РОСКОМНАДЗОР РОСФИНМОНИТОРИНГ

ОТЧЕТ О СЕКТОРАЛЬНОЙ ОЦЕНКЕ РИСКОВ ЛЕГАЛИЗАЦИИ (ОТМЫВАНИЯ) ПРЕСТУПНЫХ ДОХОДОВ И ФИНАНСИРОВАНИЯ ТЕРРОРИЗМА С ИСПОЛЬЗОВАНИЕМ СЕКТОРА ОПЕРАТОРОВ СВЯЗИ, ИМЕЮЩИХ ПРАВО САМОСТОЯТЕЛЬНО ОКАЗЫВАТЬ УСЛУГИ ПОДВИЖНОЙ РАДИОТЕЛЕФОННОЙ СВЯЗИ, А ТАКЖЕ ОПЕРАТОРОВ СВЯЗИ, ЗАНИМАЮЩИХ СУЩЕСТВЕННОЕ ПОЛОЖЕНИЕ В СЕТИ СВЯЗИ ОБЩЕГО ПОЛЬЗОВАНИЯ, КОТОРЫЕ ИМЕЮТ ПРАВО САМОСТОЯТЕЛЬНО ОКАЗЫВАТЬ УСЛУГИ СВЯЗИ ПО ПЕРЕДАЧЕ ДАННЫХ

Публичный отчет

Утверждено решением МВК
по ПОД/ФТ/ФРОМУ

6 марта 2019 года

/2018

СОДЕРЖАНИЕ

Операторы связи, имеющие право самостоятельно оказывать услуги подвижной радиотелефонной связи, а также операторы связи, занимающие существенное положение в сети связи общего пользования, которые имеют право самостоятельно оказывать услуги связи по передаче данных (далее – операторы связи) осуществляют свою деятельность на основании Федерального закона от 07.07.2003 года № 126-ФЗ «О связи» (далее - Федеральный закон № 126-ФЗ), постановления Правительства Российской Федерации от 09.12.2014 № 1342 «О порядке оказания услуг телефонной связи», постановления Правительства Российской Федерации от 23.01.2006 № 32 «Об утверждении Правил оказания услуг связи по передаче данных».

Согласно действующему законодательству, оператор связи - юридическое лицо или индивидуальный предприниматель, оказывающие услуги связи на основании соответствующей лицензии; оператор, занимающий существенное положение в сети связи общего пользования - оператор, который вместе с аффилированными лицами обладает в географически определенной зоне нумерации или на всей территории Российской Федерации не менее чем 25% монтированной емкости либо имеет возможность осуществлять пропуск не менее чем двадцати пяти процентов трафика.

Услуга связи - деятельность по приему, обработке, хранению, передаче, доставке сообщений электросвязи; абонент - пользователь услугами связи, с которым заключен договор об оказании таких услуг при выделении для этих целей абонентского номера или уникального кода идентификации.

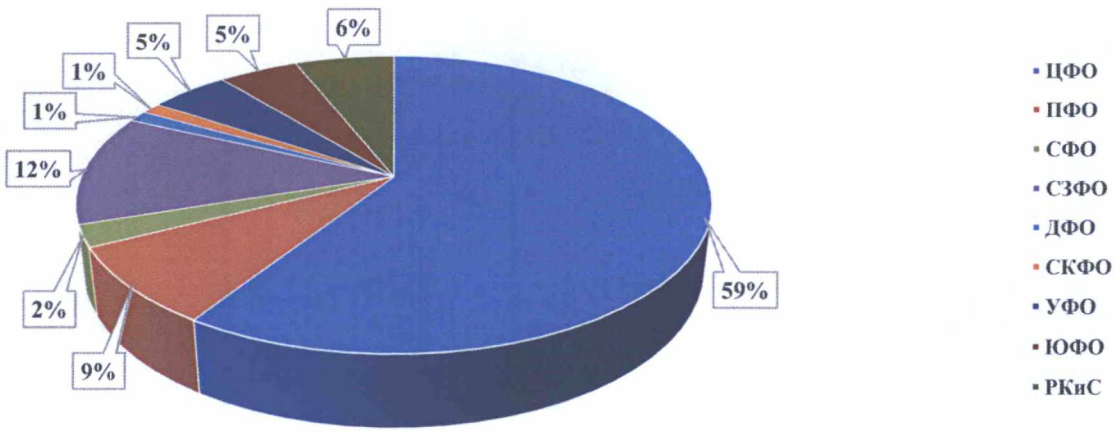
В настоящее время сектор операторов связи представлен следующими субъектами: 83 оператора связи, имеющие право самостоятельно оказывать услуги подвижной радиотелефонной связи, 9 операторов, занимающих существенное положение в сети связи общего пользования, которые имеют право самостоятельно оказывать услуги связи по передаче данных.

Операторы связи являются новыми участниками системы противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (далее – ПОД/ФТ). В 2013 году субъектами системы стали операторы подвижной радиотелефонной связи, в 2015 году - операторы, занимающие существенное положение в сети связи общего пользования.

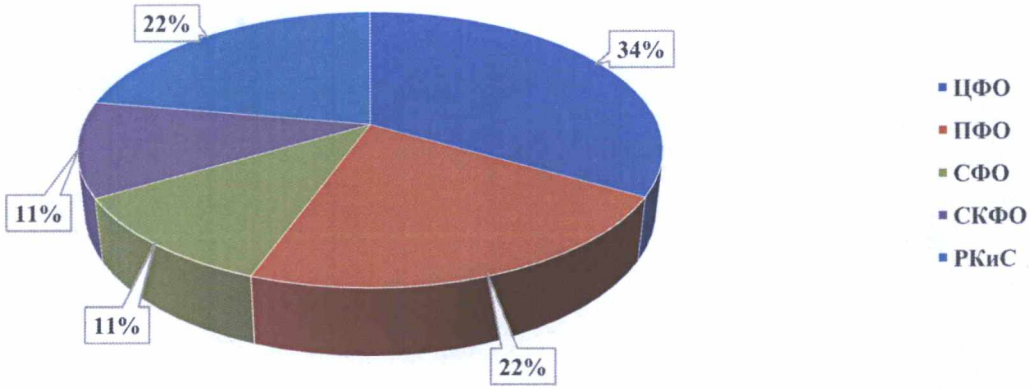
Наибольшая доля (более 50% сектора) присутствия объектов сектора приходится на Центральный федеральный округ.

Структура сектора операторов связи в региональном разрезе выглядит следующим образом:

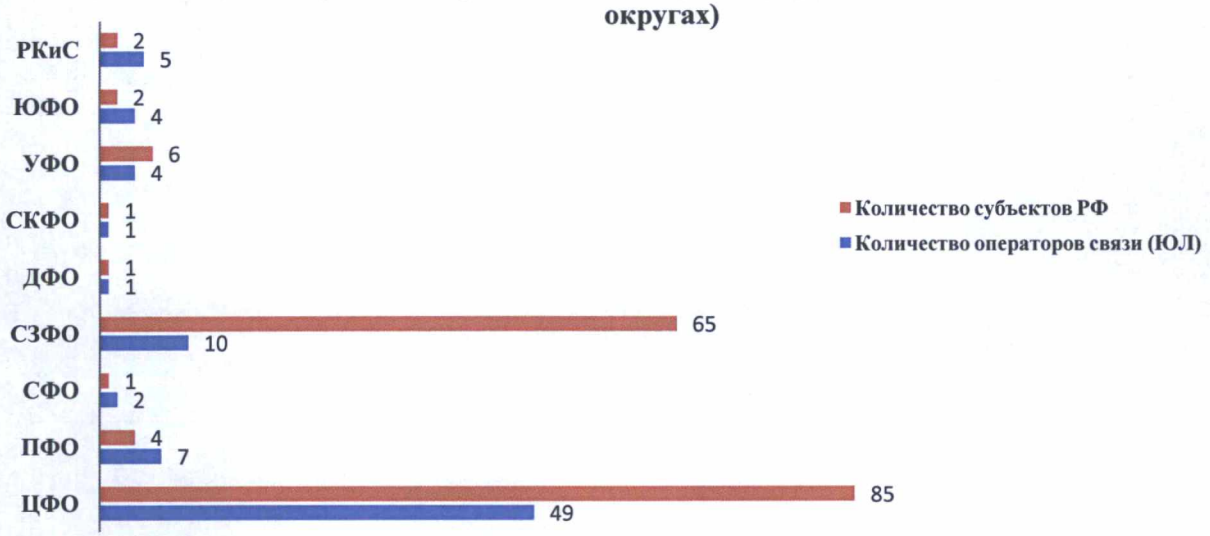
Распределение зарегистрированных субъектов сектора операторов подвижной радиотелефонной связи по федеральным округам



Распределение зарегистрированных субъектов сектора операторов, занимающих существенное положение в сети связи общего пользования, по федеральным округам



Территориальный охват (оказание услуг связи в субъектах РФ операторами подвижной радиотелефонной связи, зарегистрированными в федеральных округах)



Территориальный охват (оказание услуг связи в субъектах РФ операторами, занимающими существенное положение в сети связи общего пользования, зарегистрированными в федеральных округах)

Рынок телекоммуникационных услуг Российской Федерации находится в постоянном развитии. Основные сегменты рынка - мобильная связь и предоставление доступа в сеть «Интернет». Развитие российского рынка телекоммуникаций происходит по сценарию развития мирового рынка - растет количество абонентов связи. Увеличиваются финансовые показатели наиболее крупных компаний отрасли.

В последнее 10 лет наблюдается активное развитие подвижной радиотелефонной связи (мобильной связи)[1]. Операторы связи стремятся предоставлять качественный доступ в сеть «Интернет», развивать новые услуги и сервисы, например, совершение различного рода платежей (мобильные платежи) с использованием сотового телефона. Таким образом, множество финансовых операций совершаются с использованием услуг связи. При этом объём финансовых транзакций, осуществляемых с использованием инфраструктуры операторов связи, незначителен, по сравнению с иными финансовыми учреждениями.

На сегодня операторы связи активно развивают следующие финансовые сервисы:

1) *Мобильная коммерция*. Осуществление платежей или денежных переводов со счета телефона является сейчас основной составляющей дохода от финансовых услуг операторов связи. Ежемесячный оборот составляет 1-1,5 млрд руб., средняя доходность операторов - 5-7%. Основные категории, в рамках которых проходят платежи - денежные переводы, онлайн-игры, благотворительность. Сервис мобильной коммерции был запущен одним из первых финансовых услуг. Развитие происходит за счет подключения новых проектов, зарубежных сервисов, выхода в офлайн и новых категорий онлайн-ритейла.

2) *Микрокредитование*. На текущий момент работают сервисы микрокредитов у нескольких операторов связи. Кредитование также используется для операций в мобильной коммерции.

3) *Финансовый маркетплейс*. Предоставление собственных и партнерских услуг на «витринах» оператора. Каждый из операторов связи сейчас предлагает абонентам интернет-сервисы для оплаты товаров и услуг, совершения денежных переводов. Также появляются совместные и партнерские продукты, например, продажа страховых полисов.

4) *Финансовые услуги в офлайн-точках продаж услуг операторов связи*. Основной сервис - денежные переводы, также операторы связи развивают партнерские продажи прочих финансовых услуг.

На процедуру осуществления операторами связи финансовых услуг с использованием сотового телефона влияют требования законодательства Российской Федерации: должна быть получена максимальная информация об абоненте (клиенте), представителе клиента и (или) выгодоприобретателе, а также бенефициарных владельцев клиентов, в рамках реализации Федерального закона от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (далее - Федеральный закон № 115-ФЗ).

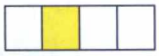
В соответствии с п. 9 ст. 7 Федерального закона № 115-ФЗ контроль за исполнением операторами связи, имеющими право самостоятельно оказывать услуги подвижной радиотелефонной связи, а также операторами связи, занимающими существенное положение в сети связи общего пользования, которые имеют право самостоятельно оказывать услуги связи по передаче данных, законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения (далее - ПОД/ФТ/ФРОМУ) возложен на Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

В настоящее время надзорная деятельность, осуществляемая Роскомнадзором в отношении сектора операторов связи, основывается на риск-ориентированном подходе, предусматривающем повышенное внимание к поднадзорным объектам, имеющим значительные и средние уровни риска нарушения требований законодательства о ПОД/ФТ/ФРОМУ (в этом случае, проводятся выездные и документарные проверки).

[1] В 2014 году абонентская база операторов мобильной связи составляла около 242 млн пользователей, на середину 2018 года - 340,3 млн абонентов. При этом замедляется темп роста объёма голосовых услуг и отправки коротких сообщений (SMS-сообщений) и одновременно увеличивается объём передачи данных.

В отношении поднадзорных субъектов с умеренным и низким уровнем риска реализуются мероприятия в формах наблюдения за соблюдением ими обязательных требований Федерального закона № 115-ФЗ (далее – обязательные требования) и профилактики нарушений обязательных требований (информирование по вопросам соблюдения обязательных требований, размещение на официальном сайте Роскомнадзора в сети Интернет программ профилактики и перечней нормативных правовых актов, содержащих обязательные требования, а также текстов соответствующих нормативных правовых актов, применение корректирующих мер в форме направления адресных писем и рекомендаций, организация и проведение семинаров, обучений, разъяснительной работы).

ХАРАКТЕРИСТИКА УГРОЗ



Умеренный уровень

Угроза — означает лицо, объект или деятельность, представляющие потенциальную опасность или могущие стать причиной ущерба или телесных повреждений.

В контексте ОД/ФТ это понятие включает преступников, их денежные средства и иные возможности, а также совершение ими приносящих доходы предикатных преступлений.

Сектор операторов связи в настоящее время характеризуется низкой криминализованностью.

Отмечаются признаки использования инфраструктуры операторов связи в финансовых схемах, целью которых может являться перемещение денежных средств и их вывод в неконтролируемый наличный оборот с участием физических лиц и юридических лиц с признаками фиктивности, в том числе для сокрытия доходов от налогообложения.

Специфика деятельности операторов связи - взаимодействие как с юридическими, так и с физическими лицами, поскольку услуга связи не ограничена предпринимательской деятельностью клиентов.

Бизнес-модель, которую используют операторы мобильной связи, преимущественно основана на агентской схеме привлечения абонентов (клиентов), в рамках которой операторы связи привлекают в качестве агентов большое число сторонних организаций, действующих, в свою очередь, от имени оператора связи по договору.

Законодательство Российской Федерации не предусматривает регистрацию и лицензирование таких агентов. Абоненты (клиенты) принимаются на обслуживание путем заключения договора на оказание услуг связи, который, во-первых, является публичной офертой, а во-вторых, в ряде случаев подписывается представителем оператора связи - агентом (действующим по доверенности), при отсутствии непосредственного взаимодействия с оператором связи. Оплата услуг подвижной радиотелефонной связи предполагает возможность установления отношений без личного присутствия.

Исходя из изложенного, основными угрозами сектора (использование «теневых» схем ОД/ФТ) являются:

1. Мошеннические действия за счет незаконно реализуемых sim-карт, использование которых потенциально может быть использовано в схемах ОД/ФТ.

Анализ последних 3-х лет работы в части ужесточения мер по незаконной продаже sim-карт и проведения совместно с правоохранительными органами контрольных мероприятий, показал увеличение количества выявляемых нарушений и, соответственно, изымаемых sim-карт. Для незаконной реализации sim-карт все активнее используется сеть «Интернет».

С целью принятия мер по минимизации угрозы в секторе в 2017 году приняты изменения в законодательные акты[2], предусматривающие предоставление услуги мобильной связи только тем абонентам, достоверные сведения о которых подтверждены в автоматизированной системе расчетов оператора связи. Также абонент - юридическое лицо либо индивидуальный предприниматель, при использовании корпоративных тарифов, обязан предоставлять оператору связи сведения о каждом фактическом пользователе.

2. Использование номеров сотовых телефонов, как инструмента, на котором могут аккумулироваться денежные средства с последующим их выводом в «теневой» оборот и (или) перемещением для целей финансирования терроризма.

Для реализации указанной схемы лица, причастные к совершению противоправных действий, используют платежные сервисы путем:
- увеличения остатка электронных денежных средств абонента (клиента) оператора связи (внесение платежей);
- возврата, в том числе в наличной форме, ранее внесенных денежных средств (платежей) по распоряжению абонента (клиента), в том числе по доверенности;
- перевода денежных средств с одного абонентского счета абонента (клиента) на иной абонентский счет.

[2] Федеральным законом от 29.07.2017 № 245-ФЗ «О внесении изменений в закон «О связи» внесены поправки в Федеральный закон № 126-ФЗ с целью пресечения распространения sim-карт без предоставления реальных паспортных данных абонента.

Для реализации схемы «обналичивания» денежных средств используются номинальные юридические лица и физические лица (подставные, посредники), например, через услугу мобильной коммерции:

- на лицевые счета абонентов (физических лиц) от организаций, деятельность которых носит подозрительный (сомнительный) характер, поступают денежные средства. Абоненты (физические лица), используя услуги мобильной коммерции, осуществляют расчёты за товары, работы, услуги, либо получают (возвращают) неиспользованный остаток денежных средств наличными или путём перевода на банковский счёт (через кредитные организации). Денежные средства могут быть также сняты в наличной форме третьими лицами через банкоматы.

Принятыми надзорными мерами угрозы снижены, усилен контроль за исполнением требований Федерального закона № 115-ФЗ. Также внесены изменения в Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платежной системе» (далее - Федеральный закон № 161-ФЗ), устанавливающие правовые ограничения по увеличению остатка электронных денежных средств физического лица – абонента[3].

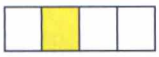
Результатом принятия мер надзорного характера, совершенствования системы внутреннего контроля операторов связи, межведомственной координации действий, стало значительное снижение на конец 2018 года (в сравнении с 2017 годом) объёмов сомнительных операций с денежными средствами, проводимых через крупных операторов связи[4].

Вывод: *последние несколько лет угроза вовлечения операторов связи в схемы ОД значительно снижена, в том числе в связи с осуществлением эффективного контроля со стороны государства, надзорного органа в данном секторе, а также кредитных организаций, в силу чего уровень оценивается, как умеренный.*

[3] Оператор электронных денежных средств не вправе осуществлять увеличение остатка электронных денежных средств физического лица – абонента при превышении сумм при использовании персонифицированного электронного средства платежа в размере, установлено ст. 10 Федерального закон № 161-ФЗ, а при использовании неперсонифицированного электронного средства платежа – в размере 15 тыс. руб. (или эквивалент данной суммы в иностранной валюте).

[4] По данным кредитных организаций и Роскомнадзора – более чем в 7 раз.

ХАРАКТЕРИСТИКА УЯЗВИМОСТЕЙ



Умеренный уровень

Уязвимость — означает свойство, присущее системе или структуре, которое делает ее «доступной» для незаконного использования в целях ОД/ФТ.

Определение уязвимости, в отличие от угрозы, означает сосредоточение внимания на слабых местах в системе или мерах контроля в сфере ПОД/ФТ или на характеристиках финансовых продуктов (услуг), которые делают их привлекательными для целей ОД/ФТ. При рассмотрении уязвимости (как элементе оценки риска) внимание будет сосредоточено, главным образом, на факторах, способных повысить вероятность совершения ОД/ФТ.

Результаты оценки уязвимости сектора на предмет удобства и видимости каналов, позволяющих реализоваться угрозам, показали, что ранее сектор организаций операторов связи характеризовался неудовлетворительным уровнем исполнения «антиотмывочного» законодательства.

Ввиду актуальности вопроса использования функционала Личного кабинета, Роскомнадзором и Росфинмониторингом уделяется повышенное внимание профилактическим мероприятиям, включающим вопросы разъяснения преимущества работы в нем: ознакомление с информационными материалами, принятие участия в «добровольном сотрудничестве», получение доступа к полному Перечню организаций, физических лиц, в отношении которых имеются сведения об их причастности к экстремистской деятельности или терроризму (далее – Перечень), направление сведений по операциям, подлежащим обязательному контролю, и о сомнительных операциях в Росфинмониторинг, а также направление информации о результатах проверки своих клиентов, в отношении которых применены либо должны применяться меры по замораживанию (блокированию) денежных средств или иного имущества (ФЭС-3).

Главным результатом проведения таких мероприятий является повышение уровня законопослушности субъектов сектора на конец 2018 года на 3% (в сравнении с началом 2018 года), в том числе за счет использования функционала Личного кабинета.

В настоящее время основными уязвимостями сектора, подтверждаемые, в том числе результатами проведенных Роскомнадзором проверок, являются:

- непроведение идентификации клиентов надлежащим образом. Гражданское законодательство и нормативные правовые акты в сфере связи позволяют операторам связи поручать третьим лицам (дилерам/агентам) заключать договора об оказании услуг связи, осуществлять расчеты с абонентами и иные действия по обслуживанию абонентов (клиентов) от имени оператора связи. Следовательно, в ряде случаев отсутствует непосредственное взаимодействие абонента (клиента) с оператором связи;

- недостаточное знание (понимание) положений нормативных правовых актов в сфере ПОД/ФТ сотрудниками операторов связи, а также возможных последствий (ущерба), следующих за противоправными действиями клиентов, направленными на ОД/ФТ.

Основные нарушения, выявленные Роскомнадзором по результатам проверок 2016-2018 гг. в отношении операторов связи

Возбужденные дела об административном производстве в соответствии с ч. 1 ст. 15.27 КоАП РФ[5]	Возбужденные дела об административном производстве в соответствии в соответствии с ч. 2,2.1 ст. 15.27 КоАП РФ
несоответствие Правил внутреннего контроля в целях ПОД/ФТ требованиям, установленным нормативными правовыми актами в сфере ПОД/ФТ, несвоевременное внесение изменений в Правила; отсутствие Правил внутреннего контроля	нарушения в части выявления операций, имеющих признаки подозрительности (необычности), не направление в уполномоченный орган сведений о таких операциях
нарушения, связанные с несоблюдением требований по подготовке и обучению кадров	направление неверных и/или недостоверных сведений об операциях, подлежащих обязательному контролю, в уполномоченный орган
нарушение (не проведение / проведение не в полном объеме, не обновление / несвоевременное обновление сведений и т.д.) порядка идентификации клиентов, представителей, выгодоприобретателей и бенефициарных владельцев	не направление в Росфинмониторинг сведений по результатам проверки наличия среди своих клиентов лиц из Перечня

Результаты проведенных проверок соблюдения требований законодательства о ПОД/ФТ в отношении операторов связи

Показатели / Период		2016 год	2017 год	2018 год
Количество проверок в отношении субъектов сектора		137	168	36
Возбужденные дела об административном правонарушении, в том числе:	часть 1 статьи 15.27 КоАП РФ	35	16	16
	часть 2 статьи 15.27 КоАП РФ	3	1	0
	часть 2.1 статьи 15.27 КоАП РФ	0	0	0
	часть 3 статьи 15.27 КоАП РФ	0	0	0
Доля существенных нарушений требований законодательства о ПОД/ФТ (количество субъектов, привлеченных к ответственности по ч. 2, ч. 2.1 и ч. 3 ст. 15.27 КоАП РФ)		8%	5,8%	0

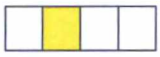
Снижению уровня уязвимости в секторе способствовало расширение (по предложению Роскомнадзора) Перечня признаков операций, осуществление которых может быть направлено на финансирование терроризма (внесены дополнения в приказ Росфинмониторинга № 103[6] по коду группы 42 «Признаки необычных сделок, выявляемые при осуществлении деятельности оператора связи, имеющего право самостоятельно оказывать услуги подвижной радиотелефонной связи»).

Вывод: *итоговые оценки уровня законопослушности в секторе операторов связи и результаты проверок позволяют сделать вывод об умеренном уровне уязвимости.*

[5] Кодекс об административных правонарушениях Российской Федерации – далее КоАП РФ

[6] Приказ Росфинмониторинга от 05.05.2009 № 103 «Об утверждении рекомендаций по разработке критериев выявления и определению признаков необычных сделок».

УРОВЕНЬ РИСКА ИСПОЛЬЗОВАНИЯ СЕКТОРА В СХЕМАХ ОД/ФТ



Умеренный уровень

Сопоставление результатов оценки угроз и уязвимостей позволяет классифицировать риск использования субъектов сектора в схемах ОД/ФТ, а также выработать меры по снижению этого риска.

Инфраструктура сектора операторов связи используется в схемах легализации преступных доходов. В значительной мере прослеживаются риски использования номинальных юридических лиц, физических лиц (подставных, посредников) в схемах «обналичивания».

Вместе с тем указанные риски вовлечения сектора и его клиентов в противоправные схемы нивелируются государственным контролем (Роскомнадзором, Росфинмониторингом, ФНС России), Банком России и кредитными организациями.

Для целей финансирования терроризма способ перемещения денежных средств в целом через операторов связи наименее востребован, поскольку требует дополнительных действий со стороны террористических групп. При этом возможность использования номеров сотовых телефонов для аккумулирования денежных средств в целях финансирования терроризма увеличивает уровень риска в этом секторе.

Сектор недостаточно информирован о возможностях вовлечения в противоправную деятельность и о рисках ОД/ФТ.

Вывод: *масштаб сектора, наличие выявленных угроз и обозначенных уязвимостей, формируют вывод об* ***умеренном*** *уровне угрозы,* ***умеренном*** *уровне уязвимости, и, как следствие,* ***умеренном*** *уровне риска использования сектора для целей ОД и ФТ.*

МЕРЫ ПО СНИЖЕНИЮ РИСКОВ

МЕРЫ МЕЖВЕДОМСТВЕННОГО ХАРАКТЕРА

В целях снижения рисков ОД/ФТ в рамках межведомственного взаимодействия реализуются следующие мероприятия:

- межведомственная координация действий в целях пресечения проводимых через сектор сомнительных операций с денежными средствами и незаконной реализации sim-карт;

- совершенствование нормативных правовых актов, предусматривающих применение риск-ориентированного подхода при планировании и проведении контрольно-надзорных мероприятий (Административный регламент).

МЕРЫ НАДЗОРНОГО РЕАГИРОВАНИЯ

- реализация мероприятий по минимизации выявленных рисков ОД/ФТ в поднадзорных секторах;

- повышение эффективности принимаемых надзорных мер за деятельностью операторов связи в части соблюдения требований законодательства о ПОД/ФТ, понимания рисков ОД/ФТ, принятия соразмерных мер по снижению рисков и повышению качества направляемых сведений об операциях в уполномоченный орган;

- повышение уровня вовлеченности в систему ПОД/ФТ сектора посредством проведения профилактических мероприятий с главным акцентом на содержательной части исполнения законодательства о ПОД/ФТ, в том числе через механизм Личного кабинета.

МЕРЫ СУБЪЕКТОВ СЕКТОРА

Использовать результаты секторальных оценок рисков ОД/ФТ при разработке внутренней политики, правил внутреннего контроля и иных документов в области управления рисками ОД/ФТ, обучения персонала, выработки механизмов и мер по выявлению и снижению рисков, в том числе по идентификации и оценке рисков клиентов (их представителей, бенефициарных владельцев), выявлению подозрительных операций и проведению иных мероприятий, направленных на ПОД/ФТ.

Москва, 2018