платежных системах».

Возможности при дистанционном установлении деловых отношений

Реализация продукта по дистанционному установлению деловых отношений дала возможность:

1

исключить посещение отделений Банка клиентами и минимизировать физический контакт в условиях пандемии;

2

сократить время открытия счета, обеспечить клиентам доступ к осуществлению операций в дистанционном формате (с учетом установленных ограничений), а также, использованию канала для получения продуктов по кредитованию;

3

осуществить процедуры KYC в дистанционном формате при соблюдении всех требований НПА РК и ВНД Банка.




Комплаенс в период НОВЫХ ВЫЗОВОВ

Тимур Мусин | MBA, CAMS

2021 год

COVID-19



**Мир сильно
изменился..**

Влияние санитарно-эпидемиологических условий:

- рост использования дистанционных каналов
- рост количества онлайн операций
- рост социальной роли финансового сектора
- проверка на прочность процессов непрерывности (недостаток ресурсов, ИТ, простота процессов)
- переход большинства работников на дистанционную работу
- возможное снижение уровня соответствия (комплаенс)
- периодичность и качество проведения проверок

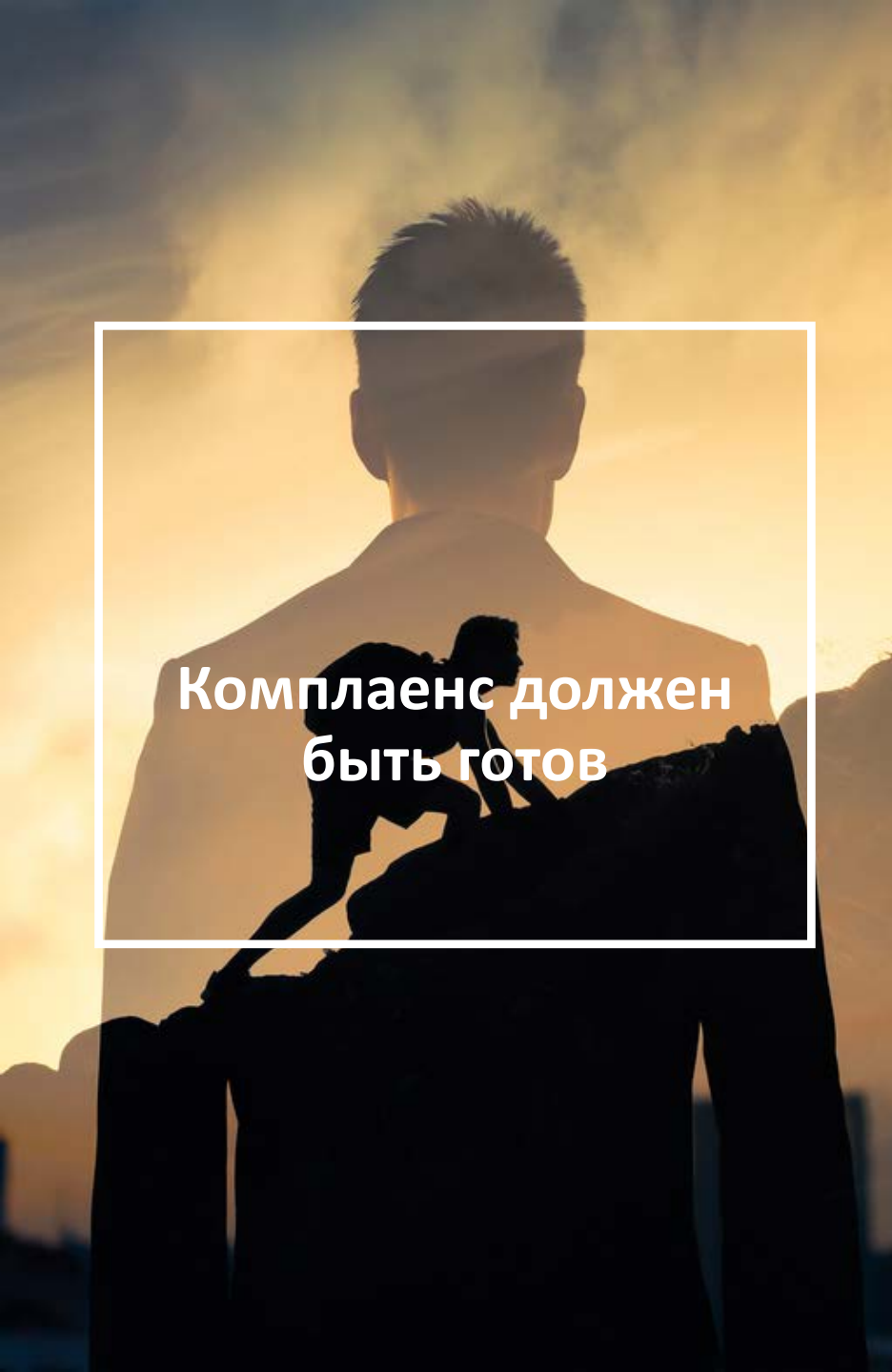
**Бизнес активно
меняется..**



АДАПТАЦИЯ

Банками и иными финансовыми организациями были осуществлены следующие мероприятия:

- сокращение количества рабочих часов/дней
- развитие инфраструктуры для удаленной работы
- обучение работников новым правилам игры
- забота о работниках (социальные программы, разделение на группы, обработка помещений, маски)
- постоянная обратная связь
- упрощение процессов (внутренних и внешних)
- активное изменение/развитие бизнеса (дистанционные каналы продаж, новые продукты/услуги)



Комплаенс должен
быть готов

НОВЫЕ ВЫЗОВЫ

Пандемия повлияла на деятельность комплаенс:

- проверка на прочность процессов комплаенс (отсутствие достаточных ресурсов и инструментов)
- резкое изменение бизнес-профиля клиентов
- новые схемы отмывания денег и рост количества подозрительных операций, связанных с коррупцией, отмыванием денег и использованием криптовалюты, мошенничеством и киберпреступностью
- риск раскрытия информации (уволненные работники, потеря данных работников, находящихся на удаленке, продукты с недостатками)
- недостаточное исполнение регуляторных требований в части своевременности предоставления информации в государственные органы
- приведение деятельности в соответствие с новыми требованиями



THIS WAY

**Что необходимо
предпринять?**

ANOTHER WAY

ОСНОВНЫЕ ШАГИ

Комплаенс необходимо обеспечить:

- тесное взаимодействие с бизнесом
- активное участие в согласовании и тестировании новых продуктов/услуг и каналов продаж
- отход от "бумажного комплаенс" в сторону развития комплаенс-культуры и задействование Whistleblowers
- работа с работниками (постоянная связь посредством внутренних социальных сетей, обучения, тона сверху)
- расширение полномочий комплаенс
- увеличение частоты взаимодействия с Правлением и Советом директоров
- своевременное предоставление отчетности и ответов
- налаживание эффективного взаимодействия с государственными органами
- поддержку достаточного уровня соответствия в дочерних организациях, особенно в части ПОД/ФТ (функционал, персонал, обучение)

ОСНОВНЫЕ ШАГИ

Комплаенс необходимо:

- переориентирование запланированных проверок в сферы с высоким риском
- автоматизация процессов комплаенс и ПОД/ФТ (уменьшение ручного труда в целях усиления аналитики, автоматические сценарии, заключения, проверки)
- совершенствование внутрибанковской типологии ПОД/ФТ, основанной на опыте собственном и международном
- развитие новых навыков и повышение универсальности работников комплаенс
- усиление процессов Know Your Employee
- участие в мероприятиях, проводимых HR
- оптимизация внутренних процессов комплаенс, повышение мобильности



Кто если не мы?



БЛАГОДАРЮ ЗА ВНИМАНИЕ!

mussintimur@mail.ru
www.linkedin.com/in/faceman/

Практика применения методов контроля для снижения рисков ОД/ФТ при принятии на обслуживание клиентов-организаций.

Минск
29 апреля 2021 г.

1. Февраль 20 года. Основной риск COVID-19, который мы ожидали.

- Вовлечение клиентов (организации, ИП) в «серую» деятельность, направленную на легализацию доходов, полученных преступным путем, из сфер бизнеса, которые наиболее серьезно пострадали, могли пострадать от экономического спада из-за вируса.

2. Меры контроля ПОД/ФТ, которые были выстроены ранее и используются сейчас.

- ✓ Обязательное предварительное согласование Compliance подразделением банка принятия на обслуживания организаций/ИП, связанных с
 - сферами бизнеса: азартные игры, финансовые услуги (лизинг, страхование, фонды, форекс, поставщики платежных услуг и т.п.);
 - странами, находящимися на контроле (оффшорные зоны, список ФАТФ, включая «усиленный мониторинг») - анализируется регистрация/гражданство/нахождение клиента, учредителей, руководителей, КБВ;

либо относящихся к категориям:

- нерезиденты;
- некоммерческие организации.
- ✓ Дополнительный (через 6 месяцев) анализ Compliance подразделением банка финансовых операций клиентов, указанных выше.
- ✓ Контроль за финансовыми операциями (особое внимание: увеличение оборотов, выплаты дивидендов, личный доход ИП).
- ✓ Вовлечение менеджеров на местах («Знай своего клиента»), особое внимание: смена предмета деятельности, смена учредителей на новых, связанных со странами, находящимися на контроле.

3. Выводы 2021 года.

- Общая тенденция: увеличилось количество финансовых операций, подпадающих под последующий мониторинг по перечислению ИП денежных средств на корпокарты и/или в целях снятия личного дохода.

Предмет деятельности ИП, по которым были направлены специальные формуляры был связан с:

Ⓜ G - ОПТОВАЯ И РОЗНИЧНАЯ ТОРГОВЛЯ; РЕМОНТ АВТОМОБИЛЕЙ И МОТОЦИКЛОВ	23.79%
Ⓜ L - ОПЕРАЦИИ С НЕДВИЖИМЫМ ИМУЩЕСТВОМ	15.16%
Ⓜ M - ПРОФЕССИОНАЛЬНАЯ, НАУЧНАЯ И ТЕХНИЧЕСКАЯ ДЕЯТЕЛЬНОСТЬ	13.68%
Ⓜ J - ИНФОРМАЦИЯ И СВЯЗЬ	11.37%
Ⓜ S - ПРЕДОСТАВЛЕНИЕ ПРОЧИХ ВИДОВ УСЛУГ	10.53%
Ⓜ F - СТРОИТЕЛЬСТВО	7.37%
Ⓜ N - ДЕЯТЕЛЬНОСТЬ В СФЕРЕ АДМИНИСТРАТИВНЫХ И ВСПОМОГАТЕЛЬНЫХ УСЛУГ	5.68%
Ⓜ H - ТРАНСПОРТНАЯ ДЕЯТЕЛЬНОСТЬ, СКЛАДИРОВАНИЕ, ПОЧТОВАЯ И КУРЬЕРСКАЯ ДЕЯТЕЛЬНОСТЬ	4.21%
Ⓜ C - ОБРАБАТЫВАЮЩАЯ ПРОМЫШЛЕННОСТЬ	4.00%
Ⓜ A - СЕЛЬСКОЕ, ЛЕСНОЕ И РЫБНОЕ ХОЗЯЙСТВО	1.47%
Ⓜ R - ТВОРЧЕСТВО, СПОРТ, РАЗВЛЕЧЕНИЯ И ОТДЫХ	1.05%
Ⓜ E - ВОДОСНАБЖЕНИЕ; СБОР, ОБРАБОТКА И УДАЛЕНИЕ ОТХОДОВ, ДЕЯТЕЛЬНОСТЬ ПО ЛИКВИДАЦИИ	0.84%

Виды деятельности ИП, открывших счета в 2020:

G - ОПТОВАЯ И РОЗНИЧНАЯ ТОРГОВЛЯ; РЕМОНТ АВТОМОБИЛЕЙ И МОТОЦИКЛОВ	22.79%
H - ТРАНСПОРТНАЯ ДЕЯТЕЛЬНОСТЬ, СКЛАДИРОВАНИЕ, ПОЧТОВАЯ И КУРЬЕРСКАЯ ДЕЯТЕЛЬНОСТЬ	15.54%
M - ПРОФЕССИОНАЛЬНАЯ, НАУЧНАЯ И ТЕХНИЧЕСКАЯ ДЕЯТЕЛЬНОСТЬ	15.52%
J - ИНФОРМАЦИЯ И СВЯЗЬ	9.24%
F - СТРОИТЕЛЬСТВО	8.80%
S - ПРЕДОСТАВЛЕНИЕ ПРОЧИХ ВИДОВ УСЛУГ	8.18%

Для примера, 2018 (было открыто в два раза меньше ИП), но сферы деятельности были схожи с «ковидным» периодом:

G - ОПТОВАЯ И РОЗНИЧНАЯ ТОРГОВЛЯ; РЕМОНТ АВТОМОБИЛЕЙ И МОТОЦИКЛОВ	29.56%
S - ПРЕДОСТАВЛЕНИЕ ПРОЧИХ ВИДОВ УСЛУГ	28.81%
H - ТРАНСПОРТНАЯ ДЕЯТЕЛЬНОСТЬ, СКЛАДИРОВАНИЕ, ПОЧТОВАЯ И КУРЬЕРСКАЯ ДЕЯТЕЛЬНОСТЬ	14.11%
M - ПРОФЕССИОНАЛЬНАЯ, НАУЧНАЯ И ТЕХНИЧЕСКАЯ ДЕЯТЕЛЬНОСТЬ	5.57%
F - СТРОИТЕЛЬСТВО	5.11%
J - ИНФОРМАЦИЯ И СВЯЗЬ	3.52%

- При проведении верификаций оснований для принятия дополнительных мер по приостановлению или отказу в осуществлении финансовых операций не выявлялось.

1. Хронология событий:

2018 год – регистрируются единичные случаи;

2019 – количество ежемесячно зарегистрированных случаев составляет десятки;

2020 – значительное увеличение.

Основная цель «мошенников» - физические лица (вишинг/фишинг*).

По нашим наблюдениям:

- при фишинге потери возникают у 55%;
- при вишинге у 24%;
- по количеству попыток – вишинг встречается чаще на 50%.

Для организаций характерны (разовые случаи):

- подмена реквизитов в договорах;
- удаленный доступ к ПК клиента.

Для успешного завершения схемы «мошенникам» необходим канал вывода денег:

- «подставные» лица;
- «добросовестные продавцы» (в основном это связано с последующими сделками по продаже крипто-валют).

* Фишинг - внутри различных сервисов (например, социальных сетей) осуществляются массовые рассылки писем, отправка личных сообщений (адресный фишинг) пользователям, где, как правило, содержится ссылка на сайт, внешне сходный с оригинальным.

Вишинг (англ. vishing – voice + phishing) – это устная разновидность фишинга, при которой злоумышленники посредством телефонной связи, используя приемы, методы и технологии социальной инженерии, под разными предлогами, искусно играя определенную роль (как правило, сотрудника банка, технического специалиста и т.д.), вынуждают человека сообщить им свои конфиденциальные банковские или персональные данные либо стимулируют к совершению определенных действий со своим банковским счетом или банковской картой

2. Методы и меры ПОД/ФТ, которые оказались востребованы в 2020 году.

✓ «К» за открытием счетов, «типовые портреты»:

организация резидент, руководителем/учредителем которой является гражданин РФ (без вида на жительство в РБ), дата регистрации которой совпадает с датой открытия счета в банке (либо предшествует ей на незначительный период: день/два);

физическое лицо: как правило, не имеющее договорные отношения с банком, гражданин РБ, со слов: безработный, основной акцент – необходимы неперсонифицированные БПК в максимально возможном количестве для личных целей.

✓ Приостановление и отказ клиенту в осуществлении финансовых операций.

Открытие счета:

- принятие решение об усилении «К» по ПОД/ФТ в целях согласования со службой Compliance банка расходных финансовых операций.

На данном этапе возможно направление специального формуляра (при дополнительных поведенческих признаках ПОД/ФТ), включая отказ в открытии счета и включение данных потенциального клиента в локальный стоп лист (в целях контроля за дальнейшими возможными операциями).

✓ **Приостановление и отказ клиенту в осуществлении финансовых операций.**

Счет открыт:

- попытка снять деньги в банкомате/кассе, осуществить перевод;
- приостановление (цель - верификация ИПДС) и/или отказ в осуществлении финансовой операции со ссылкой на нормы ПОД/ФТ;
- составление специального формуляра (в зависимости от пояснений или отказа от пояснений – количество указываемых признаков подозрительности может меняться);
- приостановление дистанционного обслуживания (возможность, предусмотренная законодательством ПОД/ФТ) с уведомлением клиента о принятом решении.

Информация от третьих лиц о подозрительном переводе или списании, попытке может также поступать в режиме 24/7 (Контакт центр банка).

В таком случае порядок «реагирования» будет аналогичным:

- ✓ незамедлительный технический арест по ДТ счета подозрительного клиента;
- ✓ приостановление проводимых платежей (если денежные средства не были еще «выведены») с верификацией и уведомлением клиента со ссылкой на нормы ПОД/ФТ;
- ✓ принятие решения об отказе в осуществлении финансовой операции, с уведомлением клиента со ссылкой на нормы ПОД/ФТ;
- ✓ принятие решения о приостановлении дистанционного обслуживания, с уведомлением клиента со ссылкой на нормы ПОД/ФТ;
- ✓ составление специального формуляра;
- ✓ присвоение высокой степени риска и включение клиента в локальный лист ограничений (в целях контроля за дальнейшими возможными операциями).

Спасибо за внимание!