

Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт экономики, управления и природопользования
кафедра финансов

УТВЕРЖДАЮ
Заведующий кафедрой

_____ И.С. Ферова

подпись

« _____ » _____ 2016 г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

Направление подготовки
080100 «Экономика»
Профиль «Финансы и кредит»

СОВЕРШЕНСТВОВАНИЯ ОРГАНИЗАЦИОННО-ЭКОНОМИЧЕСКИХ
ОСНОВ ПРОТИВОДЕЙСТВИЯ ОТМЫВАНИЯ ДЕНЕГ В
ДИСТАНЦИОННОМ БАНКОВСКОМ ОБСЛУЖИВАНИИ (НА ПРИМЕРЕ
ПАО «СБЕРБАНК РОССИИ»)

Научный

руководитель

подпись, дата

д-р.э.н., профессор

_____ И.А. Янкина

должность, ученая степень

Выпускник

подпись, дата

А.В.. Деревяшкина

Нормоконтролер

подпись, дата

Л.П. Жигаева

инициалы,

фамилия

Красноярск 2016
СОДЕРЖАНИЕ

Введение.....	4
1 Теоретические основы противодействия отмывания денег в условиях ДБО	7
1.1 Противодействия отмывания денег: понятия, нормативно методическое обеспечение, международные аспекты	7
1.2 Дистанционное банковское обслуживание как сфера деятельности банка, сопряженная с противодействием отмывания денег.....	17
1.3 Инструментарий организационно-экономических основ противодействия отмывания денег	24
2 Анализ состояния противодействия отмывания денег в дистанционном банковском обслуживании (ДБО).....	41
2.1 Организационно-экономическая характеристика банка	41
2.2 Оценка финансовых результатов и факторов снижающих эффективность ДБО с учетом противодействия отмывания денег	50
3 Совершенствование организационно-экономических основ противодействия отмывания денег в дистанционном банковском обслуживании на примере ПАО «Сбербанк».....	61
3.1 Разработка схемы противодействия отмывания денег в дистанционном банковском обслуживании на примере ПАО «Сбербанк»	61
3.2 Затраты на реализацию мероприятий.....	69
3.3 Расчет экономической эффективности мероприятий	76
Заключение	80
Список использованных источников	84
Приложения А-Б.....	89-97

ВВЕДЕНИЕ

В современных условиях легализация преступных доходов представляет опасность не только для отдельных государств, но и для всего международного сообщества. По оценкам экспертов Международного валютного фонда, преступные организации ежегодно легализуют от 0,5 до 1,5 триллионов долларов, что составляет до 5% валового мирового продукта. В настоящее время проблема отмывания денег стала одной из основных проблем глобального характера, к решению которых привлечены многие ведущие страны мира. Процедура отмывания денег характерна практически для всех форм организованной преступности, которая искажает процесс принятия экономических решений, подрывает финансовые учреждения, обостряет социальные проблемы и, что самое основное, способствует коррупции.

Проблема привлечения к ответственности за отмывание преступных доходов в последние годы приобретает все большее внимание, как у ученых-юристов, работников банковской сферы, так и у правоохранительных органов и надзорных организаций. Большинство государств – особенно это касается развитых стран мира – усиленно разрабатывают и применяют меры, направленные на борьбу с легализацией преступного движения капитала.

Актуальность темы работы определяется тем, что проблемы противодействия легализации доходов, полученных преступным путем, и финансированию терроризма возрастает в виде уменьшения доходов всех уровней бюджетной системы, увеличения расходов, необходимых для финансирования правоохранительного сектора, дефицита бюджета, сбалансированности государственной денежно-кредитной политики.

Исследования на тему отмывания денег сейчас представляют особую остроту.

Вопросы организации финансового мониторинга в коммерческих банках в различных аспектах исследованы в работах Воронина А.Н., Газияна С.В., Гамзы В.А., Дудки А.Б., Жубрина Р.В., Зубкова В.А., Каратаева М.В., Красавиной Л.Н., Лебедевой М.Е., Лебедевой Т.В., Люкевича И.Н., Ревенкова П.В., Магомедова Ш.М., Осипова С.К., Прошунина М.М., а также в трудах зарубежных специалистов Ф. Робинсона, А. Шильдера, Фитуни Л.Л., И. Кэцлер и др.

Несмотря на наличие многочисленных публикаций, посвященных сущности и особенностям реализации противозаконных процедур в деятельности кредитных организаций, вопросам организации и оптимизации деятельности финансового мониторинга в коммерческих банках, а также исследованию особенностей функционирования российских кредитных организаций в области основы противодействия отмывания денег в условиях ДБО в них уделяется мало внимания.

В связи с этим, в работе рассматриваются указанные проблемы на примере коммерческой кредитной организации.

Объект исследования - ПАО Сбербанк.

Предметом исследования выступает деятельность финансово-кредитных институтов и государственных надзорных органов по противодействию отмывания денег в условиях ДБО.

Цель данной работы – выявить перспективные меры противодействия отмывания денег в условиях ДБО на примере конкретного регионального банка. Для достижения цели будут решены задачи:

- рассмотреть понятия, нормативно методическое обеспечение, международные аспекты противодействия отмыванию денег;
- проанализировать дистанционное банковское обслуживание как сферу деятельности банка, сопряженную с противодействием отмывания денег;

- рассмотреть инструментарий организационно-экономических основ противодействия отмывания денег
- проанализировать деятельность коммерческого банка и факторов снижающих эффективность ДБО с учетом противодействия отмывания денег.

Теоретико-методологической основой работы явились нормативно – правовые акты, монографии российских специалистов, материалы периодической печати, посвящённые проблемам противодействия отмывания денег и внутренняя отчетность банка.

Эмпирическую базу исследования составили данные коммерческого банка.

Работа имеет особую практическую значимость в связи с тем, что в ней разработана схема противодействия отмывания денег в дистанционном банковском обслуживании на примере ПАО «Сбербанк».

1 Теоретические основы противодействия отмывания денег в условиях ДБО

1.1 Противодействия отмывания денег: понятия, нормативно методическое обеспечение, международные аспекты

Наиболее широкое определение термина "отмывание преступных доходов" содержится в ст. 6 Конвенции против транснациональной организованной преступности (принята в г. Нью-Йорке 15 ноября 2000 г. Резолюцией 55/25 на 62-м пленарном заседании 55-й сессии Генеральной Ассамблеи ООН). В соответствии с ней основными действиями, которые международные правоведы относят к отмыванию преступных доходов, являются:

- конверсия или перевод имущества, если известно, что такое имущество представляет собой доходы от преступлений, в целях сокрытия или утаивания преступного источника этого имущества или в целях оказания помощи любому лицу, участвующему в совершении основного правонарушения, с тем чтобы оно могло уклониться от ответственности за свои деяния;

- сокрытие или утаивание подлинного характера, источника, местонахождения, способа распоряжения, перемещения, прав на имущество или его принадлежность, если известно, что такое имущество представляет собой доходы от преступлений;

- приобретение, владение или использование имущества, если в момент его получения известно, что такое имущество представляет собой доходы от преступлений;

- участие, причастность или вступление в сговор с целью совершения любого из преступлений, признанных таковыми по настоящему определению, покушение на его совершение, а также пособничество, подстрекательство, содействие или дача советов при его совершении [12].

Таким образом, под отмыыванием преступных доходов международное сообщество призывает понимать действия (бездействие) относительно имущества, приобретенного преступным путем, независимо от того, желает ли лицо придать правомерный характер данному имуществу или нет. При этом деятельность будет преступной только в том случае, если лицо знало о преступном происхождении данного имущества.

В настоящее время российское законодательство оперирует двумя определениями легализации доходов, полученных преступным путем.

В Уголовном кодексе РФ, впервые в 1996 г. закрепившем термин "легализация (отмыывание) денежных средств или иного имущества, приобретенного преступным путем", в ст. ст. 174 и 174.1 под легализацией (отмыыванием) денежных средств или иного имущества, приобретенного преступным путем, понимается совершение финансовых операций и других сделок с денежными средствами или иным имуществом, заведомо приобретенными другими лицами преступным путем (в ст. 174.1 лицом в результате совершения им преступления), в целях придания правомерного вида владению, пользованию и распоряжению указанными денежными средствами или иным имуществом [6, с.154].

Нормативное определение легализации (отмыывания) доходов, полученных преступным путем, закреплено в Федеральном законе от 7 августа 2001 г. N 115-ФЗ "О противодействии легализации (отмыыванию) доходов, полученных преступным путем, и финансированию терроризма" (далее по тексту - Федеральный закон N 115-ФЗ). В рамках указанного Закона под легализацией (отмыыванием) доходов, полученных преступным путем, следует понимать придание правомерного вида владению,

пользованию или распоряжению денежными средствами или иным имуществом, полученными в результате совершения преступления.

Ранее нормативное определение легализации (отмывания) преступных доходов в качестве предикатных преступлений не рассматривало налоговые, валютные и таможенные преступления.

Термины "отмывание" и "легализация" доходов, полученных преступным путем, являются синонимами и могут употребляться как взаимозаменяемые понятия.

Недостаток термина "легализация преступных доходов" состоит в том, что термин "легализация" используется для определения легального процесса, а именно легализации официальных документов. В отношении легализации преступных доходов данный процесс (по правовому содержанию) никогда не станет легальным, наоборот, он является уголовным правонарушением. В свою очередь, недостаток термина "отмывание преступных доходов" - в его бытовом характере, что несколько затрудняет его использование в нормотворчестве. В российском законодательстве выходом из сложившейся ситуации стало использование обоих терминов - "отмывание" и "легализация".

В настоящее время в финансово-правовой науке практически отсутствуют определения отмывания преступных доходов, что не случайно, так как данные вопросы принято рассматривать в основном в уголовно-правовом аспекте. Одно из немногих - определение В.М. Шумилова, который в рамках международного финансового права под отмыванием денег понимает процесс преобразования нелегально полученных денег в легальные [11].

Немецкий ученый Х.Х. Кернер определяет отмывание денег как "операции, осуществляемые с целью на первой стадии утаить или скрыть наличие, происхождение или целевое назначение вещественных ценностей, проистекающих из преступления, с тем чтобы на второй стадии приступить к извлечению из них регулярных доходов" [9].

М.Е. Беар определяет отмывание преступных доходов как "перевод незаконно полученных наличных денег в другой актив, сокрытие истинного источника или собственности, от которых незаконным образом получены деньги, и создание характера законности для источника и собственности" [13].

Отмывание преступных доходов следует рассматривать в четырех основных аспектах: материальном, процедурном, экономическом и правовом.

В материальном аспекте отмывание представляет собой размещение имущества, в том числе денежных средств, в финансовые институты, проведение различного рода операций с данным имуществом и, наконец, интегрирование имущества в национальную экономику. В материальном аспекте основным является характер действий: размещение, расслоение (перемешивание) и интегрирование.

В экономическом смысле отмывание представляет собой переход денежных средств или иного имущества, полученного преступным путем, из теневой экономики в легальную экономику. В экономическом аспекте важно, что денежные средства или иное имущество попадают в легальную экономику. В этом контексте следует отличать легализацию (отмывание) преступных доходов от незаконного обналичивания денежных средств. В последнем случае имеет место перевод денежных средств из легальной экономики в теневую экономику, т.е. незаконное обналичивание денежных средств - это процесс, обратный легализации (отмыванию) преступных доходов [24, с.184].

С процедурной точки зрения отмывание преступных доходов можно определить как процесс, с помощью которого маскируются изначальное происхождение и истинные владельцы имущества, полученного в результате совершения преступления, в целях исключения любого из видов преследования (административного, уголовного). В этой связи отмывание также можно определить как процесс обработки имущества в целях сокрытия его незаконного получения фактическим владельцем.

И наконец, с правовой точки зрения отмыывание преступных доходов следует рассматривать как придание правомерного характера владению, пользованию или распоряжению денежными средствами или иным имуществом, которые получены преступным путем. В юридическом смысле главным становится именно правомерный характер, который приобретает имущество.

Нормативно-правовое регулирование в области противодействия отмыыванию денежных средств или иного имущества происходит как на международном, так и на национальном уровне. Это связано с тем, что данное преступление имеет транснациональный характер. Законодательную базу условно можно разделить на следующие группы [16]:

1) документы международных органов и институтов (ООН, ИНТО САИ, Базельский комитет, ОЭСР и др.);

2) региональные документы (Совет Европы, Европейский союз, Содружество Независимых Государств и др.);

3) документы специального органа по противодействию отмыыванию - ФАТФ;

4) национальная нормативная правовая база, внутри которой выделяются законы и иные нормативные правовые акты.

На сегодняшний день существуют следующие документы, позволяющие противодействовать легализации доходов:

- международные акты общего характера (в частности, Базельские принципы 1988 г., Венская конвенция ООН о борьбе против незаконного оборота наркотических средств и психотропных веществ от 20 декабря 1988 г., Конвенция Совета Европы об отмыывании, выявлении, изъятии и конфискации доходов от преступной деятельности от 8 ноября 1990 г., Международная конвенция ООН о борьбе с финансированием терроризма 1999 г., Конвенция ООН против транснациональной организованной преступности от 15 ноября 2000 г., Всеобщие директивы по противодействию отмыыванию доходов в частном банковском секторе от 30

октября 2000 г. (Вольфсбергские принципы), Рекомендации Базельского комитета "Знай своего клиента" от 1 октября 2001 г. (Стандарты Базельского комитета банковского надзора), Конвенция Совета Европы об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности и о финансировании терроризма от 16 мая 2005 г.);

- акты, принятые в рамках Европейского союза (в частности, Договор о создании Европейского союза (Маастрихтский договор) от 7 февраля 1992 г., Шенгенские соглашения от 14 июня 1985 г. (Шенген I) и от 19 июня 1990 г. (Шенген II), Директива по предотвращению использования финансовой системы в целях отмывания денег, заложившая вектор дальнейшей борьбы с отмыванием на уровне Европейского экономического сообщества 1991 г., Директива 2001 г. Европейского союза 2001/97/ЕС о внесении изменений в директиву 1991 г., Третья директива 2005 г. N 2005/60/ЕС "О предотвращении использования финансовой системы для отмывания денег, включая финансирование терроризма", проект Четвертой директивы от 5 февраля 2013 г. 2013/0025 (COD) "О предотвращении использования финансовой системы в целях отмывания денег и финансирования терроризма").

Изучение вышеназванных документов позволяет сделать вывод, что в мире проводится серьезная работа по совершенствованию эффективности противодействия. Поэтому и Россия не может оставаться в стороне от этих требований.

Россия как член Группы разработки финансовых мер борьбы с отмыванием денег (далее - ФАТФ) несет обязанность по выполнению рекомендаций данного органа и приведению законодательства о противодействии легализации в соответствие с требованиями международных органов [19, с.144].

Соглашаясь с мнением М.А. Филатовой, следует констатировать, что имеющаяся в настоящий момент формулировка в ст. ст. 174 и 174.1 УК РФ объективной стороны отмывания не охватывает все способы отмывания в

соответствии с международными обязательствами России. Такие действия, как конверсия или перевод, охватываются понятием "сделка". Однако что касается сокрытия или утаивания, то эти деяния могут происходить и без совершения каких-либо сделок. Приобретение, владение и пользование также весьма спорно обозначать как охватываемые объективной стороной ст. ст. 174 и 174.1 УК РФ, поскольку владение и пользование являются институтами вещного права, в то время как сделка - институт права обязательственного, поэтому "владеть" с помощью сделки представляется не всегда возможным. Также и использование имущества исключительно в определенных случаях можно рассматривать в качестве сделки. Придание правомерного вида преступно полученным доходам может иметь место и путем совершения таких фактических, а не юридических действий, как например, использование краденого оборудования с извлечением прибыли из него. Данный факт подтверждает уже высказывавшееся в литературе мнение о необходимости дополнения (или изменения) ст. ст. 174 и 174.1 УК РФ путем использования для обозначения объективной стороны деяния обобщающего термина "действие" либо - как это сделано в уголовных кодексах Австрии и Германии - путем закрепления наиболее широкого спектра потенциальных деяний по сокрытию происхождения преступного имущества и его введению в экономический оборот, независимо от того, были ли для этого совершены сделки или нет [14].

В феврале 2012 г. ФАТФ пересмотрела обязательные международные стандарты по противодействию легализации преступных доходов и финансированию терроризма. Новые единые принципы и правила потребуют от России изменений в Гражданском, Уголовном, Налоговом кодексах, а также корректировки "антиотмывочного" Федерального закона. Поводом послужили, с одной стороны, новые вызовы и угрозы, которые обозначились перед мировой финансовой системой в последние годы. С другой стороны, дальнейшего развития требовал накопленный опыт по применению старых рекомендаций [8].

Особую тревогу для всего мирового сообщества вызывает использование офшорных юрисдикций, которые тесно связаны с проблемами уклонения от налогообложения и сокрытия доходов, полученных преступным путем, в том числе в результате коррупции. В первую очередь такие схемы позволяют завуалировать конечного собственника активов - как денег, так и имущества. Основной целью должна стать - ликвидация таких юрисдикций. Для этого надо разработать и утвердить меры, как правовые, так и экономические, которые сделают невозможным и невыгодным использование офшорных территорий. Возможно, применять к ним определенные рычаги давления на международном уровне с тем, чтобы снизить экономическую привлекательность для бизнеса. Введение налога на финансовые операции с участием фирм, зарегистрированных в офшорах, может стать одной из таких мер. В развитии этого вопроса также значимыми являются "фирмы-однодневки", которые создаются для проведения нелегальных финансовых схем и имеют, как правило, небольшой жизненный цикл. Россия не является исключительным местом применения подобных структур. В международной практике они называются "фирмы-оболочки" и активно используются в теневых финансовых сделках. Главным препятствием в борьбе являются проблемы установления истинных владельцев таких псевдоструктур. ФАТФ в новых рекомендациях, которые усиливают меры по установлению реальных собственников, предлагает выявлять фирмы-однодневки в процессе финансового мониторинга с последующим ограничением их доступа к финансовым услугам. [26] Например, ограничивая возможность совершения операций по банковскому счету. Контроль должен быть налажен уже на этапе регистрации юридического лица. Также надо выявлять уже действующие структуры. Например, на основе активно используемого публичного реестра. Его могут сформировать налоговые органы. И при необходимости применять к таким фирмам жесткие санкции, вплоть до уголовной ответственности. Целесообразность введения в России уголовной ответственности для

юридических лиц сейчас тоже активно обсуждается. До сих пор в отличие от других стран такой ответственности не установлено.

Вместе с тем понятию "отмывание доходов" в современных международных документах не дается точного определения. По мнению М.В. Каратаева, данное явление должно рассматриваться в виде процесса, в ходе которого происходит сокрытие средств или имущества, полученных в результате незаконной деятельности, их размещение, перевод или любое движение через финансово-кредитную систему, приобретение на них имущества или использование иным образом в экономической деятельности так, что они в конечном итоге возвращаются к владельцу в "воспроизведенном" виде с целью придания правомерного вида этим доходам, сокрытия их реальных владельцев, или противозаконности оснований и источников получения [5].

В новых рекомендациях ужесточаются требования по идентификации клиентов банков, в том числе тех, кто зарегистрирован в офшорах. В частности, таким компаниям придется предоставлять в финансовые учреждения достоверные сведения о реальных собственниках и владельцах активов. В случае невозможности установления бенефициарного собственника, банки обязаны не открывать счет и не проводить по нему операцию, а также сообщать о таких фактах в компетентные органы.

ФАТФ рекомендует правительствам ужесточать требования в отношении национальных политических деятелей, которые могут представлять повышенный коррупционный риск в силу занимаемых ими постов. Такая обеспокоенность вызвана сохраняющейся угрозой предоставления финансовых услуг для передачи и экспорта ядерного, химического или биологического оружия, относящихся к ним материалов, а также средств его доставки.

Задача ФАТФ - стимулировать страны применять целенаправленные финансовые санкции, предусмотренные соответствующими резолюциями Совета Безопасности ООН. Это и замораживание активов, и предотвращение

передачи финансовых средств физическим и юридическим лицам, внесенным в санкционные списки Совета Безопасности. Речь идет о содействии всеобъемлющему выполнению поддержанных Россией и закрепленных в решениях совета требований международного сообщества. В соответствии с Уставом ООН они носят обязывающий характер. Распространение оружия массового уничтожения, как и терроризм, квалифицируется Советом Безопасности как угроза международному миру и безопасности.

Национальные компетентные органы смогут получать доступ к сведениям о бенефициарных собственниках того или иного бизнеса, компании или предприятия. А международный информационный обмен с ожидаемым ростом объема и качества передаваемых данных, направленный на выявление в ходе совместных финансовых расследований преступной деятельности, по отмыванию незаконно приобретенных доходов и финансированию терроризма, станет более прицельным.

ФАТФ рекомендовала странам подход, который позволяет фокусировать внимание на наиболее проблемных зонах в плане отмывания "грязных денег". Невысокому риску, по мнению экспертов, подвержены сферы рынка финансовых услуг, имеющие развитую систему регулирования и надзора. Традиционно к ним принято относить банковский сектор, который заинтересован в развитии безналичных расчетов, что создает условия для повышения прозрачности финансовых потоков. Доступность услуг, предлагаемых банками, развитие платежей с использованием банковских карт - способствуют снижению наличного оборота и рисков легализации незаконных доходов.

А к областям высокого риска относятся, как правило, новые виды финансовых услуг, которые предлагаются за пределами банковского сектора. Регулирование здесь отстает от стремительного развития отрасли. Речь идет о финансовых услугах, основанных на использовании новейших информационных технологий, - электронные деньги, предоплаченные карты, расчеты с использованием мобильной связи. Еще одним индикатором

повышенного риска для подобных услуг является их трансграничный характер в условиях отсутствия единых международных стандартов регулирования. В России эти тенденции учтены с принятием Закона о национальной платежной системе.

Несмотря на принятые меры, на сегодняшний день в теории и на практике остаются неразрешенными следующие вопросы, связанные с противодействием легализации доходов добытых преступным путем:

- не определено, что понимается под понятием "отмывание", его сущность и не проведено соотнесение с термином "легализация";
- четко не определены конкретные деяния, подпадающие под уголовно-правовую оценку;
- не разработаны четкие критерии для определения предмета преступления;
- не устранены сложности, возникающие в правоприменительной практике при установлении субъективной стороны преступления, в частности в вопросе указания на цель.

1.2 Дистанционное банковское обслуживание как сфера деятельности банка, сопряженная с противодействием отмывания денег

В то же время выяснилось, что технология дистанционного банковского обслуживания (ДБО) изначально придает отношениям между банком и клиентом своеобразную анонимность, поскольку фактически клиент работает с банком виртуально. К сожалению, следствием этого явились факты противоправного использования технологии ДБО для легализации доходов, полученных незаконным путем, совершения других экономических преступлений, а также для финансирования деятельности террористических организаций.

За последние 2–3 года в материалах зарубежных органов банковского надзора и в средствах массовой информации появился целый ряд публикаций по этой тематике. Для отмывания денег, как выясняется, по всему цивилизованному миру фактически используются технологии электронного банкинга с учетом предоставляемых ими анонимных возможностей. В последние 5–6 лет в зарубежных публикациях, относящихся к сфере финансового контроля, отмечается, что неизбежное отставание законодательной базы от практики, регулирующей новые интернет-технологии и финансово-технические, если можно так выразиться, инструменты, создает идеальные условия для их незаконного использования в целях отмывания денег. Этому способствует то обстоятельство, что многие электронные платежные инструменты отличаются предельно высокой скоростью транзакций, анонимностью, сочетаемостью с другими платежными системами, обеспечиваемой всемирными телекоммуникационными системами глобальностью и автоматизированностью, применением так называемых «безлюдных» технологий [13, с.166].

Перечисленные особенности снижают эффективность традиционных методов борьбы с отмыванием денег в виде требования предоставления банку определенной информации, отслеживания и анализа содержания операций, а также установления личности клиента и, на чем принято делать акцент в последнее время, выгодоприобретателя. Технология ДБО оказалась привлекательной для многих мошенников, так что кредитные организации, не обеспечивающие адекватного контроля за использованием систем ДБО, рискуют оказаться вовлеченными незаметно для самих себя в противоправную деятельность. Надо отметить, что во всем мире в борьбе с незаконным использованием автоматизированных систем предоставления финансовых услуг делаются попытки адаптации существующих методов и процедур к электронной торговле и платежным инструментам, например устанавливаются требования увеличения объема необходимых данных

(особенно при карточных операциях), обеспечения доступа к источникам клиентской информации, комплексного анализа ДБО через разные телекоммуникационные сети, а также совершенствуются методы проведения расследований, «интернационализируется» банковский контроль и т. д.

Очевидно, что проблемы противоправного использования кредитных организаций, например, в качестве «механизмов» отмывания денег не новы, и технологии ДБО лишь обеспечили новый «транспорт» для этого. Однако руководству кредитных организаций целесообразно адекватно учитывать новые факторы риска такого рода при внедрении и развитии ДБО.

В соответствии с письмом от 30.08.2006 №115-Т "Об исполнении ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" в части идентификации клиентов, обслуживаемых с использованием технологий дистанционного банковского обслуживания (включая Интернет-банкинг)" Банк России обязал финансовые институты при оказании таких услуг идентифицировать не только владельца счета, но и других лиц, которые будут пользоваться этим счетом.

При этом ответственность банка по данным вопросам регламентирована крайне жестко. Нарушение требований закона может повлечь применение к Банку ответственности, предусмотренной ФЗ от 10.07.2002 года №86-ФЗ "О Центральном банке Российской Федерации (Банке России)" (рекомендуемые меры воздействия предусмотрены Письмом Банка России от 13.07.2005 года №98-Т "О методических рекомендациях по применению Инструкции Банка России от 31.03.1997 № 59 "О применении к кредитным организациям мер воздействия при нарушениях кредитными организациями нормативных правовых актов в области противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма").

В условиях кризиса обостряется битва за клиента в любой сфере бизнеса. И кредитно-финансовые организации здесь не исключение. Жесткая

конкуренция приводит к необходимости улучшать обслуживание клиентов путём ввода новых видов услуг. Одним из направлений, способствующих предоставлению клиентам максимального удобства в их работе, является дистанционное банковское обслуживание, осуществляемое через сеть Интернет. Возможность полного управления своим личным счётом при условии простоты выполнения операций, комфорта и мобильности всегда привлекало и будет привлекать клиентов.

Однако наряду с удобствами, которые получает клиент, осуществление ДБО через Интернет становится причиной возникновения угроз нового типа. С одной стороны это связано с тем, что существенно возрастает доля рисков (угроз), контролировать которые силами финансовой организации практически невозможно, с другой стороны не меньшую долю рисков (угроз) приносят вопросы организации ДБО [20].

С одной стороны, предоставление коммерческим банком такой услуги как электронный банкинг, является инструментом привлечения клиентов, с другой - включает в себя и ряд специфических рисков. Главным преимуществом использования ДБО в целях легализации преступного капитала является то, что раньше клиент банка должен был прийти лично в банк для осуществления операций, а теперь клиент взаимодействует с коммерческим банком посредством сети Интернет.

Здесь тоже существуют свои сложности. Дело в том, что не все клиенты, использующие услуги ДБО являются мошенниками, а вовсе и наоборот, большинство из них законопослушные граждане, которые используют электронный банкинг для экономии времени при совершении банковских операций. Однако, фактически за последние годы количество преступлений, совершенных с использованием ДБО, выросло в несколько раз.

Следовательно, использование ДБО вызывает все большее внимание со стороны надзорных органов.

В настоящее время основными нормативными документами в данной сфере, разработанных Банком России, являются - Письмо Банка России от 05.04.2007 №44-Т «О проверке осуществления кредитными организациями идентификации клиента, обслуживаемых с использованием технологий дистанционного банковского обслуживания (включая интернет-банкинг)» и Письмо Банка России от 27.04.2007 №60-Т «Об особенностях обслуживания кредитными организациями клиентов с использованием дистанционного доступа к банковскому счету клиента (включая интернет-банкинг)».

В частности, в данных нормативных документах, даны рекомендации кредитным организациям по поводу включения в договор банковского счета ограничений использования услуг ДБО.

Кредитным организациям рекомендуется после предварительного предупреждения отказывать клиентам в приеме от них распоряжений на проведение операции по банковскому счету (вкладу), подписанных аналогом собственноручной подписи, в случае выявления сомнительных операций клиентов. При этом кредитным организациям рекомендуется принимать от таких клиентов только надлежащим образом оформленные расчетные документы на бумажном носителе.[2]

Кроме того, Банком России разработан еще один, по мнению автора, очень емкий по своему содержанию нормативный документ - Письмо Банка России от 31.03.2008 № 36-Т «О рекомендациях по организации управления рисками, возникающими при осуществлении кредитными организациями операций с применением систем интернет-банкинга». Данный документ может быть использован кредитной организацией при разработке правил работы с клиентами, использующими услуги ДБО.

Главным инструментом контроля за противоправным использованием систем электронного банкинга в кредитной организации является служба внутреннего контроля.

При выполнении своих задач служба внутреннего контроля в банке периодически проводит проверки по вопросам эффективности управления

банковскими рисками. При использовании кредитной организацией систем ДБО возникает потребность в расширении полномочий службы и, как следствие, перечня проверяемых вопросов.

Специфика новых распределенных технологий при выполнении банковских операций приводит к тому, что теперь необходимо говорить не просто о банковской деятельности и соответственно анализировать ее содержание посредством внутреннего контроля, а рассматривать так называемый информационный контур банковской деятельности (ИКБД), который реально формируется при каждом факте удаленного взаимодействия между неким клиентом и обслуживающей его кредитной организацией.[3]

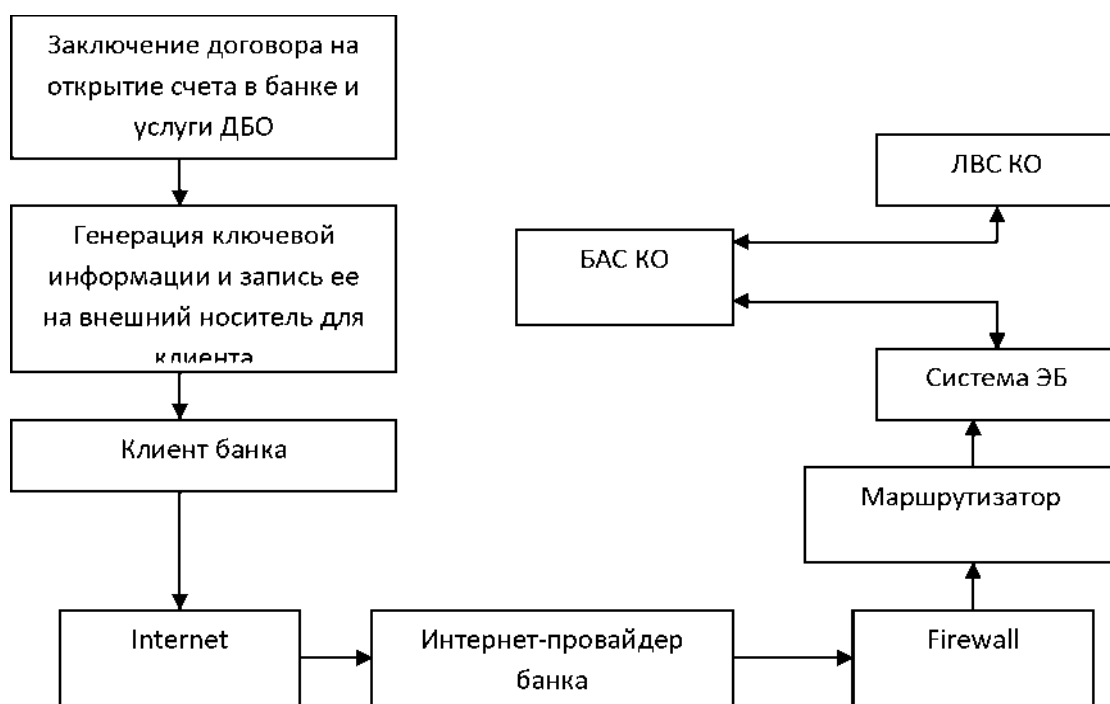


Рисунок 1.1 - Организация внутреннего контроля при использовании ДБО

ЛВС КО - локальная внутренняя сеть кредитной организации.

БАС КО - банковская автоматизированная система кредитной организацию.

Система ЭБ - система электронного банкинга.

Данный контур включает в себя реальные физические объекты, однако при осуществлении клиентом банковских операций с применением ДБО данные объекты становятся фактически виртуальными. Поэтому данные операции зачастую имеют непредсказуемый характер ввиду крупных масштабов сетевых систем, которые создаются множеством каналов связи, маршрутизаторов, компьютерных систем различных провайдеров, межсетевых шлюзов и других компонентов, ранее отсутствующих в ИКБД.

Стоит отметить, что на стадиях заключения договора на открытие счета в банке, генерации ключевой информации и записи ее на внешний носитель, работы провайдера-firewall-маршрутизатора сосредотачиваются наибольшие источники возникновения рисков [14, с.100].

Для сокращения риска на стадии «Заключение договора на открытие счета в банке и услуги ДБО» разрабатываются основные вопросы, которые могут входить в состав проверки систем ДБО, например:

- изучение уставных и финансовых документов клиента; рассмотрение деятельности клиента на рынке; анализ отзывов деловых партнеров;
- качество выпускаемой продукции или предоставляемых услуг; наличие квалифицированного персонала и т.д.

Для сокращения риска на стадии «Генерация ключевой информации и запись ее на внешний носитель для клиента» - следующие вопросы:

- наличие специально выделенного помещения для данного вида работ; наличие утвержденного руководством банка регламента выполнения данных работ и инструкции по выполнению;
- ответственные сотрудники, прошедшие соответствующее обучение и т.д. [4].

Процесс проверки экономической целесообразности операции, осуществленной клиентов посредством ДБО, затрагивает не только самого клиента, но и бенефициара, а также постоянное отслеживание сделок клиента. При идентификации бенефициара банком осуществляется проверка

собственника, которому будут переведены денежные средства, установить учредителей, если бенефициаром является юридическое лицо, и наличие аффилированности лиц.

Противодействие легализации преступного движения капитала - это всего лишь малая часть вопросов, относящихся к компетенции службы внутреннего контроля кредитной организации. Поэтому к сотрудниками указанного подразделения предъявляются жесткие требования, которые постоянно возрастают.

Именно поэтому для эффективной работы банка в процессе противодействия отмыванию денежных средств, в частности при использовании современных компьютерных технологий, наибольшее внимание необходимо уделять комплектованию квалифицированного кадрового состава службы внутреннего контроля банка и их постоянное обучение. От их опыта и квалификации фактически зависит обеспечение безопасности и репутации кредитной организации.

1.3 Инструментарий организационно-экономических основ противодействия отмывания денег

Одним из составляющих элементов противодействия отмыванию денег является анализ эффективности банковского обслуживания, в нашем случае в условиях ДБО. Говоря об оценке эффективности, обычно выделяют два направления: сравнение достигнутого и планируемого экономического эффекта (например, прибыль от использования системы за заданный период времени) и оценку текущей эффективности работы (стоимость обслуживания клиента, рентабельность и т.п.).

Оценить чистую прибыль от системы ДБО - задача весьма непростая, поскольку, как правило, основной доход эта система приносит косвенным образом. Прямой доход (плата за пользование системой) обычно

незначителен или вообще отсутствует, хотя это зависит от клиентской политики конкретного банка. Кроме того, подход к оценке эффективности по прибыли вообще неприемлем для систем ДБО, функционирующих в информационном режиме, т.е. предоставляющих клиентам бесплатные услуги. Выгодность внедрения таких систем обуславливается экономией на затратах других подразделений, но прибыли как таковой не приносит.

Более предпочтительными являются методы оценки эффективности текущей работы, выражающиеся в рентабельности затрат на обслуживание клиентов.

Совокупная стоимость владения при внедрении системы дистанционного обслуживания ТСОДБО, включает в себя как первоначальные инвестиции I , так и затраты на текущую работу $E_{мес}$ в течение периода оценки $T_{план}$:

$$ТСОДБО = I + E_{мес}T_{план} \quad (1.1)$$

Первоначальные инвестиции включают:

$$I = I_{ДБО} + I_{ПО} + I_{комп} + I_{связь} + I_{интегр} + I_{обуч}, \quad (1.2)$$

где: $I_{ДБО}$ - стоимость покупки программного обеспечения системы ДБО;

$I_{ПО}$ - стоимость покупки дополнительного к системе ДБО программного обеспечения: СУБД, веб-сервера, средств криптозащиты и т.п.;

$I_{комп}$ - стоимость приобретения аппаратного обеспечения (серверов, АРМ сотрудников поддержки и т.п.);

$I_{связь}$ - стоимость сетевой инфраструктуры (организация канала выхода в Интернет, стоимость сетевого оборудования и т.п.);

$I_{интегр}$ - стоимость проведения интеграционных работ по стыковке системы ДБО с информационными системами банка (включает в себя оплату

доработок системы ДБО, выполняемых поставщиком, и затраты на внедрение выполненных доработок в банковские информационные системы);

Иобуч - стоимость подбора и обучения персонала.

Ежемесячные затраты Емес включают:

$$I_{мес} = I_{поддержка} + I_{ДБО} + I_{интегр}, \quad (1.3)$$

где: Еподдержка - стоимость поддержки системы у поставщика;
ЕДБО - затраты на обеспечение работы ДБО (зарплата сотрудников, оплата каналов связи, косвенные затраты);

Еинтегр - затраты на обеспечение интеграции работы ДБО с информационными системами банка. Если была осуществлена так называемая online-интеграция системы ДБО с АБС банка, то Еинтегр= 0. В противном случае затраты на интеграцию складываются из затрат времени сотрудников банка на "ручное" проведение операций из системы ДБО в АБС банка.

В формуле подсчета ежемесячных затрат сознательно пропущено третье слагаемое - затраты банка на исполнение самой операции. Причины следующие:

стоимость проведения операции относится к себестоимости отдельного банковского продукта, а не к себестоимости обслуживания клиента в системе ДБО или при "классическом" обслуживании;

как правило, по каждому отдельному банковскому продукту вырабатывается такая тарифная политика, чтобы затраты на выполнение операции входили во взимаемую с клиента комиссию.

Рассмотрим пример самостоятельной разработки банком системы ДБО физических лиц. В этом случае в структуре первоначальных инвестиций исчезают затраты на приобретение ДБО, а из ежемесячных затрат - стоимость поддержки у поставщика. Однако затраты на персонал существенным образом меняются - необходимо оплачивать проектную команду программистов, тестировщиков, менеджера проекта и т.п. Кроме

того, запуск системы в эксплуатацию осуществляется только после значительного срока разработки, а не в течение 1-2 месяцев после покупки.

В свою очередь при открытии отделения банка:

$$TCO_{отд} = J + C_{отд} \cdot T_{план}, \quad (1.4)$$

где: J - размер первоначальных инвестиций;

$C_{отд}$ - ежемесячные затраты.

Анализ эффективности работы ДБО позволяет получить как общую характеристику деятельности банка, так и потенциальные возможности для отмывания денег.

Как известно, сфера деятельности, в полной мере охватывающая весь спектр основных преступлений, служащих источниками образования доходов, требующих отмывания ("грязных" денег), определяется понятием "теневая экономика". Любая форма экономической деятельности мотивирована получением прибыли. То же самое относится и к теневой экономической деятельности.

Более высокая норма прибыли, обеспечивающая удержание субъектов теневой экономики в "отрасли", предоставляет последним намного больше возможностей для ее распределения. Как показывает практика, доходы, полученные преступным путем, направляются не только на расширение преступной деятельности и вложения в недвижимость, драгоценности, автомобили, валютные ценности и проч., но и на инвестиции в различные сферы легальной финансово-хозяйственной деятельности.

Одним из мотивов подобного поведения является стремление владельцев таких средств реализовать принцип доходности своих сбережений, поскольку вложения в предметы роскоши не приносят дивидендов. Второй мотив заключается в желании скрыть реальные источники образования доходов, продолжая при этом получать новые, легальные доходы.

Безусловно, такая ситуация способствует усилению влияния преступных группировок на экономические отношения, постепенному сращиванию криминального и легального бизнеса, а также увеличению количества коррумпированных чиновников.

Таким образом, можно выделить следующие направления использования валового дохода от преступной экономической деятельности [9, с.182]:

- покрытие расходов, связанных с совершением преступления;
- покрытие расходов на личное потребление владельцев преступного бизнеса (приобретение предметов роскоши);
- дальнейшие инвестиции в сферу преступной деятельности с целью расширения и проникновения в новые сферы преступного бизнеса;
- портфельные и прямые инвестиции в легальную экономику;
- расходы на коррупцию, обеспечивающие прикрытие теневого бизнеса и проникновение в легальную экономику.

По оценкам швейцарского ученого К. Мюллера, после покрытия текущих расходов и расходов на потребление примерно 1/3 средств направляется на развитие преступного бизнеса, 1/3 размещается на международном финансовом рынке и 1/3 инвестируется в легальные предприятия [7].

В качестве основы для анализа системы источников "грязных" денег мы выбрали структуру теневой экономики, предложенную в методологии оценки теневой экономики согласно Системе национальных счетов, разработанной и рекомендованной Статистическим комитетом ООН в 1993 г.

Была построена модель, описывающая продуктивные виды экономической деятельности в зависимости от их принадлежности к теневой или легальной экономике. В результате мы получили пять условных секторов экономики, которые можно рассматривать как сферы образования доходов.

1) разрешенная уголовным законом деятельность, о которой субъекты, ее осуществляющие, в сроки и в порядке, которые предусмотрены

законодательством, отчитываются перед государственными органами и которая может быть дополнительно проверена в случае необходимости;

2) деятельность, разрешенная законом и осуществляемая субъектами хозяйствования официально, но размеры которой скрываются или приуменьшаются в целях уклонения от уплаты налогов и обязательных социальных платежей, выполнения других административных обязательств;

3) деятельность некорпорированных (принадлежащих одному владельцу, часто - семейных) предприятий, работающих для собственных нужд (производство товаров и услуг, произведенных в домашних хозяйствах и ими же потребленных), а также деятельность некорпорированных предприятий с неформальной занятостью (временные бригады строителей и т.п.);

4) запрещенная законом деятельность, направленная на производство и распространение товаров и услуг, на которые имеется рыночный спрос (производство и распространение наркотиков, проституция, контрабанда);

5) легальные виды деятельности, которыми занимаются нелегально (например, без лицензий и специальных разрешений).

Очевидно, что доходы, полученные в процессе деятельности в четвертом и пятом секторах построенной модели, в так называемой криминальной экономике, являются результатом совершения преступления.

В зависимости от степени общественной опасности и размера санкции конкретное преступление признается основным по отношению к отмыванию денег или не признается таковым. Данный подход связан с тем, что преследовать за отмывание денег, полученных в результате карманных краж или даже уличных разбоев, не имеет смысла ни с экономической, ни с профилактической точки зрения.

Также следует обратить внимание на второй сектор (скрытая экономика). Применительно к Российской Федерации это в основном налоговые преступления, которые, согласно УК РФ, вместе с уклонением от уплаты таможенных платежей и невозвратом валютной выручки не

рассматриваются как преступления, совершение которых требует соответствующего наказания. По нашему мнению, данная позиция российского законодателя не совсем верна, особенно в условиях российской действительности. В настоящее время данный вопрос остается дискуссионным и на международном уровне [5].

Полный перечень видов преступной деятельности нашел наиболее полное отражение в Сорока рекомендациях ФАТФ - Financial Action Task Force on Money Laundering. Эта межправительственная организация, созданная для выработки и реализации коллективных мер борьбы с отмыванием преступных доходов и финансированием терроризма, была учреждена в соответствии с решением саммита "большой семерки" в Париже в 1989 г. В настоящее время в ФАТФ входят 34 участника.

ФАТФ разработала в 1990 г. Сорок рекомендаций по борьбе с отмыванием денежных средств, которые были пересмотрены в 1996 и 2003 гг. с учетом развивающихся технологий отмывания доходов, и девять специальных рекомендаций по борьбе с финансированием терроризма в 2001 г., адаптированные к изменившейся политической ситуации в мире в октябре 2004 г. Эти документы признаны в качестве международных стандартов по противодействию отмыванию денег и финансированию терроризма.

Летом 2000 г. группа включила Россию в "черный список" стран, а 11 октября 2002 г. исключила ее из него.

Согласно Конвенции ООН против коррупции, принятой 31 октября 2003 г. Генеральной Ассамблеей ООН, каждое государство-участник должно рассмотреть вопрос об учреждении подразделения по финансовой оперативной информации, которое будет действовать в качестве национального центра для сбора, анализа и распространения информации, касающейся возможных случаев отмывания денежных средств.

ООН, описывая деятельность подразделений финансовой разведки, использует другой термин - "подразделения по финансовой оперативной информации". Таким образом, термины "подразделение финансовой

разведки", "орган финансового мониторинга" и "подразделения по финансовой оперативной информации" можно рассматривать в качестве синонимов.

Финансовый мониторинг является комплексным, составным понятием, поэтому, прежде чем определить его основное значение, постараемся выявить наиболее подходящие значения каждого из его составных элементов. Начнем с термина "мониторинг", поскольку именно он несет основную смысловую нагрузку, в то время как прилагательное "финансовый" имеет уточняющее значение.

В российской действительности термин "мониторинг" получил достаточно широкое распространение (мониторинг окружающей среды, мониторинг финансового состояния предприятия и т.д.). Например, Центральный банк РФ для собственных нужд проводит мониторинг предприятий, под которым понимается постоянное наблюдение за их деятельностью путем проведения опросов об изменении экономической конъюнктуры, инвестиционной активности, финансовом положении, а также систематизация и анализ полученной информации. Федеральная служба РФ по финансовому оздоровлению и банкротству также осуществляет мониторинг (систематический анализ) финансового состояния крупных экономически или социально значимых организаций.

Таким образом, понятие "финансовый мониторинг" логичнее рассматривать во взаимосвязи с полномочиями Федеральной службы по финансовому мониторингу (ФСФМ России). Во-первых, уже существует и научно признана категория финансового контроля, во-вторых, как уже было сказано, на практике содержание понятия "мониторинг", в том числе и финансовый, во многом определяется сферой его применения. Исходя из этого, под финансовым мониторингом в сфере противодействия отмыванию денег следует понимать выборочное наблюдение и контроль за финансовыми потоками между хозяйствующими субъектами.

В настоящее время сложилось три модели организации постоянного мониторинга сделок и операций [22, с.178]:

- система контроля, предусматривающая обязательное сообщение в центральное правительственное агентство обо всех сделках, превышающих определенную сумму наличными или их эквивалента;

- система контроля, предусматривающая сообщение о подозрительных сделках, требующая, чтобы банки учитывали некоторые или все крупные валютные сделки, но сообщали властям о тех из них, которые вызывают подозрение;

- система контроля, предусматривающая запрет крупных сделок с наличными, минуя законного финансового посредника. Так, итальянский закон не требует, чтобы каждый бизнесмен или профессионал вел учет и сообщал о крупных сделках с наличными, но запрещает такие сделки, если они не осуществляются через законного финансового посредника, обязанного вести учет и подлежащего контролю. Единственным возражением против подобного подхода было заявление Европейского союза, считающего, что такая практика препятствует свободному движению капитала в его рамках.

Одним из преимуществ первой модели является то, что она не зависит от определения того, какая сделка подозрительна, а какая нет.

Критерии подозрительности могут быть источником трений между властями и банкирами, поэтому необходим закон, определяющий, о чем их служащие должны сообщать.

Вместе с тем существует опасность того, что при определении перечня подозрительных обстоятельств банкиры будут сообщать только о них и не более того.

Другая проблема, касающаяся сообщений о подозрительных сделках, заключается в том, что некоторые страны требуют сообщать только о сделках, в которых могут присутствовать наркодоходы, не принимая во внимание доходы от других видов преступной деятельности. Такие законы

ставят своеобразную дилемму перед банковскими кругами, так как служащему или менеджеру банка практически невозможно определить происхождение крупных сумм наличных денег у клиента, не имеющего законных источников дохода, и квалифицировать их как доход от продажи наркотиков или от других видов преступной деятельности.

Существуют также сложности в обеспечении эффективного контроля над небанковскими финансовыми институтами. Так, если банки изначально были регулируемы организациями, в частности, на них распространялись законы о валютном регулировании, то введение дополнительных требований по учету и сбору информации об отдельных операциях клиентов было относительно легко осуществимо. В то же время против применения аналогичных требований к небанковским финансовым учреждениям, таким как пункты обмена валют и лицензированные игорные заведения, высказываются законодатели ряда стран и представители соответствующих профессий.

Многих из отмеченных недостатков лишена третья система контроля.

Первая и третья модели системы контроля применяются в США, Австралии и Италии, в то время как все остальные государства используют шаблон, предложенный международными организациями.

Таким образом, задача подразделения финансовой разведки сводится к разработке и внедрению в использование первичными субъектами финансового мониторинга собственного механизма мониторинга сделок и операций, который учитывал бы национальную специфику [16].

В Российской Федерации система уполномоченных органов и организаций в сфере финансового мониторинга представляет собой трехуровневую структуру.

Первый уровень занимает ФСФМ России (Росфинмониторинг) как уполномоченный федеральный орган исполнительной власти РФ, который обеспечивает накопление и анализ информации, поступающей от третьего

уровня, и осуществляет выявление признаков легализации незаконных доходов.

Второй уровень - надзорные органы, осуществляющие надзорные функции в отношении ряда субъектов финансового мониторинга. В настоящее время к таким надзорным органам следует отнести Банк России, Федеральную службу по надзору в сфере связи и массовых коммуникаций, Государственную пробирную палату.

И наконец, третий уровень занимают организации, осуществляющие операции с денежными средствами или иным имуществом, а именно субъекты финансового мониторинга, к которым относятся:

- кредитные организации;
- профессиональные участники рынка ценных бумаг;
- страховые организации и лизинговые компании;
- организации федеральной почтовой связи;
- ломбарды;
- организации, осуществляющие скупку, куплю-продажу драгоценных металлов и драгоценных камней, ювелирных изделий из них и лома таких изделий;
- организации, содержащие тотализаторы и букмекерские конторы, а также организующие и проводящие лотереи, тотализаторы (взаимное пари) и иные основанные на риске игры, в том числе в электронной форме;
- организации, осуществляющие управление инвестиционными фондами или негосударственными пенсионными фондами;
- организации, оказывающие посреднические услуги при осуществлении сделок купли-продажи недвижимого имущества;
- организации, не являющиеся кредитными организациями, осуществляющие прием от физических лиц наличных денежных средств в случаях, предусмотренных законодательством о банках и банковской деятельности;

- коммерческие организации, заключающие договоры финансирования под уступку денежного требования в качестве финансовых агентов (факторинговые компании);

- адвокаты;

- нотариусы;

- лица, осуществляющие предпринимательскую деятельность в сфере оказания юридических и бухгалтерских услуг.

Как уже было отмечено выше, контроль за исполнением требований законодательства в сфере ПОД/ФТ осуществляют соответствующие надзорные органы в соответствии с их компетенцией [19]:

- Банк России - за кредитными организациями;

- Федеральная служба по финансовым рынкам - за профессиональными участниками рынка ценных бумаг и организациями, осуществляющими управление инвестиционными фондами и негосударственными пенсионными фондами, а также за страховыми организациями;

- органы пробирного надзора - за организациями, осуществляющими скупку, куплю-продажу драгоценных металлов и драгоценных камней, ювелирных изделий из них и лома таких изделий;

- Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций - за организациями федеральной почтовой связи.

В случае отсутствия надзорных органов в сфере деятельности отдельных организаций контроль осуществляется Росфинмониторингом.

Одной из важнейших задач Росфинмониторинга является осуществление контроля и надзора за выполнением юридическими и физическими лицами требований законодательства Российской Федерации о ПОД/ФТ. Основными направлениями надзорной деятельности Федеральной службы по финансовому мониторингу являются следующие:

- координация деятельности надзорных органов и взаимодействие с ними в области ПОД/ФТ;

- проведение проверок организаций, осуществляющих операции с денежными средствами или иным имуществом, в сфере деятельности которых отсутствуют надзорные органы, в целях профилактики и предупреждения правонарушений в сфере ПОД/ФТ;

- взаимодействие с федеральными органами исполнительной власти, органами прокуратуры, органами исполнительной власти субъектов Российской Федерации, общественными объединениями и иными организациями по вопросам ПОД/ФТ.

К основным формам надзора, осуществляемым Росфинмониторингом и надзорными органами можно отнести:

- документарный (текущий) надзор с акцентом на реализацию проактивной функции надзора, основанной на использовании информационных и аналитических систем мониторинга текущего состояния организаций, соблюдения ими законодательства и регулятивных требований в области ПОД/ФТ для выявления на возможно более ранних стадиях негативных тенденций в деятельности организаций по ПОД/ФТ;

- инспекционные проверки организаций, основанные на данных документарного надзора, а также подготовленных надзорными органами и периодически обновляемых ими методологических рекомендациях.

Надзорная деятельность в области ПОД/ФТ осуществляется по следующим основным направлениям:

- проверка организации внутреннего контроля по соблюдению законодательства Российской Федерации и нормативных актов надзорных органов в области ПОД/ФТ;

- проверка соответствия фактической деятельности организаций положениям законодательства Российской Федерации и нормативных актов надзорных органов в области ПОД/ФТ;

- проверка соответствия фактической деятельности организаций собственным правилам внутреннего контроля в целях ПОД/ФТ и программам его осуществления.

В соответствии с Административным регламентом исполнения Федеральной службой по финансовому мониторингу и ее территориальными органами государственной функции по осуществлению контроля и надзора за выполнением юридическими и физическими лицами требований законодательства РФ о ПОД/ФТ и привлечению к ответственности лиц, допустивших нарушение этого законодательства, утвержденным Приказом Росфинмониторинга от 24 мая 2010 года N 129, исполнение государственной функции включает в себя следующие административные процедуры:

- проведение проверки;
- производство по делу об административном правонарушении.

Росфинмониторингом и его территориальными органами могут проводиться следующие виды проверок:

- по месту нахождения проверяемой организации или ее филиала (выездная проверка);
- по месту нахождения Росфинмониторинга, его территориальных органов (камеральная проверка);
- в рамках производства по делам об административных правонарушениях.

По фактам нарушений законодательства о ПОД/ФТ виновные лица привлекаются к административной ответственности по ст. 15.27 Кодекса Российской Федерации об административных правонарушениях.

Кроме организационных, можно выделить экономические инструменты противодействия отмыванию денег. К таким можно отнести:

- 1) Общее улучшение экономической обстановки.

Предполагается, что повышение инвестиционной привлекательности российских активов не только привлечет иностранные инвестиции, но и снизит стимулы к оттоку российского капитала. Это, однако, верно лишь отчасти, причем в основном в отношении лишь легального вывоза. Как уже отмечалось, при нелегальном вывозе чаще всего основные стимулы - не столько поиск возможности наиболее эффективных вложений, сколько

стремление вывести средства из зоны политического и экономического риска, а также нередко из-под налогообложения и (или) из-под контроля акционеров. Вернуть же при необходимости вывезенные средства в Россию не составляет труда.

2) Экономические меры противодействия вывозу.

Имеются в виду прежде всего обеспечительные меры против нарушения валютного законодательства, такие как требование депонирования определенных сумм, которые возвращаются владельцам только после успешного завершения валютной операции. В настоящее время применяется депонирование 20% суммы предоплаты при импорте: если оплаченный товар на самом деле не ввозится (фиктивный контракт), депозит не возвращается.

Сходная идеология нашла широкое применение в законе о валютном регулировании: существующая разрешительная система в отношении капитальных валютных операций отменяется, но зато по ряду операций вводится обязательное резервирование средств в размере определенного процента от суммы операции на тот или иной срок. Данная мера эффективна прежде всего для борьбы с легальным оттоком капитала; она позволяет смягчить эффект возможных кризисных ситуаций, противодействуя паническому оттоку капитала.

Можно сделать вывод, что Развитие систем электронных денег чревато опаснейшими последствиями с точки зрения отмывания денег. Так, некоторые из используемых сейчас способов регистрации совершенных операций в действующих системах электронных денег позволяют переводить крупные суммы, практически не оставляя следов ни на бумаге, ни в центральном компьютере (сервере) системы. Это особенно характерно для систем многосторонних расчетов и платежей с многочисленными участниками, территориально удаленными друг от друга.

Оборачиваясь в виртуальной среде, эти деньги не оставляют следов, которые можно было бы использовать для последующего контроля.

В настоящее время все применяемые меры контроля над такими операциями основаны на использовании регистрации переводимых сумм и реквизитов получателей банками и другими финансовыми учреждениями. При осуществлении многозвенных расчетов такие записи не позволяют понять и проанализировать действительные аспекты и сущность совершенной операции.

Надзорные органы обеспокоены системами электронных денег, где электронные деньги оборачиваются в виртуальной среде, не оставляя следов, по которым можно было бы осуществить контроль.

С экономической точки зрения для борьбы с отмыванием денег в условиях ДБО надо обеспечить выгодные условия инвестиций внутри страны, причем условия даже более выгодные, нежели инвестиции в любых других странах мирового сообщества, принципиальные предпосылки для этого, как известно, в нашей стране имеются.

Исходя из вышеизложенного, для сокращения масштабов легализации (отмывания) денег необходимо:

- 1) сформировать благоприятную макроэкономическую обстановку в стране, побуждающую к инвестированию в рамках Российской Федерации, и проводить эффективную инвестиционную и инновационную политику.

- 2) совершенствовать законодательную базу, направленную на идентификацию форм вывоза капитала, которые наносят прямой ущерб государству и противоречат интересам развития национальной экономики, а также ввести четкое и жесткое регулирование вывоза капитала за счет принятия комплекса нормативных актов, заполняющих правовой вакуум в некоторых аспектах внешнеэкономической деятельности;

- 3) создать надежную систему таможенного и финансового контроля, включая комплекс валютного контроля международных расчетов, усилить ответственность за использование нелегальных и полунелегальных схем бегства капитала.

Касательно противодействия отмыванию денег в условиях дистанционного банковского обслуживания следует отслеживать и оценивать следующие показатели и факторы:

- осуществление операций на значительно большие суммы, чем можно было бы ожидать в обычном случае, учитывая характер деятельности владельца счета;
- документация, которая представляется в обеспечение сделки (при отмывании денег документация зачастую оказывается подложной или имеет существенные изъяны с правовой точки зрения);
- коммерческое предприятие, которому принадлежит счет, оформлено в качестве юридического лица или зарегистрировано в регистрационной палате на весьма ограниченный период времени;
- обе стороны сделки фактически являются одним и тем же лицом.
- рост объемов денежных переводов, не сопровождаемый соответственным ростом числа счетов.
- хранимая наличность нередко превышает пределы, установленные программой безопасности и (или) общим порядком покрытия обязательств.
- счета с большим количеством небольших вкладов и небольшим числом крупных чеков, по которым остаток на счете сохраняется относительно малым и постоянным. Такой счет имеет много общих характеристик со счетом, используемым для выписывания фиктивных счетов до инкассации.
- крупный объем вкладов на несколько различных счетов с частым переводом основной части остатка на этих счетах на один и тот же счет в том же банке или в другом банке.
- большие объемы кассирских чеков или платежных поручений депонируются на счет, когда род деловых занятий владельца счета, как представляется, не соответствует подобным действиям.
- крупные объемы вкладов наличностью от делового предприятия, которое обычно не отличается интенсивностью операций с наличностью.

Таким образом, следует обращать внимание на нехарактерные для клиента операции, а также на операции, которые потенциально могут преследовать цель отмывания денег.

2 Анализ состояния противодействия отмывания денег в дистанционном банковском обслуживании (ДБО)

2.1 Организационно-экономическая характеристика банка

Объект исследования - ПАО «Сбербанк России». Сбербанк — российский коммерческий банк, международная финансовая группа, один из крупнейших банков России и Европы. Полное наименование — публичное акционерное общество «Сбербанк России».

Сбербанк — универсальный банк, предоставляющий широкий спектр банковских услуг. Доля Сбербанка в общем объеме активов российского банковского сектора составляла на 1 января 2016 года 28,7 %; на рынке частных вкладов — 46 %; кредитный портфель соответствовал 38,7 % всех выданных кредитов населению.

Сбербанк России обладает самой широкой филиальной сетью: в настоящее время в нее входят 17 территориальных банков и около 19 тысяч подразделений по всей стране. Дочерние банки Сбербанка России работают в Казахстане, на Украине и в Беларуси. В соответствии со Стратегией развития, Сбербанк России расширил свое международное присутствие, открыв представительство в Германии и филиал в Индии, а также зарегистрировав представительство в Китае. В конце 2011 Сбербанк закрыл сделку по приобретению SLB Commercial Bank AG, переименованного в Sberbank (Switzerland) AG. В январе 2012 банк завершил сделку по приобретению «Тройки Диалог», крупнейшей российской инвестиционной компании. После приобретения Volksbank International в структуру Сбербанка вошли подразделения в 9 странах Центральной и Восточной

Европы. В августе Сбербанк создал совместный банк на рынке кредитования в точках продаж с Cetelem (Группа BNP Paribas). В сентябре 2012 года Сбербанк приобрел 99,85% акций банка DenizBank. Эта эпохальная сделка стала крупнейшим приобретением за 170-тилетнюю историю банка.

Филиалы Банка (территориальные банки, отделения) не наделены правами юридических лиц и действуют на основании Положений, утверждаемых Правлением Банка, имеют печать с изображением эмблемы Банка со своим наименованием, а также другие печати и штампы, имеют баланс, который входит в баланс банка. Филиальная сеть Сбербанка России представлена 17 территориальными Банками, расположенные на всей территории Российской Федерации (рисунок 2.1).

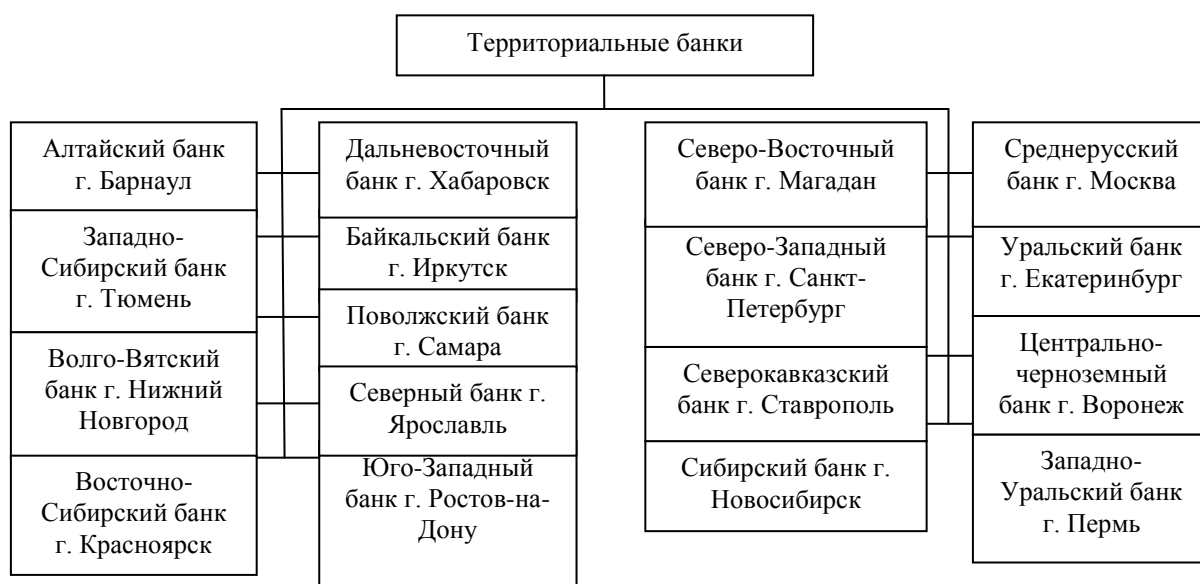


Рисунок 2.1 - Филиальная сеть Сбербанка России

Сбербанк продолжил работу по улучшению качества клиентского сервиса. Наиболее значимой услугой Сбербанка остается прием платежей населения. Их объем за год превысил 1,8 трлн руб., общее количество принятых платежей почти достигло 1 млрд. Доля платежей, принятых по биллинговой технологии, превысила 74% в общем объеме принятых Банком платежей.

Организационная структура Сбербанка России представлена на рисунке 2.2.

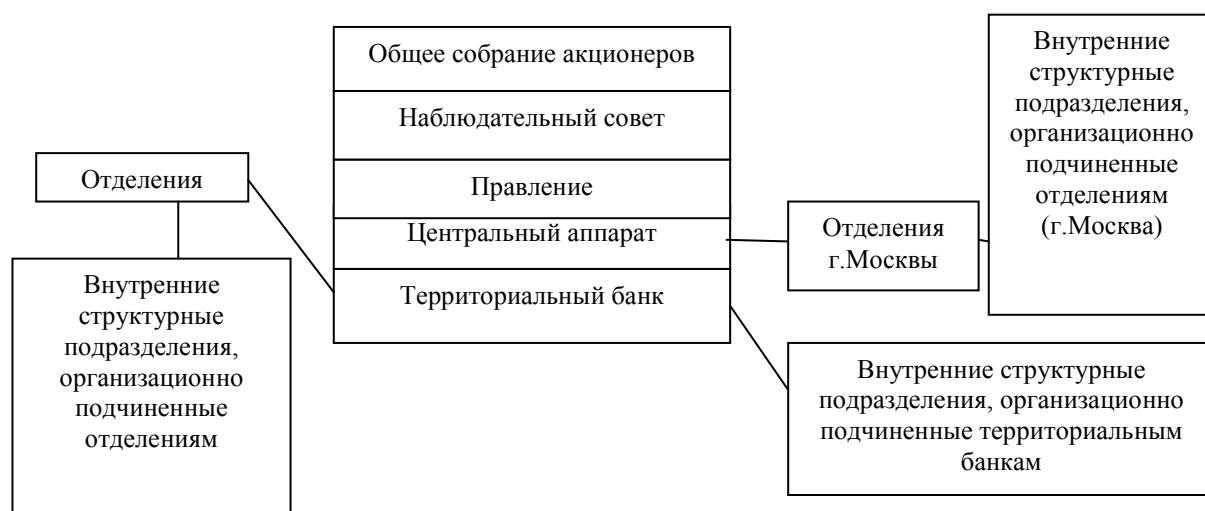


Рисунок 2.2 - Организационная структура Сбербанка России

На конец 2015 года банк имел 117 структурных подразделений по всей стране, в том числе 16 филиалов. Его клиентская база состоит из 50 тыс. юридических и 1 019 тыс. физических лиц. Сеть устройств самообслуживания банка насчитывает 6,7 тыс. банкоматов, устройств самообслуживания и POS-терминалов. Ссудный портфель (брутто) за 2015 год вырос на 8,6%. Объем привлеченных средств клиентов за отчетный год вырос на 37,6%.

В 2015 году Банк запустил новый розничный продукт на рынке Казахстана – продажу золотых слитков.

В 2014 году из-за падения цен на нефть, закрывшихся рынков капитала, роста геополитической напряженности, накопленных структурных диспропорций российская экономика перешла в фазу рецессии, которая еще больше усилилась в 2015 году.

Макроэкономические изменения не могли не сказаться на банковских рынках, которые быстро отреагировали на кризис острой нехваткой ликвидности, а также ростом процентных ставок и уровня кредитного риска.

К данному кризису группа компаний ПАО Сбербанк оказались готовы лучше, чем к кризису 2009 года. В явном виде это проявилось в конце 2014 года, когда все наши системы и команда подверглись беспрецедентным нагрузкам в момент шока процентных ставок и кризиса ликвидности. Можно отметить, что Сбербанк обслуживал клиентов без единого сбоя, все ИТ-системы выдержали, а наиболее проблемный декабрь 2014 года банк завершил с прибылью и притоком средств клиентов.

За весь кризисный период 2014-2015 годов группа компаний ПАО Сбербанк ни разу не обратилась за докапитализацией к Банку России - собственные ресурсы позволяли эффективно работать даже в тяжелейших условиях острой фазы кризиса. Более того, за 2015 год удалось вернуть почти 3 трлн. рублей средств Банка России и Федерального казначейства, снизив их долю в обязательствах банка с 16 до 1 % и тем самым практически ликвидировав зависимость финансового результата от процентной политики Банка России.

Несмотря на кризис Сбербанк не остановил ни одного проекта и продолжает реализовывать все стратегические инициативы, необходимые для обеспечения долгосрочной жизнедеятельности и конкурентоспособности.

Высокими темпами развивались удаленные каналы, выросло качество клиентского обслуживания, что отразилось в динамике показателя NPS (англ. Net Promoter Score - индекс готовности рекомендовать) для розничных клиентов и индекса лояльности для корпоративных клиентов.

Увеличено количество корпоративных клиентов на 245 000.

Группа компаний ПАО Сбербанк обеспечила повышение уровня надежности ИТ-услуг банка (до 99,97%), завершена программа централизации ИТ. В 2015 году был дан старт реализации нескольких новых крупных ИТ-программ, достигнуты положительные результаты в развитии системы управления рисками и управлении операционными расходами.

Все это позволило обеспечить достойный финансовый результат даже в непростых экономических условиях. Чистая прибыль по международным

стандартам финансовой отчетности (МСФО) за 2015 год составила 222,9 млрд.рублей.

Финансовые показатели группа компаний ПАО Сбербанк представлена в таблице 2.1.

Таблица 2.1 - Финансовые показатели группа компаний ПАО Сбербанк в динамике 2011-2015 гг., %

Показатели	2011	2012	2013	2014	2015	темпы роста, %
Активы	26,8	27,1	29,6	29,1	30,2	112,69
Кредиты корпоративным клиентам	32,9	33,6	33,3	35	32,2	97,87
Кредиты частным клиентам	32	32,7	33,5	35,9	38,7	120,94
Средства корпоративных клиентов	17	17,2	17,2	21,9	25	147,06
Средства частных клиентов	46,6	45,7	46,7	45	46	98,71

Данные таблицы отражают тот факт, что за исследуемый период активы банка, не смотря на кризисный период выросли на 12,69%. Значительный рост показало кредитование частных клиентов (20,94%). Высокие показатели характерны для роста средств корпоративных клиентов (на 47,06%). Средства частных клиентов не значительно снизились (на 1,29%). Кредиты корпоративным клиентам тоже уменьшились (на 2,13%).

Характеризуя деятельность банка, необходимо отметить, что главными драйверами роста непроцентных доходов в розничном бизнесе за последние несколько лет являются операции с банковскими картами, эквайринг, платежи и переводы (табл.2.2).

Таблица 2.2 – Количество банковских карт банка

млн.штук

Показатели	2011	2012	2013	2014	2015	темпы роста,%
Дебетовые карты	69,88	78,6	87,5	96,2	102,3	146,39
Кредитные карты	10,12	11,15	12,8	14,6	15,6	154,15
Итого действующих карт Сбербанка	80	89,75	100,3	110,8	117,9	147,38

Рост эмиссии банковских карт продолжает ускорять рост объемов операций по карточным счетам. Количество дебетовых карт за период выросло на 46,39%, а рост кредитных карт составил 54,15%. Банк объявлен победителем в номинации Лучший банк по субсидированию в рамках Программы «Дорожная карта бизнеса 2020», назван победителем в номинации «Лучший продукт с гарантией», а также вошел в число лидеров по итогам акции «Успех гарантирован!», организованной Фондом развития предпринимательства «Даму». Мобильное приложение «Сбербанк Онлайн» признано лучшим мобильным приложением Казахстана в категории «Дизайн и Юзабилити» на IV международной конференции MobiEvent'15.

Анализ статей баланса и отчета о финансовых результатах за 2015 год относительно 2014 года характеризуется следующим:

- процентный доход увеличился на 21,3%, процентные расходы увеличились на 59,5%; чистый процентный доход снизился на 11,1%;
- комиссионный доход, не связанный с кредитованием, увеличился на 17,0%, чистый комиссионный доход увеличился на 4,4%;
- операционный доход до совокупных резервов снизился на 9,2%;
- расходы на создание совокупных резервов составили 397,6 млрд.рублей против 397,9 млрд.рублей годом ранее;
- операционные расходы снизились на 1,0%;
- прибыль до уплаты налога на прибыль составила 283,9 млрд.рублей против 394,6 млрд.рублей годом ранее (рисунок 2.3).
- чистая прибыль составила 222,9 млрд.рублей без учета событий после отчетной даты против 290,3 млрд.рублей с учетом событий после отчетной даты годом ранее.

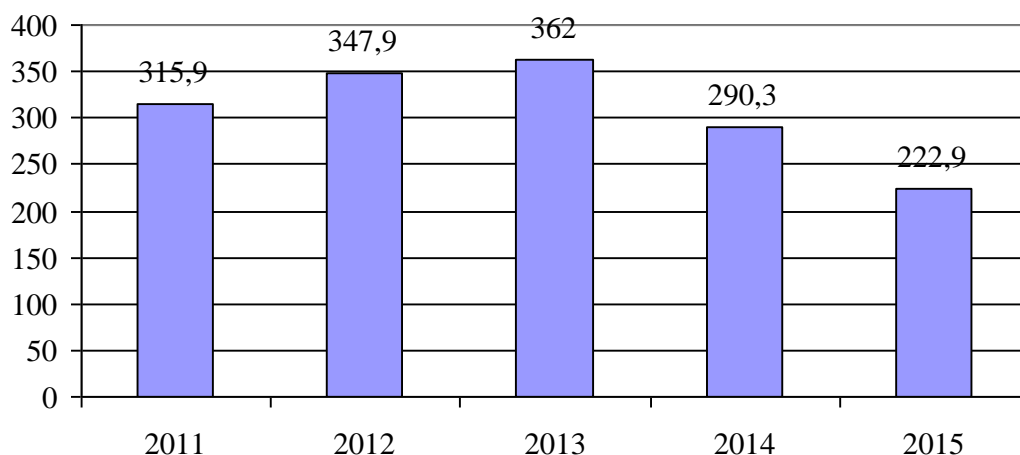


Рисунок 2.3 – Чистая прибыль банка, млрд. руб.

Динамика прибыли банка отражает кризисные явления 2014-2015 года. Темпы роста прибыли, которые наблюдались до 2013 года снизились, прибыль значительно уменьшилась.

Тем не менее, собственные средства компании выросли. Динамика этого показателя представлена на рисунке 2.4

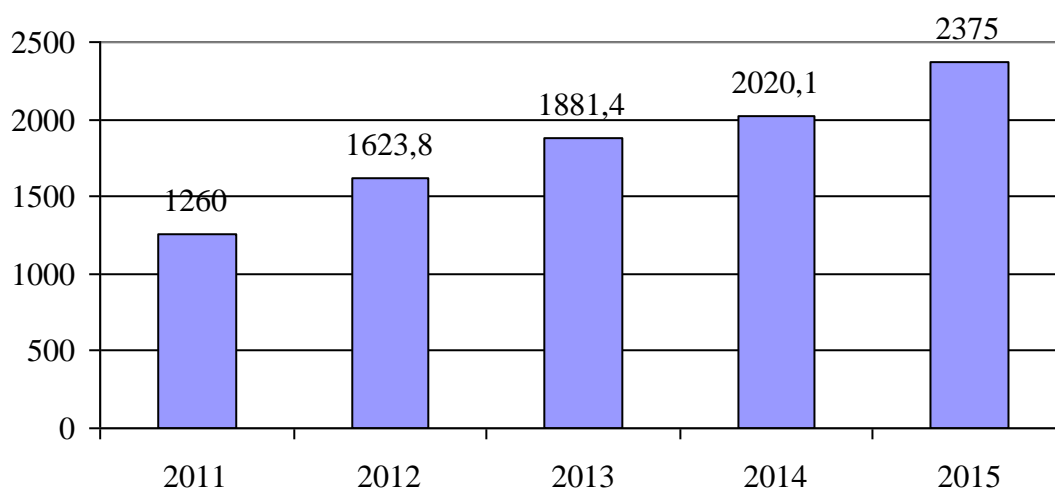


Рисунок 2.4 – Динамика собственных средств банка

Несколько факторов повлияли на рост собственных средств, в том числе, положительная динамика показателей, представленная в таблице 2.3.

Таблица 2.3 – Количественные показатели деятельности ОАО «Сбербанк»

Показатели	2013	2014	2015	темпы роста, %
------------	------	------	------	----------------

Общее количество поставщиков, привлеченных организацией. ед.	1323	1798	39295	2970,14
Общая сумма платежей, направленная поставщикам, тыс. рублей	66798455	92582343	183025498	274,00
в том числе местным поставщикам, тыс. рублей	62257485	87869310	176212669	283,04
Доля местных поставщиков в закупочном бюджете. %	93	95	96	103,23
в том числе представителям малого и среднего бизнеса, тыс. рублей	18677693	30312385	72119537	386,13
Доля малого и среднего бизнеса в закупочном бюджете, %	28	33	39	139,29

Можно говорить, по данным таблицы, что количество предприятий, которые привлекает ПАО «Сбербанк» растет очень быстрыми темпами. При этом, в 2015 году почти в 4 раза увеличилось число представителей малого и среднего бизнеса. Доля местных поставщиков финансовых ресурсов постоянно растет и приближается к 100 %. Роста за исследуемый период составил 3,23%. Данные таблицы показывают, что в банке за 2013-2015 годы расширилась сеть устройств самообслуживания с новым программным обеспечением, которое предоставляет клиентам единое пространство для выполнения операций. В этих устройствах (более 53 тыс. штук) клиент видит свои операции, проведенные в интернет-банке «Сбербанк Онлайн», может распечатать по ним чек-подтверждение и повторить платеж по созданному ранее в интернет-банке шаблону. Показатель технической доступности устройств для клиентов повысился с 93.2 до 95.1 %. В 2015 завершена программа централизации ИТ-систем, которую в течение четырех лет реализовывала команда из 32 тыс. человек. В итоге создана одна из крупнейших в мире единая централизованная ИТ-платформа, которая позволила повысить эффективность и надежность бизнес-процессов. Реализация этого проекта создала фундамент для появления принципиально новых технологических решений для удержания конкурентоспособности в будущем. Структура системы дистанционного обслуживания представлена на рисунке



Рисунок 2.5 – Система дистанционного обслуживания ПАО «Сбербанк»

На рисунке представлено:

- Сбербанк Бизнес Онлайн. Это система дистанционного банковского обслуживания, предоставляющая возможность посредством стандартного интернет-браузера подготавливать и отправлять платежные документы, а также совершать другие операции.
- Мобильное приложение “Сбербанк Бизнес Онлайн”
- Мобильное приложение “Сбербанк Бизнес Онлайн” для юридических лиц и предпринимателей - планирование, контроль, управление финансами вашей компании в одно касание.
- E-invoicing. Это универсальная система электронного документооборота, с помощью которой Вы можете решать бизнес-задачи вне зависимости от расстояния между контрагентами, масштабов бизнеса и вида деятельности.
- Сбербанк Бизнес. АС Сбербанк Бизнес – это система дистанционного банковского обслуживания на основе приложения, устанавливаемого на стороне клиента.

Итак, рассмотрена положительная динамика дистанционного обслуживания, которая приводит к изучению состояния дистанционного банковского обслуживания. Поэтому в следующем разделе мы исследуем влияния рисков на финансовые результаты деятельности банка.

2.2 Оценка финансовых результатов и факторов снижающих эффективность ДБО с учетом противодействия отмывания денег

Информационные технологии сопровождают все направления нашего бизнеса.

В целях совершенствования дистанционного банковского обслуживания в 2015 году в Сбербанке предприняты следующие действия:

- создана полная актуальная эталонная база клиентов Сбербанка по всем сегментам розничного бизнеса за счет подключения систем территориальных банков к системе единого профиля клиента в режиме онлайн;
- запущено СМС-информирование клиентов о статусе выпуска и доставки карт. Клиент теперь может получить карту в любом регионе присутствия Сбербанка вне зависимости от места ведения его счета;
- управление персоналом Сбербанка ведется в единой системе SAP HR. Это крупнейший в мире проект по внедрению SAP HR, который охватывает 11 часовых поясов, 230 тыс. табельных номеров в 82 субъектах страны, 89 разрозненных исторических систем выведены из эксплуатации;
- внедрен автоматизированный процесс оценки кредитной истории в технологиях «Кредитный конвейер» и «Кредитная фабрика» для клиентских сегментов «Микро Бизнес» и «Малый Бизнес»;
- в 6 тысячах отделений Сбербанка по всей стране организована сеть Wi-Fi для сотрудников и клиентов. Более 10 тысяч сотрудников этих отделений используют корпоративные планшеты для обслуживания клиентов и подключения им продуктов и услуг ПАО Сбербанк.

Новая версия корпоративного портала объединила все территориальные банки группы компаний Сбербанка на одной площадке -до этого момента существовало 15 разрозненных порталов. В МегаЦОД

Сбербанка создан центр обработки данных для Sberbank Europe AG. Это первый проект в России по ИТ-сопровождению европейских банков, который сэкономил дочерним банкам около 50 млн евро на стоимости сопровождения ИТ.

Таблица 2.4 – Развитие каналов дистанционного банковского обслуживания в группе компаний Сбербанка,

тыс.активных пользователей

Услуга	2013	2014	2015	Изменение за отчетный период, %
Мобильный банк. тыс. активных пользователей, в том числе:	11760	21240	27283	28
Сбербанк	14658	20918	26809	28
Дочерние банки	102		474	47
Онлайн банкинг, тыс. активных пользователей, в том числе:	10120	20359	30438	50
Сбербанк	9441	19386	29236	01
Дочерние банки	679	973	1202	24
Количество банкоматов, в том числе:	93067	94289	90444	-4
Сбербанк	89016	90059	85914	_5
Дочерние банки	4051	4230	4530	7

Данные таблицы 2.4 отражают тот факт, что количество операций, производимых через удаленные банковские каналы, растет высокими темпами: в 2015 году количество активных пользователей онлайн банкинга по Группе увеличилось на 50 %. а мобильного банка - на 28 %.

В тоже время незначительно снизилось количество банкоматов, что обусловлено улучшением качества он-лайн сервисов и соответственно ростом популярности безналичного способа оплаты.

На рисунке 2.6 представлена характеристика показателей дистанционного банковского обслуживания в ОАО «Сбербанк».

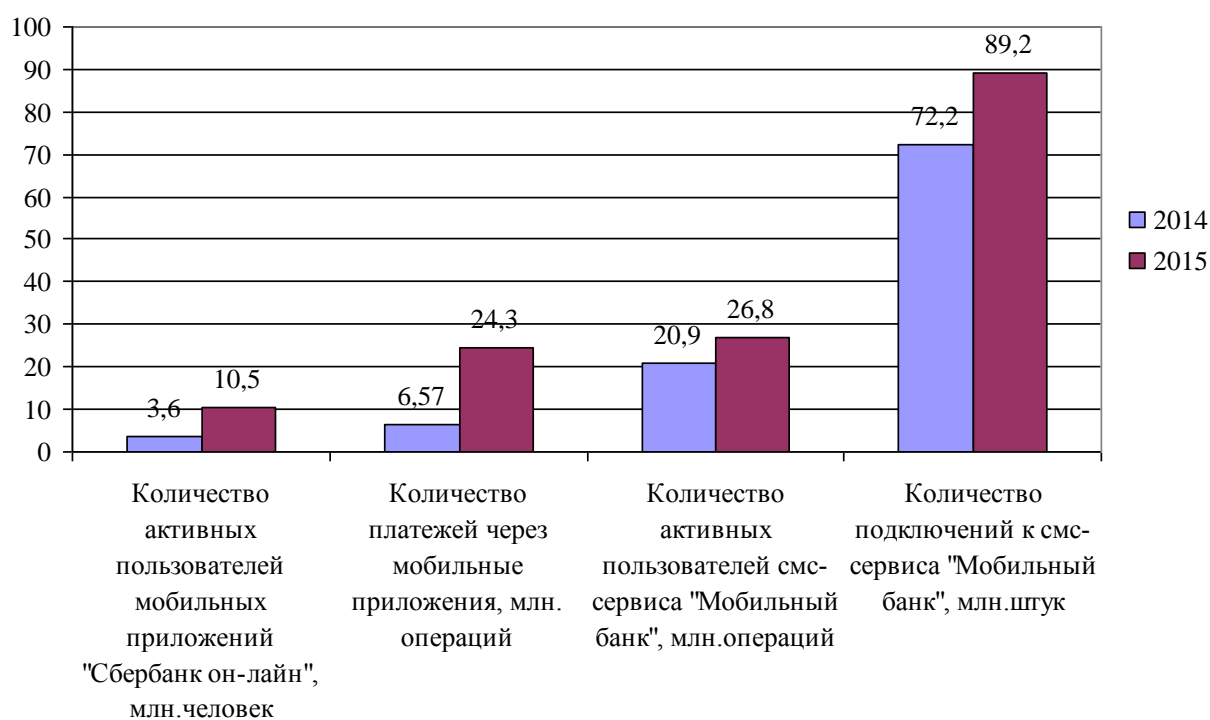


Рисунок 2.6 - Характеристика показателей дистанционного банковского обслуживания в ОАО «Сбербанк»

С увеличением количества удаленных транзакций, которые совершают клиенты, вопросы безопасности данных становятся критически важными (рисунок 2.7).

количество переводов, млн. операций

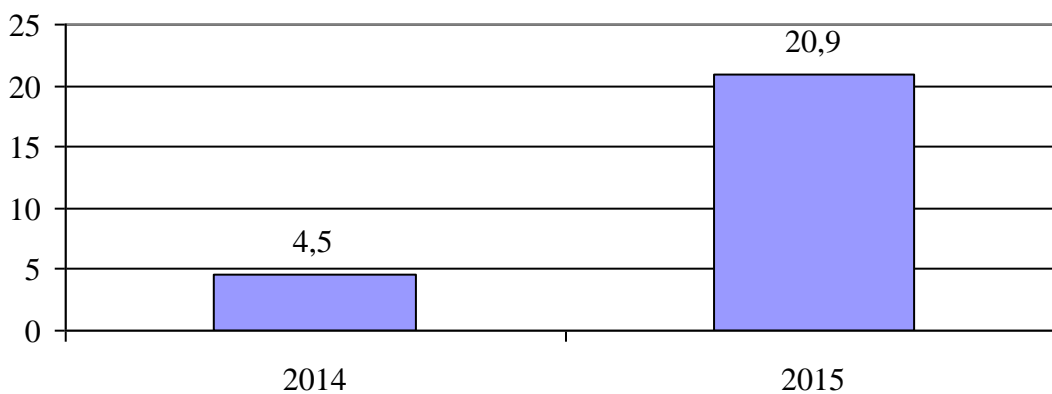


Рисунок 2.7 – Среднее количество переводов в месяц через систему ДБО

В среднем в 2015 году через ДБО в Сбербанке ежемесячно совершается 20,9 млн. переводов.

ОАО «Сбербанк» совершенствует системы обеспечения безопасности с учетом актуальных рисков и угроз, а также сотрудничаем с правоохранительными органами по пресечению преступной деятельности в отношении клиентов Сбербанка.

Основным инструментом контроля за выполнением мероприятий по отмыванию денежных средств через ДБО является служба внутреннего контроля Сбербанка.

Соответствие процедур внутреннего контроля установленным требованиям зависит от целого ряда факторов, таких, как:

- организационная структура банка, его размеры и характер деятельности,
- конкретная область деятельности, в которой применяется тот или иной метод.

В Сбербанке разработана политика ДБ АО «Сбербанк» по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (с учетом изменений, утвержденных Советом директоров ДБ АО «Сбербанк» от 02.12.2014 г., регистрационный № 3784) (Приложение 1).

Целью политики является защита деловой репутации Банка и недопущение вовлечение Банка в проведение банковских и иных операций Клиентом, связанных с легализацией (отмыванием) доходов, полученных преступным путем, и финансированием терроризма.

В целях эффективной реализации положений настоящей Политики Банк осуществляет следующие основные мероприятия:

- надлежащую проверку Клиента и (или) его представителя, бенефициарного собственника;
- надлежащую проверку ИПДЛ, членов его семьи и близких родственников;

- установление предполагаемой цели и характера деловых отношений;
- фиксирование сведений и документов, предоставляемых Клиентом и (или) его представителем;
- сбор дополнительной информации и сведений о репутации Клиента и (или) его представителя и бенефициарного собственника;
- мониторинг операций, проводимых Клиентом;
- взаимодействие с Уполномоченным органом;
- применение эффективных процедур оценки рисков операций Клиента, связанных с легализацией (отмыванием) доходов, полученных преступным путем, и финансированием терроризма;
- соблюдение сохранности сведений, составляющих банковскую, служебную или коммерческую тайну и сохранение режима конфиденциальности информации, получаемой в процессе осуществления внутреннего контроля в целях ПОД и ФТ;
- обновление информации о Клиенте и (или) его представителе, бенефициарном собственнике.

Контролер Сбербанка несет ответственность за организацию построения системы внутреннего контроля, которая включает:

- разрабатывает и актуализирует правила внутреннего контроля и программы его осуществления;
- разрабатывает в Банке единые требования по соблюдению принципа «Знай своего клиента» для применения в работе всеми работниками Банка;
- представляет отчеты.

Руководитель структурного подразделения Центрального офиса несет ответственность за отражение программ внутреннего контроля во внутренних нормативных и иных документах Банка, регламентирующих установление деловых отношений и осуществление операций с деньгами и (или) иным имуществом, подлежащих финансовому мониторингу в соответствии с требованиями настоящей Политики и Инструкции «Правила

внутреннего контроля в ДБ АО «Сбербанк» в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» от 10.07.2013г., регистрационный № 3186.

Юридическая служба несет ответственность за разработку типовых форм договоров на обслуживание клиентов и организацию работы по фиксации в указанных документах норм, требуемых настоящей Политикой, ВНД Банка в области ПОД и ФТ и законодательству РК.

Каждый работник Сбербанка обязан сохранять режим конфиденциальности ставшей ему известной информации о принимаемых конкретных мерах по ПОД и ФТ в отношении конкретного Клиента и его операций.

Система внутреннего контроля Сбербанка является:

- комплексной, охватывающей все виды деятельности, особое внимание уделяют финансовым нововведениям;
- приспособленной для предотвращения и выявления фактов мошенничества и других нарушений;
- увязанной с эффективной информационной системой и системой связи Сбербанка, с тем, чтобы обеспечить поток информации, необходимой для осуществления контроля;
- все аспекты службы внутреннего контроля должны отражены в соответствующей документации;
- Основная цель системы внутреннего контроля Сбербанка достигается путем организации контроля за соблюдением требований законодательства и иных нормативных актов, обеспечения контроля за банковскими рисками и надлежащим уровнем надежности кредитной организации, а также путем разрешения возникающих в процессе деятельности Сбербанка конфликтов интересов акционеров, совета директоров и менеджмента.

Меры по предотвращению отмыванию денег предпринимаются Сбербанком не только в соответствии с требованиями законодательства, но и

в собственных интересах. На рисунке 2.8 представлены последствия от неэффективной работы службы внутреннего контроля.

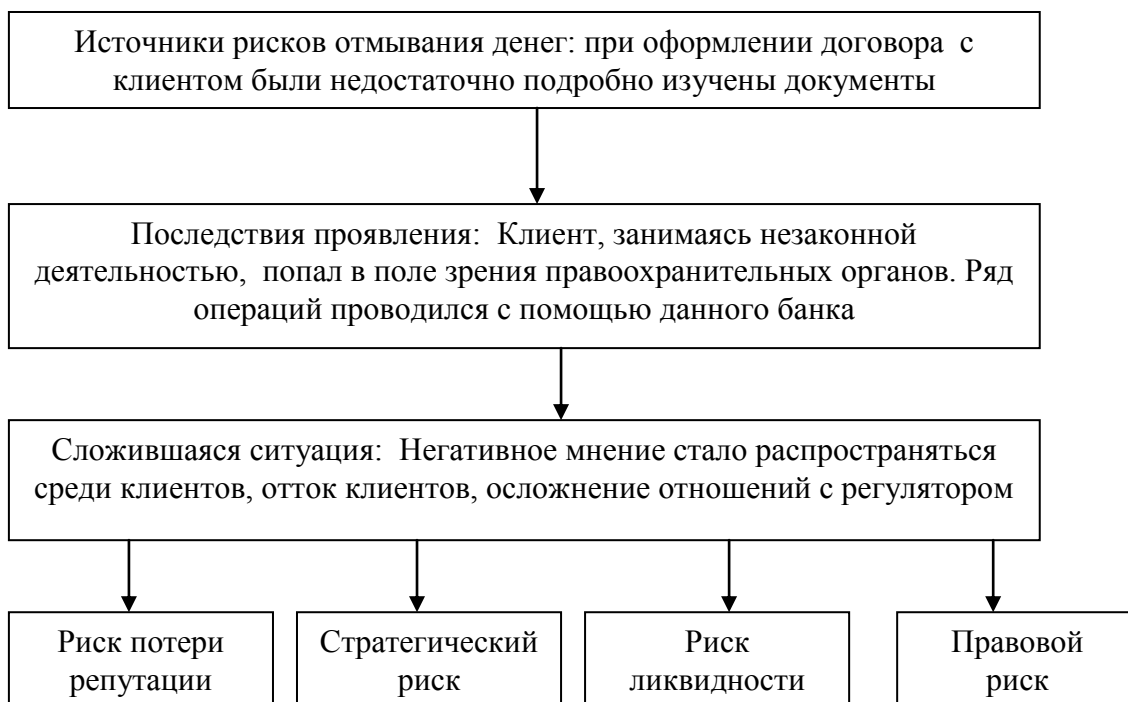


Рисунок 2.8 - Последствия от неэффективной работы службы внутреннего контроля

В связи с этим у Сбербанка сформирована внутренняя методика риск-подразделений и служб внутреннего контроля, касающаяся выполнения мер по противодействию отмыванию денег через ДБО. Особое внимание в системе внутреннего контроля Сбербанка уделяется принципу «Знай своего клиента», одной из основных составляющих которого является проведение процедур по идентификации клиентов.

В таблице 2.5 представлены случаи, выявленные специалистами банка, которые явились подозрительными фактами и подлежали проверке.

Таблица 2.5 – Случаи выявления отмывания денег через ДБО, тыс.раз

Наименование фактора	2014	2015	Темпы роста,%
осуществление операций на значительно большие суммы, чем можно было бы ожидать в обычном случае, учитывая характер деятельности владельца счета	563,4	852,3	151,278
случаи выявления подложной документации	851,8	1012,7	118,8894
случаи выявления сомнительной истории коммерческого предприятия	583,4	1251,88	214,5835
случаи, когда обе стороны сделки, проводимой при помощи ДБО фактически являются одним и тем же лицом	128,7	156,8	121,8337
рост объемов денежных переводов, не сопровождаемый соответственным ростом числа счетов, %	23,74	37,88	159,5619
превышение пределов хранимой наличности, установленной программой безопасности, %	24,5	25,6	104,4898
количество счетов с большим количеством небольших вкладов, млн.штук	896,4	914,5	102,0192
количество счетов с крупным объемом вкладов на несколько различных счетов с частым переводом основной части остатка на этих счетах на один и тот же счет в Сбербанке или в другом банке	1078,5	987,57	91,56885
число крупных вкладов, которое не отличается интенсивностью операций с наличностью	987,45	746,9	75,63927

Данные таблицы 2.5 отражают тот факт, что практически все факторы имеют тенденцию к росту, не смотря на все предпринимаемые меры. Это связано с расширением деятельности Сбербанка в сфере ДБО и развитием Интернет-технологий.

Некоторые показатели, такие как количество счетов с крупным объемом вкладов на несколько различных счетов с частым переводом основной части остатка на этих счетах на один и тот же счет в Сбербанке или в другом банке и число крупных вкладов, которое не отличается интенсивностью операций с наличностью снизились. Это произошло в связи с тем, что в 2015 году Сбербанку удалось достичь следующих результатов:

– прекращена деятельность шести киберпреступных групп, осуществляющих массовые атаки на клиентов Сбербанка, задержано и привлечено к ответственности 15 человек;

- выявлены и предотвращены попытки мошенничества в торговых точках, находящихся на обслуживании Сбербанка, на сумму около 0,6 млрд руб.;
- пресечено 25 попыток хищения средств юридических и более 154 тыс. попыток хищения средств физических лиц, предотвращен ущерб на сумму более 2,8 млрд.руб.;
- в рамках процедуры fraud-мониторинга «Красная кнопка - AP» (противодействие мошенничеству в сфере корпоративного кредитования) подтверждены риск-факторы по 181 кредитной заявке, в связи с чем предотвращена выдача недобросовестным заемщикам кредитных средств на общую сумму 6,9 млрд руб.;
- проведены аудиты и приемо-сдаточные испытания ключевых автоматизированных банковских систем.

В 2015 году Сбербанк проделал масштабную работу по борьбе со скиммингом. В частности, установили 12 тыс. комплектов активного антискиммингового оборудования. За счет мер, предпринятых Сбербанком, количество установки мошеннических устройств в отчетном периоде снизилось в три раза. На месте преступления при активном содействии подразделений экономической безопасности Сбербанка сотрудниками правоохранительных органов было задержано 36 человек. Предотвращенный ущерб от скимминга составил в 2015 году около 3.2 млрд рублей.

Тем не менее, в 2015 году в Сбербанке осуществление операций на значительно большие суммы, чем можно было бы ожидать в обычном случае, учитывая характер деятельности владельца счета выросло на 51%. Все факты были проверены, предприняты меры по предотвращению процесса отмывания денег. Для Сбербанка, как для лидера отрасли очень актуальна проблема предотвращения отмывания денег через ДБО. Эти факты приобрели в 2015 -2016 годах особую остроту и подтверждаются переменами, происходящими в национальных системах финансового мониторинга:

- увеличение числа агентов финансового мониторинга;
- усложнение мероприятий, направленных на противодействие легализации доходов, полученных преступным путем и финансированию терроризма.

В заключение главы необходимо сделать вывод, что мер, предпринимаемых Сбербанком в настоящее время не достаточно. Система ДБО развивается быстрыми темпами, а система внутреннего контроля работает по форме, принятой три года назад в 2013 году. В связи с этим полагаем, что Сбербанку следует:

- разработать и внедрить комплексные процедуры проверки сведений, представляемых клиентами;
- иметь данные о подлинном владельце счета (если счет был открыт на другое имя) и тщательно проверять данные, удостоверяющие личность, во избежание открытия счетов для фиктивных пользователей;
- располагать данными о профессиональной деятельности клиента и источниках его доходов;
- знать цель, с которой открывается счет, и представлять типы операций, в которые обычно вовлечен данный клиент. при открытии счета сотрудники банка должны понимать, нужно ли отнести клиента к категории высокого риска, требующей повышенного внимания.

В рамках выполнения процедуры мониторинга кредитным организациям можно было бы рекомендовать:

- иметь внутренние системы для проведения мониторинга операций, вызывающих подозрения;
- оценивать риск, исходя из конкретных видов счетов, регионов и операций;
- обращать внимание на любую операцию, превышающую установленный денежный порог депозитов;

- при открытии счета, ежемесячных телеграфных переводов, операций с наличностью, дорожными чеками, получения кредитов и заключения сделок, включая покупку и продажу валют, опционов и драгоценных металлов;
- обращать внимание на усиление активности по банковским счетам, особенно тем, которые могут стать объектами сомнительных операций (офшорные и корреспондентские счета, счета небанковских финансовых институтов, политических деятелей и личных инвестиций сотрудников компаний, счета, информация о которых может быть затребована судебными органами и др.);
- руководству Сбербанка стремиться к постановке и практической реализации задач в области предотвращения незаконных операций и заботиться о своей репутации не меньше, чем о прибылях, маркетинге и качестве обслуживания клиентов.

В заключение хотелось бы сказать, что ни одна программа по борьбе с отмыванием денег не может выявить все банковские операции, направленные на легализацию доходов, полученных преступным путем. Злоумышленники постоянно придумывают новые способы обхода банковских программ по выявлению незаконных операций, и только хорошо налаженная система по отмыванию денег в банках, которая находится в непрерывном развитии и учитывает все особенности современного банковского бизнеса, способна существенно минимизировать риски, связанные с отмыванием незаконных доходов.

3 Совершенствования организационно-экономических основ противодействия отмывания денег в дистанционном банковском обслуживании на примере АО «Сбербанк»

3.1 Разработка схемы противодействия отмывания денег в дистанционном банковском обслуживании на примере АО «Сбербанк»

ПАО Сбербанк является лидером в своей отрасли, на основании деятельности банка в сфере противодействия отмыванию денег в дистанционном банковском обслуживании проанализируем существующую схему и разработаем мероприятия по ее совершенствованию. Эта схема может стать основой для подобных мероприятий по противодействию для более мелких банков.

На рисунке 3.1 представлена схема

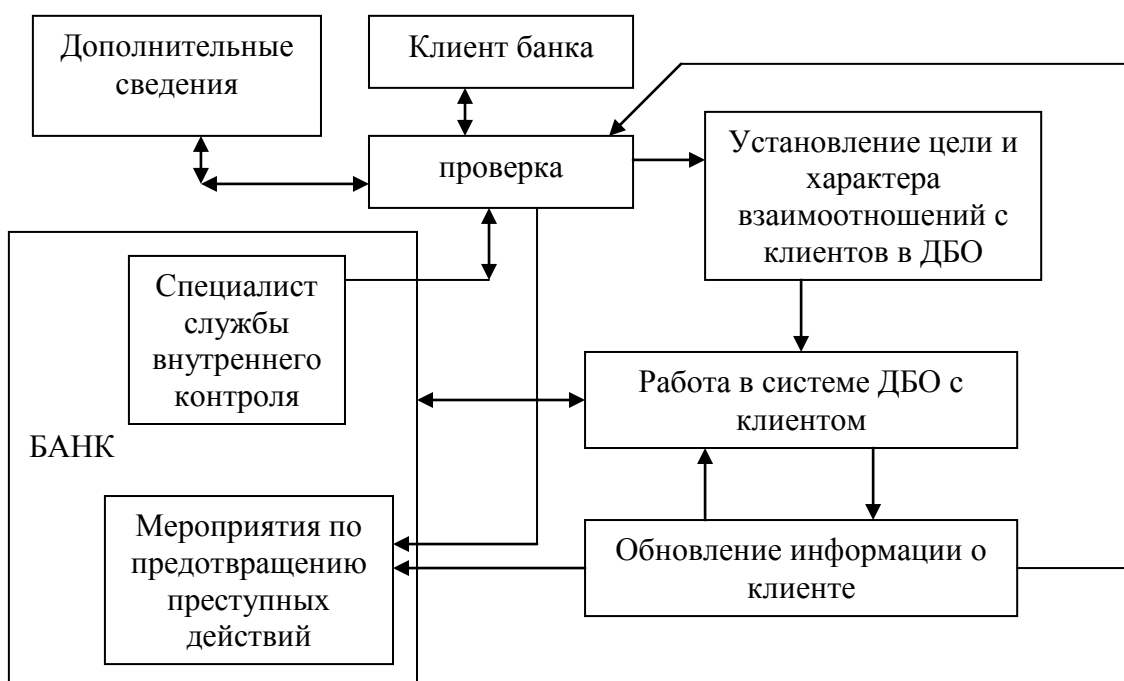


Рисунок 3.1 - Схема работы специалиста внутреннего контроля ПАО «Сбербанк»

Схема показывает, что главным инструментом контроля за противоправным использованием систем ДБО в кредитной организации является служба внутреннего контроля.

При выполнении своих задач служба внутреннего контроля в банке периодически проводит проверки по вопросам эффективности управления банковскими рисками.

При этом, необходимо отметить, что при использовании кредитной организацией систем ДБО возникает потребность в расширении полномочий службы и, как следствие, перечня проверяемых вопросов.

Специфика новых распределенных технологий при выполнении банковских операций приводит к тому, что теперь необходимо говорить не просто о банковской деятельности и соответственно анализировать ее содержание посредством внутреннего контроля, а рассматривать так называемый информационный контур банковской деятельности (ИКБД), который требует знаний в области инновационных информационных технологий банка в сфере ДБО.

Организация системы внутреннего контроля в ДБО представлена на рисунке 3.2.

Обозначения на схеме:

- ЛВС КО – локальная внутренняя сеть кредитной организации.
- БАС КО – банковская автоматизированная система кредитной организацию.
- Система ЭБ – система электронного банкинга.

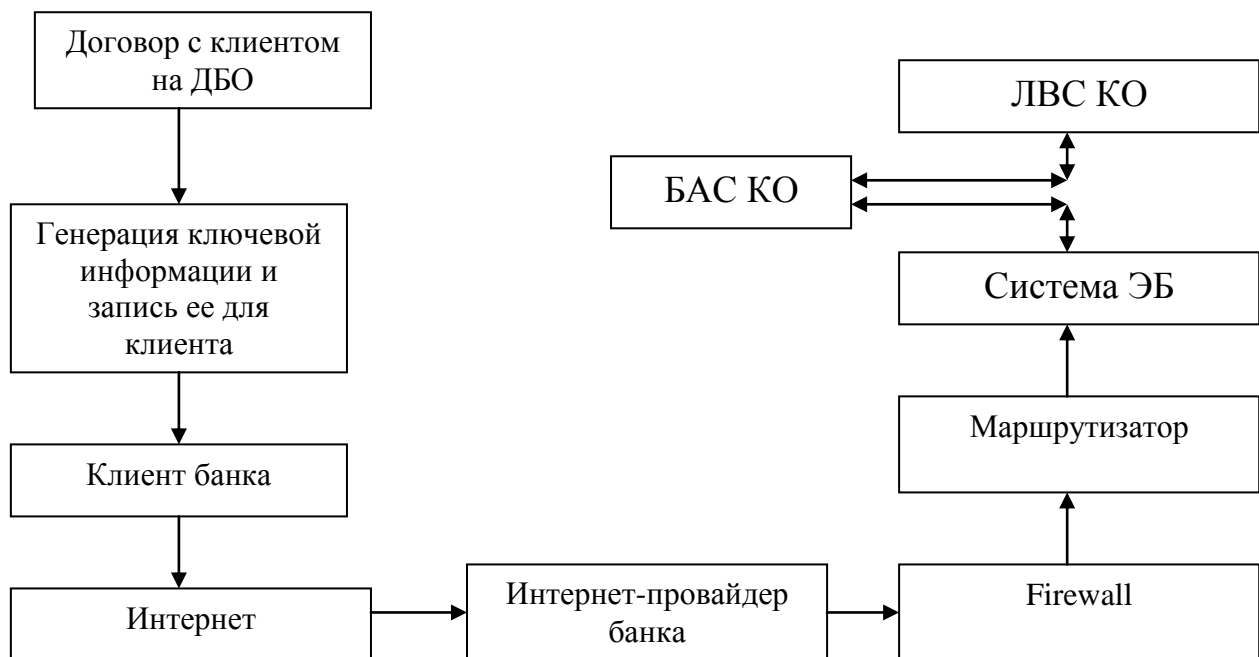


Рисунок 3.2 - Организация внутреннего контроля при использовании ДБО

Контур на рисунке 3.2 включает в себя реальные физические объекты, однако при осуществлении клиентом банковских операций с применением ДБО данные объекты становятся фактически виртуальными. Поэтому данные операции зачастую имеют непредсказуемый характер ввиду крупных масштабов сетевых систем, которые создаются множеством каналов связи в ПАО «Сбербанк», маршрутизаторов, компьютерных систем различных провайдеров, межсетевых шлюзов и других компонентов, ранее отсутствующих в ИКБД.

Стоит отметить, что на стадиях заключения договора на открытие счета в банке, генерации ключевой информации и записи ее на внешний носитель, работы провайдера-firewall-маршрутизатора сосредотачиваются наибольшие источники возникновения рисков.

Для сокращения риска на стадии «Заключение договора на открытие счета в банке и услуги ДБО» предлагается специалисту службы контроля изучить дополнительно следующие вопросы, которые могут входить в состав проверки систем ДБО, например:

- изучение уставных и финансовых документов клиента;
- рассмотрение деятельности клиента на рынке;
- анализ отзывов деловых партнеров;
- качество выпускаемой продукции или предоставляемых услуг;
- наличие квалифицированного персонала.

Для сокращения риска на стадии «Генерация ключевой информации и запись ее на внешний носитель для клиента» выделить основные требования к специалисту службы внутреннего контроля. Необходимо выделить:

- наличие специально выделенного помещения для данного вида работ;
- наличие утвержденного руководством банка регламента выполнения данных работ и инструкции по выполнению;
- ответственные сотрудники, прошедшие соответствующее обучение.

Процесс проверки экономической целесообразности операции, осуществленной клиентов посредством ДБО, затрагивает не только самого клиента, а также постоянное отслеживание сделок клиента. При идентификации бенефициара банком осуществляется проверка собственника, которому будут переведены денежные средства, установить учредителей, если бенефициаром является юридическое лицо, и наличие аффилированности лиц.

Противодействие легализации преступного движения капитала – это всего лишь малая часть вопросов, относящихся к компетенции специалиста службы внутреннего контроля ПАО «Сбербанк». Поэтому к сотрудниками указанного подразделения предъявляются жесткие требования, которые постоянно возрастают.

Именно поэтому для эффективной работы банка в процессе противодействия отмыванию денежных средств, в частности при использовании современных компьютерных технологий, наибольшее внимание необходимо уделять комплектованию квалифицированного кадрового состава службы внутреннего контроля банка и их постоянное

обучение. От их опыта и квалификации фактически зависит обеспечение безопасности и репутации кредитной организации.

На рисунке 3.4 представлена организационная структура стандартного офиса в отделении Сбербанка. На рисунке 3.3 представлена структура офиса.

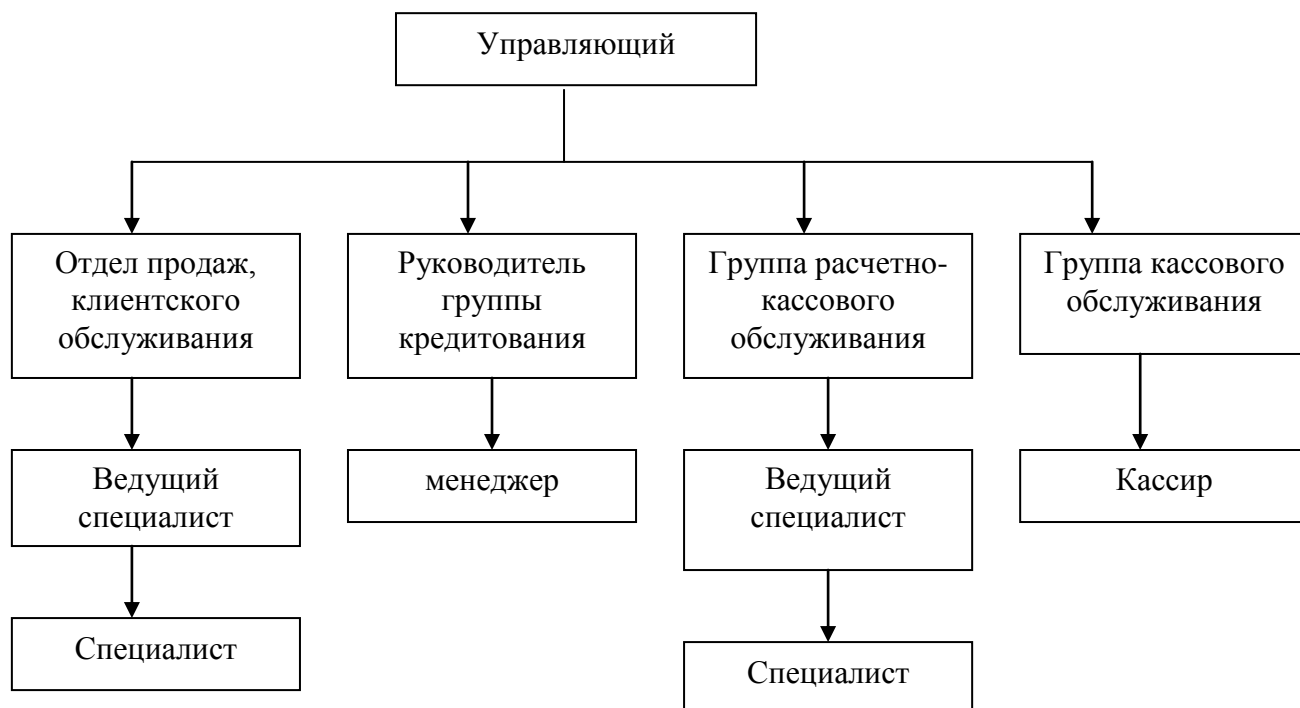


Рисунок 3.3 - Организационная структура офиса отделения Сбербанка

Рисунок показывает, что в региональных подразделениях Сбербанка не учитываются существующие схемы противодействия отмыванию денег в дистанционном банковском обслуживании, этой деятельности банка не уделяется должного внимания. Более того, у специалистов региональных подразделений не хватает необходимых знаний.

Увеличение числа потенциальных клиентов ДБО в ПАО «Сбербанк» приводит к необходимости разработки новой схемы работы службы внутреннего контроля.

В целях совершенствования управления процессом совершенствования схемы противодействия отмыванию денег в дистанционном банковском обслуживании в муниципальных районах Красноярского края предлагается разработать Программу создания и развития информационных взаимосвязей

между субъектами процесса контроля, формирование узлов удаленного доступа подразделений внутреннего контроля банков и органами полиции и прокуратуры (рисунок 3.4).



Рисунок 3.5 - Модернизация телекоммуникационной сети в целях совершенствования работы службы внутреннего контроля

Модернизацию деятельности банковских подразделений отдаленных муниципальных районов необходимо осуществлять по следующим направлениям:

- доступность и качество информации;
- открытый диалог;
- новый формат информационно-аналитического обеспечения подготовки и принятия управленческих решений в сфере банковских инноваций;
- позиционирование ПАО «Сбербанк» в регионе, стране, мире, повышение его привлекательности для сообщества как ведущего банка в деле организации внутреннего контроля при использовании ДБО;
- содействие развитию информационных ресурсов и инфраструктуры муниципального района.

Итак, для ОАО «Сбербанк» предлагается разработать комплексную методику совершенствования процесса в региональных отделениях ОАО «Сбербанк».

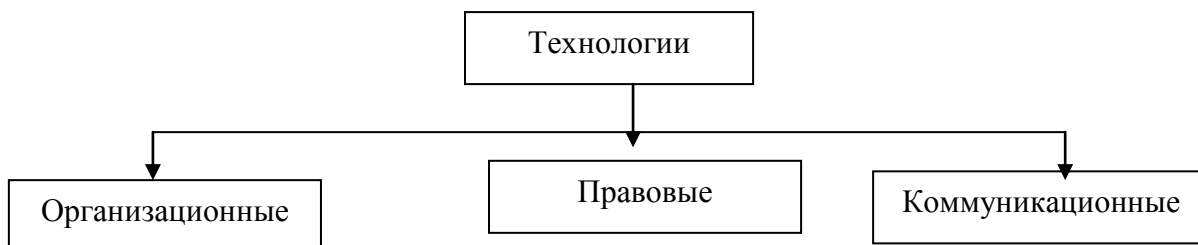


Рисунок 3.6 – Технологии комплексной схемы противодействия отмывания денег в дистанционном банковском обслуживании

ПАО «Сбербанк» предлагается формирование новой схемы, которая учитывает взаимодействие нескольких кредитных организаций по обмену информацией, правоохранительными органами и предполагает повышение грамотности специалистов кредитной организации в сфере противодействия отмывания денег в дистанционном банковском обслуживании. Новая схема работы представлена на рисунке 3.7.



Рисунок 3.7 - Новая схема работы

В настоящее время в ПАО «Сбербанк» трудности выявления экономического преступления, связанного с отмыванием преступного капитала, определяются применением новых экономических схем и инструментов со стороны преступного контингента, с работой которых не всегда знакомы специалисты кредитных организаций.

Постоянно применяются более усложненные схемы с участием множества юридических лиц, которые могут находиться как на территории одного государства, так и в нескольких странах мира. Процесс легализации преступных доходов включает в себя применение новых банковских инструментов и новых видов экономической деятельности.

Поэтому развитие правовой составляющей схемы, представленной на рисунке 3.7 будет способствовать формированию общего информационного банка данных. А организация специального обучения сотрудников банка позволит повысить уровень квалификации региональных подразделений ПАО «Сбербанк».

3.2 Затраты на реализацию мероприятий

В рамках данной работы проведено анкетирование 50 специалистов отделений ПАО «Сбербанк» Красноярского края – с целью выявления потребности в обучении в сфере противодействия отмыванию денег в ДБО. Метод анкетирования выбран в связи с его достоинством – оперативностью. В Приложении 2 представлена анкета.

Анкета составлена таким образом, чтобы позволяла однозначно и адекватно оценить потребности в обучении. Кроме того, она позволяет дать и более расширенные ответы, высказать свое мнение, предложить возможные решения проблем информирования в сфере противодействия отмывания денег в дистанционном банковском обслуживании. Результаты анкетирования помогут определить, кого и о чем необходимо информировать.

Содержание анкеты является предполагаемым перечнем вопросов плана обучения на квартал, полугодие, год. Ответы на вопросы анкеты помогут выявить новые направления обучения или сформировать однородные по уровню и потребностям группы для обучения.

В анкетировании приняли участие разные группы респондентов, в том числе сотрудники, работающие с клиентами в ДБО и специалисты отдела внутреннего контроля, разных возрастов и различного стажа работы. Результаты анкетирования респондентов представлены в таблицах ниже.

Таблица 3.1 - Характеристика респондентов, принявших участие в анкетировании

категория	пол		Возраст, лет					Стаж работы в должности	
	жен	муж	18-25	25-30	30-40	40-50	50 и выше	до 3-х лет	более 3-х лет
руководители	1	3		3	5				4

Окончание таблицы 3.1

категория	пол		Возраст, лет					Стаж работы в должности	
	жен	муж	18-25	25-30	30-40	40-50	50 и выше	до 3-х лет	более 3-х лет
специалист по работе с клиентами в ДБО	23	4		2	2	16		7	22
Специалисты банка	14	1	2	1	7			5	8
обеспечивающий специалист (отдел внутреннего контроля)	3	1	0	4	4	4	0	3	1
итого	41	9	2	10	18	20	0	15	35

Результаты опроса потребности в обучении показали следующее (таблица 3.2).

Необходимо отметить, что респонденты задавали уточняющие вопросы и интересовались о необходимости и периодичности проведения подобных мероприятий в будущем.

Таблица 3.2 -Результаты опроса потребности в обучении, %

Вопрос анкеты	да	нет	затруднились с ответом	другие ответы	итого
Как Вы считаете, в процессе трудовой деятельности необходимо проходить информирование по вопросам противодействия отмывания денег в дистанционном банковском обслуживании?	96%	4%	0%	0%	100%

Окончание таблицы 3.2

Вопрос анкеты	да	нет	затруднились с ответом	другие ответы	итого
По Вашему мнению, влияет ли на появление потребности в по вопросам противодействия отмывания денег в дистанционном банковском обслуживании					100%
сложный характер работы	25%	25%	0%	50%	100%
требования к квалификации	58%	8%	8%	25%	100%
возможность карьерного роста	75%	7%	4%	14%	100%
повышение заработной платы	67%	17%	0%	17%	100%
Влияет ли обучение, по Вашему мнению, на профессионализм работника	62%	8%	14%	16%	100%
Испытываете ли Вы необходимость в информации по противодействия отмывания денег в дистанционном банковском обслуживании?	46%	2%	0%	52%	100%
Обучение связано с Вашим карьерным ростом?	84%	0%	4%	12%	100%

С целью повышения эффективности деятельности ПАО «Сбербанк» предлагается создание центра обучения в банке.

В процессе своей деятельности сотрудники банка часто вынуждены давать рекомендации гражданам или другим заинтересованным лицам в применении системы ДБО, а для таких консультаций у сотрудников региональных подразделений нет достаточных знаний и времени. В связи с этим, заинтересованное лицо не может воспользоваться электронным сервисом ПАО «Сбербанк» или допустить невнимательность при выявлении преступлений в сфере ДБО.

Для решения данной проблемы в качестве повышения квалификации предлагает создание Центра консультаций на базе ПАО «Сбербанк».

Специалист службы внутреннего контроля при обращении лично или в режиме он-лайн проведет квалифицированную консультацию по работе в системе ДБО.

Проанализировав особенности традиционной и дистанционной форм консультаций, можно говорить о том, что обучение с применением компьютерных обучающих систем позволяет преодолеть недостатки традиционных очной и заочной форм обучения, ориентируясь на индивидуализацию процесса: формирует у обучаемых позитивное отношение к учебе; поддерживает компетентность и уверенность в себе; повышает объективность самооценки, дисциплинированность, интеллектуальную активность и тем самым эффективность обучения в целом.

При условии стабилизации ресурсного обеспечения (финансового, организационно-экономического, кадрового, информационного, материально-технического) обеих систем, использование технологий дистанционных консультаций может стать основой для становления принципиально новой формы непрерывного образования в сфере противодействия отмывания денег в дистанционном банковском обслуживании, опирающейся на индивидуализацию и самообразовательную мотивацию банковского служащего, поддерживаемую современными техническими средствами, что позволит сформировать ориентированную на профессионализацию эффективную обучающую систему консультирования.

Имеются три причины огромного интереса к дистанционному консультированию через Интернет:

- первая состоит в том, что существует потребность в простой достоверной информации;
- вторая – в том, что технологии для удовлетворения этих потребностей есть уже сейчас и в дальнейшем будут только совершенствоваться;

- третья причина состоит в том, что все сферы деятельности рассматривают дистанционное консультирование как новый важный рынок и, следовательно, возможность деловой деятельности;
- многие клиенты банка не всегда могут получить личную консультацию, получение он-лайн консультаций с последующей работой с электронным документооборотом он-лайн будет способствовать повышению качества обслуживания.

Материально-техническое обеспечение ИКЦ осуществляется за счёт средств, предусмотренных на противодействие отмывания денег в дистанционном банковском обслуживании.

Функциональные обязанности специалиста ИКЦ по противодействию отмывания денег в дистанционном банковском обслуживании:

- предоставление адресной методической, информационной, консультационной, образовательной поддержки предпринимателей по вопросам ДБО Красноярского края;
- оформление и наполнение информационно–справочного стенда по актуальным вопросам ведения ДБО,; нормативно-правовые акты Красноярского края, муниципального образования, методические, справочные, новостные материалы.
- формирование библиотеки деловой литературы по вопросам ДБО;
- консультации других кредитных организаций по противодействию отмывания денег в дистанционном банковском обслуживании.
- проведение анкетирования среди предпринимателей с целью изучения состояния предпринимательской деятельности, потребности в консультациях;
- системное информирование руководителя ПАО «Сбербанк» о результатах работы ИКЦ.

Проанализируем затраты на создание ИКЦ.

Расходы на услуги связи, Internet. В качестве одного из необходимых элементов функционирования ИКЦ ПАО «Сбербанк» является обмен информацией между территориально расположенными подразделениями банка, компаниями, другими банками, правоохранительными органами в режиме реального времени, что требует выхода в Internet.

Таблица 3.3 - Затраты на создание проекта ИКЦ ПАО «Сбербанк»

Наименование	Количество	Цена	Итого
Единовременные затраты на формирование отдела маркетинга			
1. Компьютер	3	15000	45000
2. Принтер, сканер, ксерокс.	1	12000	12000
3. Подключение к Интернет	-	1500	1500
4. Рабочее место	3	2500	7500
Итого	-	-	66000
Ежемесячные затраты по проекту			
Заработная плата сотрудников, том числе:			39000
юрис	1	15000	15000
диспетчер	1	12000	12000
консультант	1	12000	12000
Начисления на ФОТ (13%)			5070
Амортизация (10 % в год, линейный метод начисления)			4500
Проведение мероприятий по стимулированию оказанных информационных услуг (регулярные)	-	350	350
Электроэнергия		650	650
Итого в месяц	-		49570
Всего за год			660840

Единовременные затраты составляют 66000 рублей, а ежемесячные 49570 рублей.

Ниже приведен расчет средней стоимости разовой консультации по проекту.

Консультант работает на постоянной основе, получает заработную плату, составляет график обучения специалистов Сбербанка, планирует свою деятельность. Для персонала Сбербанка это обучение бесплатное. Для

специалистов других банков или заинтересованных клиентов – платное.

Выручка от этих консультаций представлена в табл.3.4

Таблица 3.4 - Расчет услуги для другого банка или юридического лица

№ п/п	Вид юридической помощи	Цена за час	Трудозатраты, часов	Стоимость
1.	Устная консультация	1700 рублей	0,5-1,0 часа	1700 рублей
2.	Ознакомление с отчетностью клиента – юридического лица	1700 рублей	1 час	1700 рублей
3.	Подготовка информации по клиенту, помощь	1700 рублей	1 час	1700 рублей
4.	Поиск и анализ судебной практики в случае необходимости	1700 рублей	2 часа	3400 рублей

В рамках проекта стоимость услуги может быть безвозмездной или со скидкой в 50% для правоохранительных органов или особых клиентов банка.

Услуги включают и консультирование, и сопровождение спорных вопросов в органах государственной власти, а также представление интересов в судебных спорах. Консультанты нового центра ПАО «Сбербанк» помогут в очень широком перечне вопросов юридического характера в сфере противодействия отмывания денег в дистанционном банковском обслуживании.

Среди них:

- подготовка и разработка договоров, регламентов, положений, правил, инструкций, иных актов для юридических лиц;
- экспертиза договоров, правил, инструкций и других актов для юридических лиц;
- составление исковых заявлений, претензий, жалоб, физическим и юридическим лицам;
- помощь при работе с ДБО;

– представление интересов физических и юридических лиц в судах общей юрисдикции, арбитражных судах первой, апелляционной, кассационной и надзорной инстанций.

Таблица 3.5 - Месячный доход ИКЦ ПАО «Сбербанк»

Услуга	Макс. кол-во клиентов в день	Средняя цена 1 услуги	Выручка в месяц	Выручка в год, тыс.руб	Расход в год, тыс.руб.	Прибыль
консультант	5	1000	150 000	1 800	660,48	1140

5 клиентов в день – это люди, которые обратились за консультацией по проблемам противодействия отмыванию денег. Необходимо отметить, что люди редко обращаются за такой консультацией в настоящее время.

Итак, дополнительная прибыль банка в год составит 1140 тыс.руб.*12*5 = 68,4 (млн.руб.)

Это при том, что работа по проекту имеет огромное значение – банки могут сократить свои расходы и убытки от отмывания денег в дистанционном банковском обслуживании.

Рассчитаем возможный экономический эффект.

3.3 Расчет экономической эффективности мероприятий

По оценкам Росфинмониторинга, в России ежегодно легализуется 250-300 млрд. руб. через ДБО, при этом правоохрнительными органами выявляется порядка 30 млрд. руб. легализованных криминальных доходов. Отмывание является одним из видов противоправного бизнеса, тесно связанного с деятельностью транснациональных преступных групп.

Согласно внутреннему отчету ПАО «Сбербанк» за 2015 год кредитная организация несет значительные финансовые потери, связанные с отмыванием доходов в системе ДБО (таблица 3.6).

Таблица 3.6 – Размер потерь банка от отмывания денег в дистанционном банковском обслуживании ПАО «Сбербанк»,

млн.руб.

Наименование фактора	2014	2015	Темпы роста, %
Возвращено денежных средств по суду со счета клиента, признаны незаконными (чистый убыток банка)	19,52	26,85	137,55
– в том числе по причине некомпетентности сотрудника ПАО «Сбербанк»	4,49	6,18	137,55
– в том числе по причине некомпетентности другого банка (в условиях межбанковского перевода)	15,03	20,67	137,55
Убытки от несостоявшихся сделок в связи с подложной документации	52,87	98,13	185,61
– в том числе по причине некомпетентности сотрудника ПАО «Сбербанк»	24,32	45,14	185,61
– в том числе по причине некомпетентности другого банка (в условиях межбанковского перевода)	28,55	52,99	185,61

Предполагается, что в связи с развитием коммуникаций в сфере противодействия преступлений в сфере ДБО, повышению уровня квалификации специалистов банка, созданию общего банка данных случаи некомпетентной работы сотрудников сократятся на 30%. Об этом свидетельствует опыт создания центров обучения в банках.

В таблице 3.7 представлена эффективность предлагаемой схемы, случаи отмывания незаконных доходов сокращаются, сокращаются и убытки.

Таблица 3.7 – Размер потерь банка от отмывания денег в дистанционном банковском обслуживании ПАО «Сбербанк»

млн.руб.

Наименование фактора	2014	2015	Темпы роста,%	проект ИКЦ	темпы роста (снижения) проект к 2015 году, %	темпы роста (снижения) проект к 2014 году, %
Возвращено денежных средств по суду со счета клиента, признаны незаконными (чистый убыток банка)	19,52	26,85	137,55	20,65	23,09	105,79
- в том числе по причине некомпетентности сотрудника ПАО «Сбербанк»	4,49	6,18	137,55	4,75	23,14	105,79
- в том числе по причине некомпетентности другого банка (в условиях межбанковского перевода)	15,03	20,67	137,55	15,9	23,08	105,79
Убытки от несостоявшихся сделок в связи с подложной документацией	52,87	98,13	185,61	75,48	23,08	142,77
- в том числе по причине некомпетентности сотрудника ПАО «Сбербанк»	24,32	45,14	185,61	34,72	23,08	142,76
- в том числе по причине некомпетентности другого банка (в условиях межбанковского перевода)	28,55	52,99	185,61	40,76	23,08	142,77

В расчете эффективности не учитывались потери от операций, которые связаны с процентными ставками, поскольку лица, отмывающие свои доходы, реинвестируют средства в те области, где менее вероятно раскрытие их схем, а не в те, где выше норма отдачи.

Операции, направленные на отмывание денег, снижают налоговые доходы правительства (тем самым наносят косвенный ущерб честным налогоплательщикам). Как правило, данная потеря доходов означает более

высокие ставки налогообложения по сравнению с нормальной ситуацией, при которой преступные доходы были бы законными и облагались налогами.

Кроме того, для банков, участвующих в отмывании денег, возникает риск потери репутации. Его значимость возрастает в условиях современного ДБО.

Данные таблицы 3.7 и анализ представленных выше схем предполагает эффективную систему борьбы по противодействию отмывания денег в дистанционном банковском обслуживании на примере АО «Сбербанк». Введение преступных доходов в легальный экономический оборот связано с риском привлечь внимание органов государственного контроля и правоохранительных органов, что требует маскировки происхождения криминальных средств. Для этих целей совершается множество фиктивных или запутанных сделок, преступные доходы инвестируются в предпринимательскую деятельность, где они преобразуются в результате хозяйственных процессов.

Создание единой схемы, коммуникации в режиме реального времени, повышение квалификации сотрудников позволит сократить потери банка и государства.

ЗАКЛЮЧЕНИЕ

Итак, в работе проведено исследование процессов противодействия отмыванию денег в условиях ДБО. Основным выводом после изучения теоретических аспектов проблемы стало то, что неразрешенной общеправовой проблемой на пути развития электронных расчетов, осуществляемых с использованием Интернета в Российской Федерации, а также основной проблемой развития всего электронного сегмента российской экономики в целом следует признать пассивность государства в установлении правового регулирования общественных отношений в данной сфере. В настоящее время не сформирован внутренний механизм работы банка, сложную систему противодействия могут позволить создать только крупные кредитные организации, такие как ПАО «Сбербанк».

На его примере проведено исследование факторов, влияющих на деятельность кредитной организации и связанной с объемами легализованных денежных средств путем преступных схем.

В работе подробно изучена структура системы дистанционного обслуживания. Выявлена положительная динамика дистанционного обслуживания, исследовано влияние рисков, связанных с отмыванием денежных средств, на финансовые результаты деятельности банка.

Анализ показал, что количество операций, производимых через удаленные банковские каналы, растет высокими темпами: в 2015 году количество активных пользователей он-лайн банкинга по Группе увеличилось на 50 %. а мобильного банка - на 28 %.

В тоже время незначительно снизилось количество банкоматов, что обусловлено улучшением качества он-лайн сервисов и соответственно ростом популярности безналичного способа оплаты.

ОАО «Сбербанк» совершенствует системы обеспечения безопасности с учетом актуальных рисков и угроз, а также сотрудничаем с

правоохранительными органами по пресечению преступной деятельности в отношении клиентов Сбербанка.

Основным инструментом контроля за выполнением мероприятий по отмыванию денежных средств через ДБО является служба внутреннего контроля Сбербанка.

Соответствие процедур внутреннего контроля установленным требованиям зависит от целого ряда факторов, таких, как:

- организационная структура банка, его размеры и характер деятельности,
- конкретная область деятельности, в которой применяется тот или иной метод.

В Сбербанке разработана политика ДБ АО «Сбербанк» по противодействию легализации (отмыванию) доходов, полученных преступным путем. У Сбербанка сформирована внутренняя методика риск-подразделений и служб внутреннего контроля, касающаяся выполнения мер по противодействию отмыванию денег через ДБО. Особое внимание в системе внутреннего контроля Сбербанка уделяется принципу «Знай своего клиента», одной из основных составляющих которого является проведение процедур по идентификации клиентов.

Тем не менее, анализ показал, что мер, предпринимаемых Сбербанком в настоящее время не достаточно. Система ДБО развивается быстрыми темпами, а система внутреннего контроля работает по форме, принятой три года назад в 2013 году. В связи с этим полагаем, что Сбербанку следует:

- разработать и внедрить комплексные процедуры проверки сведений, представляемых клиентами;
- иметь данные о подлинном владельце счета (если счет был открыт на другое имя) и тщательно проверять данные, удостоверяющие личность, во избежание открытия счетов для фиктивных пользователей;
- располагать данными о профессиональной деятельности клиента и источниках его доходов;

– знать цель, с которой открывается счет, и представлять типы операций, в которые обычно вовлечен данный клиент. при открытии счета сотрудники банка должны понимать, нужно ли отнести клиента к категории высокого риска, требующей повышенного внимания.

На основе проведенного анализа автором работы была разработана схема может стать основой противодействия отмыванию денег через ДБО для более мелких банков. Схема показывает, что главным инструментом контроля за противоправным использованием систем ДБО в кредитной организации является служба внутреннего контроля. Предлагается разработать комплексную методику совершенствования процесса в региональных отделениях ОАО «Сбербанк».

ПАО «Сбербанк» предлагается формирование новой схемы, которая учитывает взаимодействие нескольких кредитных организаций по обмену информацией, правоохранительными органами и предполагает повышение грамотности специалистов кредитной организации в сфере противодействия отмывания денег в дистанционном банковском обслуживании.

В настоящее время в ПАО «Сбербанк» трудности выявления экономического преступления, связанного с отмыванием преступного капитала, определяются применением новых экономических схем и инструментов со стороны преступного контингента, с работой которых не всегда знакомы специалисты кредитных организаций.

Постоянно применяются более усложненные схемы с участием множества юридических лиц, которые могут находиться как на территории одного государства, так и в нескольких странах мира. Процесс легализации преступных доходов включает в себя применение новых банковских инструментов и новых видов экономической деятельности, правовой составляющей схемы. В работе предлагается провести обучение специалистов банка по мерам противодействия отмыванию денежных средств в условиях ДБО. Это очень важный аспект исследованных проблем, так как специалист банка сможет распознать проблемы на ранних стадиях

общения с клиентом, обратить внимание на особенные операции, чем повысить эффективность деятельности по противодействию преступности в банковской сфере.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

- 1 Федеральный закон от 07.08.2001 N 115-ФЗ (ред. от 29.12.2015) "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма"// СПС «Консультант плюс»
- 2 Уголовный кодекс РФ Глава 22 статья 174 «Легализация (отмывание) денежных средств или иного имущества, приобретенных другими лицами преступным путем»
- 3 Письмо Банка России от 05.04.2007 N 44-Т "О проверке осуществления кредитными организациями идентификации клиентов, обслуживаемых с использованием технологий дистанционного банковского обслуживания (включая интернет-банкинг)"
- 4 Письмо Банка России от 27.04.2007 №60-Т «Об особенностях обслуживания кредитными организациями клиентов с использованием дистанционного доступа к банковскому счету клиента (включая интернет-банкинг)».
- 5 Письмо Банка России от 10.01.2007 N 1-Т "О Методических рекомендациях по проведению проверок работы кредитных организаций по выявлению, фиксированию и направлению в уполномоченный орган сведений по операциям с денежными средствами в наличной форме, подлежащим обязательному контролю".
- 6 Письмо Банка России от 13.03.2008 N 24-Т "О повышении эффективности работы по предотвращению сомнительных операций
- 7 Письмо Банка России от 17.01.2013 N 2-Т "О применении части 2 статьи 15.27 Кодекса Российской Федерации об административных правонарушениях".
- 8 Указание Банка России от 09.08.2004 N 1486-У "О квалификационных требованиях к специальным должностным лицам, ответственным за соблюдение правил внутреннего контроля в целях противодействия

легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма и программ его осуществления в кредитных организациях».

9 Указание Банка России от 14.09.2011 N 2696-У "Об установлении срока передачи сведений, полученных при проведении идентификации".

10 Указание Банка России от 04.03.2014 N 3207-У "О перечне должностных лиц Банка России, уполномоченных составлять протоколы об административных правонарушениях".

11 Beare M.E. Tracing of illicit funds: money laundering in Canada. Ottawa, 1990. P. 304

12 Агапцов С.А. Государственный финансовый контроль и бюджетная политика Российского государства. М., 2004.

13 Актуальные проблемы теории и практики финансового права Российской Федерации / Под ред. проф. д.ю.н. А.Н. Козырина // СПС "Гарант", 2009.

14 Бурцев В.В. Факторы финансовой безопасности России // Менеджмент в России и за рубежом. 2001. N 1.

15 Волеводз А.Г. Международный розыск, арест и конфискация полученных преступным путем средств и имущества. М., 2000.

16 Волженкин Б.В. Отмывание денег. СПб., 2014. С. 9 - 10.

17 Волженкин Б.В. Экономические преступления. СПб., 2013.

18 Громов И.В. Способы совершения мошенничества в финансово-кредитной сфере // Российский следователь. 2008. N 15.

19 Жубрин Р.В. Борьба с легализацией преступных доходов: теоретические и практические аспекты. М.: Волтерс Клувер, 2011.

20 Зрелов А.П., Краснов М.В. Налоговые преступления / Под ред. К.К. Саркисова. М.: Статус-Кво, 2004.

21 Иванов Э.А. Отмывание денег и правовое регулирование борьбы с ним. М.: ИГП РАН, 1999.

- 22 Ильин И. Е. Новое в борьбе с отмыванием "грязных" денег // Управление в кредитной организации. 2009. № 4
- 23 Иноземцев В. За пределами экономического общества. М., 1988.
- 24 Исправников В.О. Теневая экономика: иной путь и третья сила // Российский экономический журнал. 2008.
- 25 Кадовик Е.И. Организованные группы, преступные сообщества и легализация (отмывание) денежных средств // Юридический мир. 2002. N 4.
- 26 Камынин И.Н. Новое законодательство о борьбе с легализацией (отмыванием) преступных доходов // Законность. 2001. N 11.
- 27 Каратаев М.В. Управление риском вовлечения российских банков в процессы легализации преступных доходов: Автореф. дис. ... к.э.н. Иваново, 2011. С. 7.
- 28 Карпович О.Г. Вопросы международно-правового подхода борьбы с отмыванием преступных доходов // Внешнеторговое право. 2014. N 2.
- 29 Кернер Х.Х., Дах Э. Отмывание денег. М., 2013. С. 37 - 38.
- 30 Кондрат Е.Н. Правонарушения в финансовой сфере России. Угрозы финансовой безопасности и пути противодействия. М.: Юстицинформ, 2014. 928 с.
- 31 Котов К.В. Легализация доходов как способ борьбы с теневой экономикой // Налоговая политика и практика. 2010. Июнь. N 6.
- 32 Кочетов Э., Петрова Г. Геоэкономика: финансы реальные и виртуальные (финансовый дуализм и его правовые аспекты) // Общество и экономика. 2000. N 1.
- 33 Кудрин А.Л. Мировой финансовый кризис и его влияние на Россию. // Вопросы экономики №1 2009.
- 34 Лебедев А.Е. Отмывать — не обналачивать // Газета «Парламентская газета», № 177 (2027), 26.10.2006.
- 35 Лямин Л.В. Интернет-банкинг: сопутствующие факторы банковских рисков и организация регулирования и надзора // Проблемы управления банковскими и корпоративными рисками. - М.: Финансы и статистика, 2005.

- 36 Мельников В.Н., Мовсесян А.Г. Противодействие легализации незаконных доходов. М: МЦФЭР, 2007. — 528 с. — (Приложение к журналу «Налоговые споры», 6-2007).
- 37 Мюллер К., Пикель А. Смена парадигм посткоммунистической трансформации // Социологические исследования. 2002. N 9
- 38 Новикова В. Зачем создавать плохие банки? Давайте создавать и развивать хорошие // Аналитический банковский журнал №3 (166) март 2009.
- 39 Новикова В. Цена денег вопрос серьезный // Аналитический банковский журнал №3 (166) март 2009.
- 40 Ореховский П. «Теневые» параметры реформируемой экономики (по материалам научной конференции) // Российский экономический журнал. 1996. №8-9.
- 41 Орлова Н. Трудно быть банком // Forbes.-2004 №4.
- 42 Ревенков П.В., Воронин А.Н. Электронный банкинг: организация и методика защиты от противоправных действий // Расчеты и операционная работа в коммерческом банке, №2, 2009.
- 43 Ревенков П.В., Дудка А.Б., Воронин А.Н., Каратаев М.В. Финансовый мониторинг: управление рисками отмывания денег в банках. - М.: КНОРУС: ЦИПСИР, 2012. 280 с.
- 44 Филатова М.А. Уголовная ответственность за легализацию (отмывание) денежных средств или иного имущества, полученных преступным путем, по законодательству России и Австрии: Автореф. дис. ... к.ю.н. М., 2014. С. 20.
- 45 Чупрова Е.В. Особенности ответственности за отмывание незаконных доходов по законодательству некоторых стран//Международное и зарубежное банковское право.№3.2006.
- 46 Шевлоков В.Финансовый контроль как функция финансового управления //Финансы.№1.2004.

- 47 Шохин С. О. Противодействие легализации доходов полученных преступным путем: роль Счетной палаты Российской Федерации // Банковское право. - 2004. - №3.
- 48 Шумилов В.М. Международное финансовое право: Учебник. М., 2015. С. 285
- 49 Сбербанк России — [Электронный ресурс] — Режим доступа. — URL: <http://www.sberbank.ru/ru/about/today>
- 50 Центральный банк РФ — [Электронный ресурс] — Режим доступа. — URL: <http://www.cbr.ru> (дата обращения 09.03.2016)

Приложение А

Приложение 1 к решению Совета директоров
ДБ АО «Сбербанк» № 31 от 18 октября 2013 года

«Согласовано»
Правлением ДБ АО «Сбербанк»
от «10» июля 2013 г.
от «16» сентября 2013 г.

«Утверждено»
Советом директоров ДБ АО «Сбербанк»
от «18» октября 2013 г.
Рег. № 3448

**Политика ДБ АО «Сбербанк»
по противодействию легализации (отмыванию) доходов,
полученных преступным путем, и финансированию терроризма
(с учетом изменений, утвержденных Советом директоров ДБ
АО «Сбербанк» от 02.12.2014 г., регистрационный № 3784)**

Продолжение приложения А

РЕЗЮМЕ ПО ВНД

Наименование ВНД	Политика ДБ АО «Сбербанк» по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма
Необходимость в разработке/изменении ВНД	Политика определяет порядок соблюдения требований законодательства Республики Казахстан о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма
Краткое описание ВНД	Политика устанавливает цели, задачи и основные мероприятия ДБ АО «Сбербанк» в целях исключения его прямого или косвенного участия/вовлечения в проведение банковских и иных операций, связанных с легализацией (отмыванием) доходов, полученных преступным путем, а также с финансированием терроризма
Какие процессы в Банке затрагивает ВНД	Установление деловых отношений с Клиентом
Работу, каких структурных подразделений Банка затрагивает ВНД	Все структурные подразделения и должностные лица Банка
Дополнительная информация	–

Продолжение приложения А

Содержание

ГЛАВА 1. ОБЩИЕ ПОЛОЖЕНИЯ 92

ГЛАВА 2. ЦЕЛИ И ЗАДАЧИ 94

ГЛАВА 3. ОСНОВНЫЕ МЕРОПРИЯТИЯ, ПРЕДПРИНИМАЕМЫЕ БАНКОМ В ЦЕЛЯХ ПРОТИВОДЕЙСТВИЯ ЛЕГАЛИЗАЦИИ (ОТМЫВАНИЮ) ДОХОДОВ, ПОЛУЧЕННЫХ ПРЕСТУПНЫМ ПУТЕМ, И ФИНАНСИРОВАНИЮ ТЕРРОРИЗМА.. 94

ГЛАВА 4. ОРГАНИЗАЦИЯ РАБОТЫ И ОТВЕТСТВЕННОСТЬ РАБОТНИКОВ БАНКА ПО ПРОТИВОДЕЙСТВИЮ ЛЕГАЛИЗАЦИИ (ОТМЫВАНИЮ) ДОХОДОВ, ПОЛУЧЕННЫХ ПРЕСТУПНЫМ ПУТЕМ, И ФИНАНСИРОВАНИЮ ТЕРРОРИЗМА В БАНКЕ 95

ГЛАВА 5. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ 96

ПЛАН ВНЕДРЕНИЯ ОШИБКА! ЗАКЛАДКА НЕ ОПРЕДЕЛЕНА.

Продолжение приложения А

ПОЛИТИКА ДБ АО «СБЕРБАНК» ПО ПРОТИВОДЕЙСТВИЮ ЛЕГАЛИЗАЦИИ (ОТМЫВАНИЮ) ДОХОДОВ, ПОЛУЧЕННЫХ ПРЕСТУПНЫМ ПУТЕМ, И ФИНАНСИРОВАНИЮ ТЕРРОРИЗМА

ГЛАВА 1. ОБЩИЕ ПОЛОЖЕНИЯ

1. Политика ДБ АО «Сбербанк» по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (далее – Политика) устанавливает цели, задачи и основные мероприятия ДБ АО «Сбербанк» (далее – Банк) в целях исключения его прямого или косвенного участия/вовлечения в проведение банковских и иных операций, связанных с легализацией (отмыванием) доходов, полученных преступным путем, а также с финансированием терроризма.

2. Настоящая Политика разработана в целях обеспечения надлежащего исполнения Закона Республики Казахстан «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» от 28 августа 2009 года №191-IV (далее – Закон о ПОД и ФТ), в рамках рекомендаций Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ) и Всеобщих директив по противодействию отмыванию доходов в частном банковском секторе (Вольфсбергские принципы).

3. Настоящая Политика подлежит обязательному применению и соблюдению всеми структурными подразделениями, должностными лицами и ответственными работниками Банка.

4. В настоящей Политике используются следующие понятия и термины:

1) *Всеобщие директивы по противодействию отмыванию доходов в частном банковском секторе (Вольфсбергские принципы)* – свод рекомендаций, которые определяют предупреждение транснациональных переводов нелегальных денег, как основную задачу всех банков мира и банковской политики в целом, подписаны 30 октября 2000 г.;

1-1) *бенефициарный собственник* – физическое лицо, которому прямо или косвенно принадлежат более 25 % (двадцати пяти процентов) долей участия в уставном капитале, либо размещенных (за вычетом привилегированных и выкупленных обществом) акций клиента Банка – юридического лица, а равно физическое лицо, осуществляющее контроль над клиентом Банка иным образом, либо в интересах которого клиентом Банка совершаются операции с деньгами и (или) иным имуществом;

2) *Группа разработки финансовых мер борьбы с отмыванием денег* (далее - ФАТФ) - межправительственная организация (группа), которая занимается выработкой мировых стандартов в сфере противодействия отмыванию преступных доходов и финансированию терроризма, а также осуществляет оценки соответствия национальных систем этим стандартам. Основным инструментом ФАТФ в реализации своего мандата являются рекомендации в сфере противодействия отмыванию преступных доходов и финансированию терроризма, впервые были разработаны в 1990 году;

3) *деловые отношения* – отношения с Клиентами, возникающие в процессе осуществления Банком профессиональной деятельности;

4) *ИПДЛ* – иностранное публичное должностное лицо, назначаемое или избираемое, занимающее какую-либо должность в законодательном, исполнительном, административном или судебном органе иностранного государства, а также любое лицо, выполняющее какую-либо публичную функцию для иностранного государства;

5) *Клиент* – физическое и (или) юридическое лицо, получающее услуги Банка;

6) *легализация (отмывание) доходов, полученных преступным путем* – вовлечение в законный оборот денег и (или) иного имущества, полученного преступным

Продолжение приложения А

путем, посредством совершения сделок, а равно использование указанных денег и (или) иного имущества;

7) **операции с деньгами и (или) иным имуществом** - действия физических и/или юридических лиц с деньгами и/или иным имуществом независимо от формы и способа их осуществления, направленные на установление, изменение или прекращение связанных с ними гражданских прав и обязанностей;

8) **перечень КФМ** - перечень организаций и лиц, связанных с финансированием терроризма и экстремизма, утвержденный Комитетом по финансовому мониторингу Министерства финансов Республики Казахстан (далее – КФМ);

9) **подозрительная операция с деньгами и (или) иным имуществом** (далее – подозрительная операция) – операция клиента (включая попытку совершения такой операции, операцию, находящуюся в процессе совершения или уже совершенную операцию), в отношении которой возникают подозрения о том, что деньги и (или) иное имущество, используемые для ее совершения, являются доходом от преступной деятельности, либо сама операция направлена на легализацию (отмывание) доходов, полученных преступным путем, или финансирование терроризма либо иную преступную деятельность;

9-1) **ПО «AML»** – программное обеспечение «Система финансового мониторинга AML», предназначенное для выявления подлежащих финансовому мониторингу операций из общего числа операций, проводимых в банковских системах, с последующей отправкой в КФМ МФ РК и контролем доставки, возможностью формирования отчетов, а также ведением справочников (стоп-листов);

10) **ПОД и ФТ** – противодействие легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

10-1) **руководитель структурного подразделения** – Директор Департамента/Управления/Филиала Банка или Начальник Отдела/Сектора, и/или лицо, его замещающее;

11) **Уполномоченный орган** – государственный орган Республики Казахстан (далее – РК), осуществляющий финансовый мониторинг и принимающий меры по ПОД и ФТ;

11-1) **физическое присутствие** – место ведения деятельности банка, расположенное по постоянному адресу (кроме адреса почтового ящика или электронного адреса), в котором имеются органы управления и персонал банка, ведутся учет и хранение документов, относящихся к банковской деятельности, и проводятся проверки уполномоченного органа, выдавшего банку-нерезиденту лицензию на осуществление банковской деятельности;

12) **финансовый мониторинг** – совокупность мер по сбору, обработке, анализу и использованию сведений и информации об операциях с деньгами и (или) иным имуществом, осуществляемых уполномоченным органом и Банком;

13) **финансирование терроризма (террористической деятельности)** - предоставление или сбор денег и (или) иного имущества либо оказание финансовых услуг террористам и (или) террористическим организациям для осуществления террористической деятельности;

13-1) **члены семьи** - супруги, родители и дети, связанные имущественными и личными неимущественными правами и обязанностями, вытекающими из брака (супружества), родства, свойства, усыновления (удочерения) или иной формы принятия детей на воспитание.

Примечание: *Иные специфические термины и сокращения, используемые по тексту Политики, используются в соответствии со значением, закрепленном в иных внутренних нормативных документах*

Продолжение приложения А

Банка, а при их отсутствии в иных внутренних нормативных документах Банка - в соответствии со значением, закрепленном в законодательстве РК или принятым в международной банковской практике.

ГЛАВА 2. ЦЕЛИ И ЗАДАЧИ

5. Целью настоящей Политики является защита деловой репутации Банка и недопущение вовлечение Банка в проведение банковских и иных операций Клиентом, связанных с легализацией (отмыванием) доходов, полученных преступным путем, и финансированием терроризма.

6. Основными задачами Политики являются:

1) недопустимость установления деловых отношений и совершение банковских операций с/на анонимным (-ого) Клиентом (-а);

2) предотвращение деловых отношений с Клиентом, в отношении которого имеются подозрения о его причастности к деятельности, связанной с легализацией (отмыванием) доходов, полученных преступным путем, и финансированием терроризма;

3) отказ в установлении деловых отношений/проведении операции, а также прекращение деловых отношений с клиентом в случаях, предусмотренных законодательством РК в области ПОД/ФТ, в т.ч., но, не ограничиваясь:

наличия сведений о Клиенте в перечне КФМ;

если одной стороной/участником операции/сделки или обязательства по сделке является лицо, зарегистрированное/находящееся в стране со значительными рисками отмывания денег и финансирования терроризма, определенной международной организацией или иностранным государством или Уполномоченным органом, либо если в исполнении этой операции/сделки участвует такое лицо;

4) запрет на установление отношений с банками, которые не принимают надлежащих мер для предотвращения легализации (отмывания) доходов, полученных преступным путем, либо не имеют физического присутствия в государствах (территориях), в которых они зарегистрированы в качестве банка и (или) получили лицензию на осуществление банковской деятельности, за исключением нахождения таких банков в прямом или косвенном владении банковского холдинга, подлежащего консолидированному надзору в государстве (территории), в котором они зарегистрированы.

ГЛАВА 3. ОСНОВНЫЕ МЕРОПРИЯТИЯ, ПРЕДПРИНИМАЕМЫЕ БАНКОМ В ЦЕЛЯХ ПРОТИВОДЕЙСТВИЯ ЛЕГАЛИЗАЦИИ (ОТМЫВАНИЮ) ДОХОДОВ, ПОЛУЧЕННЫХ ПРЕСТУПНЫМ ПУТЕМ, И ФИНАНСИРОВАНИЮ ТЕРРОРИЗМА

7. В целях эффективной реализации положений настоящей Политики Банк осуществляет следующие основные мероприятия:

1) надлежащую проверку Клиента и (или) его представителя, бенефициарного собственника;

2) надлежащую проверку ИПДЛ, членов его семьи и близких родственников;

3) установление предполагаемой цели и характера деловых отношений;

4) фиксирование сведений и документов, предоставляемых Клиентом и (или) его представителем;

5) сбор дополнительной информации и сведений о репутации Клиента и (или) его представителя и бенефициарного собственника;

6) мониторинг операций, проводимых Клиентом;

Продолжение приложения А

- 7) взаимодействие с Уполномоченным органом;
- 8) применение эффективных процедур оценки рисков операций Клиента, связанных с легализацией (отмыванием) доходов, полученных преступным путем, и финансированием терроризма;
- 9) соблюдение сохранности сведений, составляющих банковскую, служебную или коммерческую тайну и сохранение режима конфиденциальности информации, получаемой в процессе осуществления внутреннего контроля в целях ПОД и ФТ;
- 10) обновление информации о Клиенте и (или) его представителе, бенефициарном собственнике.

8. Принципы и положения настоящей Политики, а так же нормы Закона о ПОД и ФТ, являются основополагающими при разработке внутренних нормативных документов Банка (далее – ВНД Банка), регламентирующие процессы установления деловых отношений и взаимодействия с Клиентом.

8-1. Доработка автоматизированного банковского программного комплекса и дополнительно приобретенного программного обеспечения осуществляется с учетом необходимости соблюдения требований законодательства РК и ВНД Банка, регламентирующих вопросы ПОД и ФТ.

ГЛАВА 4. ОРГАНИЗАЦИЯ РАБОТЫ И ОТВЕТСТВЕННОСТЬ РАБОТНИКОВ БАНКА ПО ПРОТИВОДЕЙСТВИЮ ЛЕГАЛИЗАЦИИ (ОТМЫВАНИЮ) ДОХОДОВ, ПОЛУЧЕННЫХ ПРЕСТУПНЫМ ПУТЕМ, И ФИНАНСИРОВАНИЮ ТЕРРОРИЗМА В БАНКЕ

9. Главный комплаенс – контролер несет ответственность за организацию построения системы внутреннего контроля по ПОД и ФТ, в соответствии с законодательством РК в области ПОД и ФТ. Департамент комплаенс – контроля (далее – ДК-К), в том числе, но не ограничиваясь:

- 1)разрабатывает и актуализирует правила внутреннего контроля и программы его осуществления;
- 2)разрабатывает в Банке единые требования по соблюдению принципа «Знай своего клиента» для применения в работе всеми работниками Банка;
- 3)представляет отчеты и ответы на запросы Уполномоченного органа, по операциям, подлежащим финансовому мониторингу, в случаях, установленных Законом о ПОД и ФТ;
- 4)информирует Уполномоченный орган об операциях, подлежащих финансовому мониторингу, в случаях, в порядке и в сроки, установленных Законом о ПОД и ФТ;
- 5)проводит учебно-методическую работу с работниками Банка;
- 6)консультируют работников Банка по вопросам, возникающим при реализации программ осуществления внутреннего контроля в целях ПОД и ФТ, в том числе при идентификации и изучении Клиента Банка и оценке риска операций Клиента;
- 7)осуществляет мероприятия по обеспечению возможности использования актуальной версии перечня КФМ в деятельности Банка;
- 7-1)разрабатывает и актуализирует ВНД Банка и организационно-распорядительные документы Банка в области ПОД и ФТ;
- 7-2)разрабатывает и актуализирует сценарии выявления операций, подлежащих финансовому мониторингу в ПО «АМЛ»;
- 7-3)принимает решение, оценивающее операцию как подозрительную.

10. При реализации своих полномочий, работник ДК-К обладает правом доступа к сведениям по Клиенту, включая все без исключения сегменты клиентов, и информации, полученной в результате осуществления требований Закона о ПОД и ФТ и настоящей Политики.

Окончание приложения А

11. При осуществлении своих функций работник ДК-К обязан соблюдать режим конфиденциальности и нераспространение третьим лицам сведений и информации о процедурах, осуществляемых Банком в целях ПОД и ФТ;

12. Все работники Банка, участвующие в установлении деловых отношений с Клиентом, в пределах своей компетенции, осуществляют мониторинг операций Клиента с целью выявления операций, подлежащих финансовому мониторингу в соответствии с Инструкцией «Правила внутреннего контроля в ДБ АО «Сбербанк» в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», утвержденную Правлением Банка 10.07.2013 г., регистрационный № 3186.

13. Руководитель структурного подразделения Центрального офиса несет ответственность за отражение программ внутреннего контроля во внутренних нормативных и иных документах Банка, регламентирующих установление деловых отношений и осуществление операций с деньгами и (или) иным имуществом, подлежащих финансовому мониторингу в соответствии с требованиями настоящей Политики и Инструкции «Правила внутреннего контроля в ДБ АО «Сбербанк» в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» от 10.07.2013г., регистрационный № 3186.

14. Юридическая служба несет ответственность за разработку типовых форм договоров на обслуживание клиентов и организацию работы по фиксации в указанных документах норм, требуемых настоящей Политикой, ВНД Банка в области ПОД и ФТ и законодательству РК.

15. Каждый работник Банка обязан сохранять режим конфиденциальности ставшей ему известной информации о принимаемых конкретных мерах по ПОД и ФТ в отношении конкретного Клиента и его операций. При предоставлении Банком информации в КФМ, Банк не вправе извещать об этом Клиента.

16. Срок хранения Банком документов, идентифицирующих Клиента, документов по операциям, подлежащим обязательному контролю, и по подозрительным операциям не может быть менее 5 (пяти) лет со дня прекращения отношений с Клиентом.

17. Руководитель структурного подразделения несет ответственность за своевременное, полное и качественное выполнение задач и функций структурного подразделения, определенных в настоящей Политике, ВНД и иных документах Банка, регламентирующих процедуры в области ПОД и ФТ.

18. Ответственность за неисполнение и/или ненадлежащее исполнение норм Политики, законодательства РК и ВНД Банка в области ПОД и ФТ несут руководители структурных подразделений/Директоры филиалов Банка.

ГЛАВА 5. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

19. Во всем, что прямо не урегулировано настоящей Политикой ПОД/ФТ необходимо руководствоваться нормами и требованиями законодательства РК и ВНД Банка.

20. Изменения и дополнения в Политику могут быть внесены по мере необходимости, в соответствии с требованиями нормативных правовых актов РК и ВНД Банка, на основании решения Совета Директоров Банка.

21. Если в результате изменения законодательства РК отдельные пункты (нормы) настоящей Политики вступают в противоречие с законодательством, эти пункты (нормы) утрачивают силу и до момента внесения соответствующих изменений в Политику, Банк руководствуется нормативными правовыми актами РК.

Приложение Б

АНКЕТА

Доброго времени суток!

Цель данной анкеты – выявить потребность в обучении специалистов банка, а также ваши предложения по этому поводу. Просим Вас принять участие в анкетировании. Прочитав вопрос, выберите ответ из предложенных вариантов и подчеркните его, или напишите свой на отведенном месте. Анкета анонимная, можно не подписываться, Благодарим за сотрудничество!

1. Пол

- а) мужской
- б) женский

2. Возраст

- а) 18-25
- б) 25-30
- в) 30-40
- г) 40-50
- д) 50 и выше

3. Образование

- а) высшее
- б) неоконченное высшее
- в) среднее специальное
- г) среднее

4. Стаж работы (общий)

- а) менее 5 лет
- б) 5-10 лет
- в) 10-15 лет
- г) 15-20 лет
- д) 20 лет и выше

5. Стаж работы в данной организации

- а) менее 3 лет
- б) 3-5 лет
- в) 5-10 лет
- г) 10-15 лет
- д) 15 лет и выше

6. Стаж работы в должности

- а) до 1 года
- б) до 3-х лет
- в) до 5-ти лет
- г) до 10 лет
- д) свыше 15 лет

7. Категория персонала

- а) руководитель
- б) специалист
- в) помощник
- г) обеспечивающий специалист

8. Как Вы считаете, в процессе трудовой деятельности необходимо проходить обучение?

- а) да, конечно
- б) нет, приобретаемый опыт компенсирует недостаток знаний

Продолжение приложения Б

- в) это зависит от человека, его квалификации и способностей
- г) затрудняюсь ответить
- д) другое _____

9. По Вашему мнению, влияет ли на появление потребности в обучении (можно выбрать несколько вариантов ответа)

- а) сложный характер работы
- б) требования к квалификации
- в) возможность карьерного роста
- г) повышение заработной платы
- д) возможность войти в состав кадрового резерва
- е) появление новых нормативных актов и технологий
- ж) затрудняюсь ответить
- з) другое _____

10. Если обучение необходимо, то с какой периодичностью его следует проводить?

- а) не чаще одного раза в 5 лет
- б) один раз в 3 года
- в) не реже одного раза в год
- г) два раза в год и чаще
- д) затрудняюсь ответить
- е) другое _____

11. На какие стороны профессиональной деятельности, по-Вашему, должно быть направлено обучение специалистов банка?

- а) изучение нормативно-законодательной базы
- б) изучение основ управленческой деятельности
- в) повышение коммуникативной компетентности
- г) развитие познавательных способностей
- д) затрудняюсь ответить
- е) другое _____

12. Как часто Вас посылают на обучение?

- а) регулярно
- б) по необходимости
- в) считают, что в этом нет необходимости

13. Влияет ли обучение, по Вашему мнению, на профессионализм работника?

- а) безусловно, влияет
- б) не влияет
- в) влияет незначительно

14. Какую форму обучения Вы считаете предпочтительной (можно выбрать несколько вариантов ответа)?

- а) повышение квалификации на различных курсах
- б) профессиональная переподготовка в вузе
- в) тематические семинары
- г) тренинги
- д) наставничество
- е) затрудняюсь ответить
- ж) другое _____

15. Кто, на Ваш взгляд, должен проводить обучение?

- а) коллеги, в рамках обмена опытом, и руководитель
- б) специалисты обучающих центров, специализированных курсов
- в) самообразование
- г) затрудняюсь ответить

Окончание приложения Б

е) другое _____

16. Как Вы считаете, от чего зависит успех обучения?

- а) квалификации преподавателей
- б) качества учебных материалов
- в) поддержка руководства
- г) заинтересованности самих обучающихся
- д) не задумывался

17. Испытываете ли Вы необходимость в повышении квалификации?

- а) да
- б) нет
- в) не задумывался

18. Обучение связано с Вашим карьерным ростом?

- а) да
- б) нет
- в) зависит от руководства
- г) не в этой организации

19. Мы бы хотели знать Ваши предложения по поводу обучения (какое обучение, кто должен проводить, с какой периодичностью и т.д.)

Спасибо за ответы!