PRIME LEGAL LLC
Юридическая фирма

125009, Россия, г. Москва, ул. Тверская, 22а.
Тел./факс: +7 (495) 649-87-37

Эл. почта: info@primelegal.ru
Интернет: www.primelegal.ru

Образец правового заключения по вопросам функционирования системы дистанционного банковского обслуживания банка « ххх », подготовленный юристами фирмы PRIME LEGAL.

СОДЕРЖАНИЕ

Введение

Предмет исследования

Оценка документации банка осуществлена применительно к системе ДБО и не включает в себя анализ положений документов, которые непосредственно не связаны с функционированием и использованием системы ДБО. Предметом исследования является сама система ДБО, соблюдение обязательных требований к системе ДБО и легитимность документации, регулирующей ее использование или связанной с таким использованием.

Вместе с тем, в тексте правовой оценки могут встречаться замечания относительно положений документов, которыми не регулируются вопросы функционирования ДБО. Подобные замечания не могут рассматриваться в качестве основного предмета исследования, приводятся для сведения и не могут претендовать на полноту проведенной оценки.

В тексте документа приводятся замечания, при этом двойным нижним подчеркиванием выделены те замечания, которые имеют существенное значение. Остальные замечания не являются существенными, поскольку не влекут серьезных финансовых и правовых рисков для банка.

Правовое регулирование

Системы дистанционного банковского обслуживания должны отвечать требованиям, установленным законодательством РФ. Основным документом, которым устанавливаются требования к системам ДБО, является «Положение о требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» (утв. Банком России 09.06.2012 N 382-П), а также Указание Банка России от 09.06.2012 N 2831-У.

Все остальные документы носят общий характер (например, Федеральный закон от 27.06.2011 N 161-ФЗ «О национальной платежной системе», Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных», Федеральный закон от 02.12.1990 N 395-1 «О банках и банковской деятельности» и т.п.), либо не являются источниками права (например, <Письмо> Банка России от 31.03.2008 N 36-Т «О Рекомендациях по организации управления рисками, возникающими при осуществлении кредитными организациями операций с применением систем Интернет-банкинга», «Методические рекомендации о порядке действий в случае выявления хищения денежных средств в системах дистанционного банковского обслуживания, использующих электронные устройства клиента», <Письмо> Банка России от 26.10.2010 N 141-Т «О Рекомендациях по подходам кредитных организаций к выбору провайдеров и взаимодействию с ними при осуществлении дистанционного банковского обслуживания» и т.п.).

Правовая оценка по своему содержанию основана по большей части, исходя из нормативно-правовых актов, которые носят обязательный характер при использовании систем ДБО и осуществлении банковской или иной деятельности.

ОЦЕНКА ДОКУМЕНТАЦИИ

Общие сведения

Статьей 9 Федерального закона от 27.06.2011 N 161-ФЗ «О национальной платежной системе» определен порядок и условия использования электронных средств платежа (ЭСП). Данной статьей закреплены основные обязанности банка при использовании ЭСП, в частности:

- банк обязан информировать клиента о совершении каждой операции с использованием ЭСП путем направления клиенту соответствующего уведомления в порядке, установленном договором с клиентом (ч. 4 ст. 9).
- банк обязан обеспечить возможность направления ему клиентом уведомления об утрате ЭСП и (или) о его использовании без согласия клиента (ч. 5 ст. 9).
- банк обязан фиксировать направленные клиенту и полученные от клиента уведомления, а также хранить соответствующую информацию не менее 3 лет (ч. 6 ст. 9).
- банк обязан предоставлять клиенту документы и информацию, которые связаны с использованием клиентом его ЭСП, в порядке, установленном договором (ч. 7 ст. 9).

Положения, установленные частями 11 - 15 статьи 9 N 161-ФЗ, сводятся к обязанности банка возместить клиенту сумму операции, совершенной без согласия клиента или в случае нарушения правил информирования клиента об оспоренной операции (транзакции). В частности, данными положениями предусмотрено следующее:

1) Если банк не направлял клиенту уведомления об операциях, он обязан возместить клиенту суммы операций, которые были совершены без согласия клиента (далее также - несанкционированные операции) и о которых клиенту не был проинформирован банком.
2) Если банк надлежащим образом направлял клиенту уведомления об операциях и клиент вовремя представили в банк уведомление о несогласии, банк обязан возместить клиенту суммы несанкционированных операций, совершенных после представления уведомления о несогласии (если уведомление предоставлено в установленный срок).
3) Если банк надлежащим образом направлял клиенту уведомления об операциях и клиент вовремя представили в банк уведомление о несогласии, банк обязан возместить клиенту суммы несанкционированных операций, совершенных до момента представления клиентом указанного уведомления о несогласии, но только в том случае, если не сможет доказать, что клиент сам нарушил порядок использования ЭСП, из-за чего и произошли несанкционированные операции.

В первом и втором случаях банк возмещает клиенту суммы несанкционированных операций вне зависимости от нарушения порядка использования ЭСП. В связи с этим очень важное значение имеет надлежащее уведомление клиента о совершении операций, информирование о сроке направления такого уведомления (уведомление должно быть направлено не позднее дня, следующего за днем совершения операции) и предоставление возможности такого информирования.

Данные положения имеют очень важное практическое значение. В соответствии с пунктом 11 статьи 9 Федерального закона от 27.06.2011 N 161-ФЗ «О национальной платежной системе» в случае утраты электронного средства платежа и (или) его использования без согласия клиента клиент обязан направить соответствующее

уведомление оператору по переводу денежных средств в предусмотренной договором форме незамедлительно после обнаружения факта утраты электронного средства платежа и (или) его использования без согласия клиента, но не позднее дня, следующего за днем получения от оператора по переводу денежных средств уведомления о совершенной операции.

При нарушении срока для предъявления претензии суды отказывают клиенту во взыскании денежных средств с банка, что подтверждается судебной практикой (Апелляционное определение Санкт-Петербургского городского суда от 17.05.2017 N 33-8312/2017 по делу N 2-10633/2016, Апелляционное определение Московского городского суда от 14.04.2017 по делу N 33-6598/2017, Апелляционное определение Санкт-Петербургского городского суда от 22.03.2017 N 33-5814/2017, Апелляционное определение Московского городского суда от 12.01.2017 по делу N 33-230/2017).

Также при использовании системы ДБО необходимо учитывать, что в силу ст. 25 Федерального закона от 27.06.2011 N 161-ФЗ «О национальной платежной системе» банк до заключения договора с физическим лицом обязан предоставить ему информацию:

- о наименовании и месте нахождения банка, номере лицензии;
- об условиях использования ДБО, в том числе в автономном режиме;
- о способах и местах осуществления перевода;
- о способах и местах предоставления денежных средств физическим лицом банку;
- о размере и порядке взимания банком вознаграждения с физического лица (если предусмотрено)
- о способах подачи претензий и порядке их рассмотрения, включая информацию для связи с оператором электронных денежных средств.

Такая информация может размещаться в самой системе ДБО, либо в документах, к которым клиент имеет доступ при работе с системой ДБО.

Условия использования ДБО

Соответствие законодательству и риски:

Условия предоставления услуги Интернет-банк XXX частично не соответствуют законодательству РФ, некоторые положения являются рискованными.

Замечания:

- Некоторые термины, для которых в разделе 1 закреплено обозначение, написаны по-разному: иногда с заглавной буквы, иногда со строчной (например, клиент, регистрация, компрометация и т.д.).
- Не указан порядок принятия условий. Если они принимаются путем подписания, то это нужно прямо указать (например, сделав ссылку на статью 428 Гражданского кодекса РФ (далее – «ГК РФ)). Если речь идет об акцепте, то он может осуществляться в рамках статьи 437 ГК РФ, что также целесообразно отразить в документе. При необходимости можно отразить возможность использования обоих способов одновременно.
- Условиями не определен порядок информирования клиентов об операциях, совершаемых в системе ДБО (в силу ч. 4 ст. 9 N 161-ФЗ договором должен быть определен порядок информирования клиентов о совершаемых в системе ДБО операциях).

- Условиями не определен порядок предоставления документов, связанных с использованием его ЭСП (в силу ч. 7 ст. 9 N 161-ФЗ банк обязан предоставлять клиенту информацию и документы в порядке, определенном договором).
- Не установлен срок для рассмотрения заявлений и претензий клиента, в т.ч. связанных с использованием ЭСП (в силу ч. 8 ст. 9 N 161-ФЗ заявления рассматриваются в сроки, определенные договором, но не позднее 30 дней с момента их поступления, а для трансграничных операций – не позднее 60 дней).
- Условиями не установлены все основания для приостановления или прекращения использования системы ДБО (в силу ч. 9 ст. 9 N 161-ФЗ использование ЭСП может быть прекращено по заявлению клиента или по инициативе банка в случаях, установленных договором).
- В условиях нет информации относительно политики обработки персональных данных, принимаемых оператором мерах по обеспечению безопасности (в силу ст. 18.1 Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных» оператор должен опубликовать на сайте политику обработки персональных данных (далее – «ПД» и разместить ее для постоянного доступа). Политика в качестве отдельного документа на сайте также не размещена.
- Условиями не предусмотрена форма для клиента, предназначенная для уведомления банка об утрате ЭСП или его использовании без согласия клиента (в силу ч. 15 ст. 9 N 161-ФЗ В случае утраты ЭСП и (или) его использования без согласия клиента клиент обязан уведомить банк в предусмотренной договором форме).
- В условиях целесообразно прописать, что днем получения уведомления от банка является день направления соответствующего сообщения по каналам связи, определенным условиями.
- Отсутствует сведения о сроках направления уведомления клиентом об утрате ЭСП или его использовании без согласия клиента осуществляется.
- Нет информации о том, что при переводе средств между счетами клиента, открытыми в банке ХХХ, подтверждение операции кодом подтверждения не требуется (в инструкции указывается, что платеж будет совершен сразу при нажатии на кнопку Подтвердить/Оплатить).
- Не установлена максимальная сумма перевода денежных средств с использованием ДБО за определенный период времени (день, месяц и т.п.) (п. 2.8.3 Положения N 382-П, утв. Банком России 09.06.2012);
- не определен перечень возможных получателей денежных средств, в адрес которых могут быть совершены переводы денежных средств с использованием системы ДБО (п. 2.8.3 Положения N 382-П, утв. Банком России 09.06.2012);
- не определен перечень устройств, с использованием которых может осуществляться доступ к системе ДБО (п. 2.8.3 Положения N 382-П, утв. Банком России 09.06.2012);
- не определен перечень услуг, предоставляемых с использованием системы ДБО (п. 2.8.3 Положения N 382-П, утв. Банком России 09.06.2012);
- не определен временной период, в который могут быть совершены переводы денежных средств с использованием системы Интернет-банкинга (п. 2.8.3 Положения N 382-П, утв. Банком России 09.06.2012);

Рекомендации:

- Привести Условия в единообразную форму, указав только те термины, которые определены в разделе 1 условий. Указывать термины с заглавной буквы.
- Указать порядок одобрения условий в соответствии со статьями 428, 437 ГК РФ в зависимости от способа принятия условий.
- Определить, каким образом клиенты получают информацию об операциях, совершенных в ДБО (например, путем получения смс-сообщений).
- Определить способы и условия предоставления документов, связанных с использованием его ЭСП (например, по электронной почте или в отделениях банка);
- Установить 30-дневный срок для рассмотрения заявлений клиента, в т.ч. связанных с использованием ЭСП (для трансграничных операций –60 дней): «Претензии, связанные с использованием Системы «Интернет - банк « ххх », рассматриваются Банком в 30-дневный срок с момента их поступления (60-дневный срок для трансграничных операций)».
- Указать основания для приостановления или прекращения использования системы ДБО: «Использование Системы «Интернет - банк « ххх » может быть прекращено: по заявлению клиента; при нарушении клиентом условий использования системы ДБО, при несанкционированном доступе и подозрительных операциях, в случае превышения лимитов; иных случаях, предусмотренных законодательством РФ».
- Разместить отдельным документом политику обработки ПД, в которой отразить способы обработки ПД, случаи и основания такой обработки, меры, применяемые для защиты ПД, сроки хранения ПД, а также иную информацию, связанную с обработкой ПД.
- Разработать и сделать приложениям к условиям форму уведомления банка об утрате доступа к ЭСП или в случае его использования без согласия клиента. Кроме того, прямо прописать в условиях, что использование такой формы является обязательным, определить способ и срок ее направления (не позднее 1 дня с момента получения уведомления о совершении несанкционированной операции).
- Добавить в условия пункт следующего содержания: «Уведомление Клиентом об утрате ЭСП или его использовании без согласия клиента осуществляется не позднее дня, следующего за днем наступления указанного события».
- Добавить в условия пункт следующего содержания: «Днем получения любого уведомления от Банка является день направления соответствующего сообщения по каналам связи, определенным условиями».
- Добавить п. 2.14 следующего содержания: «При переводе Клиентом денежных средств между счетами Клиента, открытыми в банке ххх, пароля для подтверждения операции не требуется».
- Добавить раздел 5 и п. 5.1 следующего содержания: «Максимальная сумма перевода денежных средств с использованием Системы «Интернет - банк « ххх » не может превышать сумму, эквивалентную ____________ рублей в день». При необходимости установить лимиты на иные сроки (час, месяц, год и т.п.).
- Добавить п. 5.2 следующего содержания: «Получателями денежных средств, в адрес которых могут быть совершены переводы денежных средств с

использованием Системы «Интернет - банк « ххх » могут быть физические и юридические лица».

- Добавить п. 5.3 следующего содержания: «К устройствам, с использованием которых может осуществляться доступ к Системе «Интернет - банк « ххх », являются: персональные компьютеры, мобильные телефоны, обладающие техническими параметрами, позволяющие использовать Систему «Интернет - банк « ххх ».
- Добавить п. 5.4 следующего содержания: «К услугам, предоставляемых с использованием Системы «Интернет - банк « ххх », относятся: _____».
- Добавить п. 5.5 следующего содержания: «Использование Системы «Интернет - банк « ххх » может осуществляться круглосуточно, использование в автономном режиме не предусмотрено».

Банковский вклад

Договор срочного банковского вклада, Правила размещения физическими лицами банковских вкладов в БАНК « ххх » и Условия привлечения вкладов частично соответствуют законодательству РФ. Правила содержат ссылку на условия предоставления услуги «Интернет - банк ххх» (п. 5.11 правил).

Вместе с тем, рекомендуется в условиях привлечения вкладов добавить отсылку на договор срочного банковского вклада или правила размещения банковских вкладов. Кроме того, правила размещения физическими лицами банковских вкладов в БАНК «ХХХ» подготовлены без учета возможности открытия вклада при помощи системы ДБО, что видно из п. 3.2 правил. В связи с этим рекомендуется добавить п. 3.12 следующего содержания: «Договор банковского вклада может быть заключен с использованием системы «Интернет - банк « ххх » в порядке статьи 428 Гражданского кодекса РФ за счет совершения Вкладчиком конклюдентных действий, направленные на открытие Вклада».

Кредитные карты с лимитом

Индивидуальные условия предоставления кредита по карте с кредитным лимитом и Общие условия договоров кредитования карт с кредитным лимитом БАНК « ххх » частично не соответствуют законодательству РФ, некоторые положения являются рискованными.

Замечания:

- Табличная часть индивидуальных условий не соответствует Указанию Банка России от 23.04.2014 N 3240-У «О табличной форме индивидуальных условий договора потребительского кредита (займа)» (в п. 4 не указаны слова: «или порядок ее (их) определения»). Несмотря на несущественность замечание точное несоответствие табличной части Указанию Банка России N 3240-У может послужить основанием для предъявления претензий со стороны ЦБ РФ.
- Третья страница табличной части не повторяет заголовок (п. 3 Указания).
- ПСК указана в прямоугольной рамке (в силу ст. 6 Федерального закона от 21.12.2013 N 353-ФЗ «О потребительском кредите (займе)» ПСК размещается в квадратной рамке).

- Пунктом 16 индивидуальных условий не определен порядок предоставления информации по операциям при использовании системы ДБО (в силу ч. 7 ст. 9 N 161-ФЗ банк обязан предоставлять клиенту информацию и документы в порядке, определенном договором).
- В общих условиях договоров кредитования отсутствует ссылка на условия предоставления услуги «Интернет - банк ххх».

Рекомендации:

- Пункт 4 табличной части индивидуальных условий изложить в следующей редакции: «Процентная ставка (процентные ставки) (в процентах годовых) или порядок ее (их) определения».
- На третьей странице табличной добавить повторение заголовка в соответствии с п. 3 Указания.
- Указать ПСК в квадратной рамке.
- Указать в п. 16 индивидуальных условий порядок предоставления информации по операциям при использовании системы ДБО.
- Общие условия договоров кредитования необходимо дополнить пунктом 7.6 следующего содержания: «Порядок и условия использования ДБО определяется Условиями предоставления услуги «Интернет - банк ххх», утверждаемыми Банком».
- Добавить пункт следующего содержания: «Договор может быть заключен с использованием системы «Интернет - банк «ххх» в порядке статьи 428 Гражданского кодекса РФ за счет совершения Заемщиком конклюдентных действий, направленные на получение кредита».

Банковские карты

Условия пользования банковскими картами БАНК «ххх» частично не соответствуют законодательству РФ, некоторые положения являются рискованными.

Замечания:

- В п. 9.4 указано, что для получения Выписок Клиент может воспользоваться услугой ДБО (после оформления соответствующего заявления на ДБО). Возможно, данный пункт входит в противоречие с условиями использования ДБО, поскольку в Условиях предоставления услуги «Интернет - банк ххх» ничего не говориться о необходимости написания заявления.
- В общих условиях пользования банковскими картами отсутствует ссылка на условия предоставления услуги «Интернет - банк ххх».

Рекомендации:

- Устранить противоречие, содержащееся в п. 9.4 (либо указать в Условиях предоставления услуги «Интернет - банк ххх» на необходимость написания заявления, либо в п. 9.4 убрать: (после оформления соответствующего заявления на ДБО).
- Общие условия пользования банковскими картами необходимо дополнить пунктом 9.9 следующего содержания: «Порядок и условия использования ДБО определяется

Условиями предоставления услуги «Интернет - банк ххх», утверждаемыми Банком».

Договор потребительского кредита

Индивидуальные и общие условия договора потребительского кредита частично не соответствуют законодательству РФ, некоторые положения являются рискованными.

Замечания:

- Пункт 4 табличной части индивидуальных условий изложить в следующей редакции: «Процентная ставка (процентные ставки) (в процентах годовых) или порядок ее (их) определения».
- ПСК указана в прямоугольной рамке (в силу ст. 6 Федерального закона от 21.12.2013 N 353-ФЗ «О потребительском кредите (займе)» ПСК размещается в квадратной рамке).
- Пунктом 16 индивидуальных условий не определен порядок предоставления информации по операциям при использовании системы ДБО (в силу ч. 7 ст. 9 N 161-ФЗ банк обязан предоставлять клиенту информацию и документы в порядке, определенном договором). Если использование системы ДБО предполагается, то необходимо прямо указать, что способы информирования при использовании системы ДБО, если они отличаются от приведенных.
- В общих условиях договора потребительского кредита отсутствует ссылка на условия предоставления услуги «Интернет - банк ххх».

Рекомендации:

- Пункт 4 табличной части индивидуальных условий изложить в следующей редакции: «Процентная ставка (процентные ставки) (в процентах годовых) или порядок ее (их) определения».
- Указать ПСК в квадратной рамке.
- Указать в п. 16 индивидуальных условий порядок предоставления информации по операциям при использовании системы ДБО.
- Общие условия потребительского кредита необходимо дополнить пунктом 6.7 следующего содержания: «В случае применения сторонами системы дистанционного банковского обслуживания Заемщик обязуется соблюдать Условиями предоставления услуги «Интернет - банк ххх», утвержденные Банком».
- Добавить пункт следующего содержания: «Договор может быть заключен с использованием системы «Интернет - банк « ххх » в порядке статьи 428 Гражданского кодекса РФ за счет совершения Заемщиком конклюдентных действий, направленные на получение кредита».

Руководство клиента

Руководство клиента по использованию системы «Интернет - банк « ххх » соответствуют законодательству РФ, некоторые положения являются рискованными, однако имеет некоторые неточности, связанные с описанием системы ДБО.

Замечания:

- На странице 19 руководства указан порядок перехода по страницам: «Платежи и переводы - История операций». В действительности «история платежей» в ДБО названа «история операций».
- На странице 26 руководства указано, что вкладка называется «Переводы и платежи». В действительности в ДБО она называется «Платежи и переводы».
- На странице 28 руководства, видимо, пропущено слово «выбрать» в следующем предложении: «В результате появится страница, на которой необходимо будет счет списания, с которого будет произведена оплата, сумму платежа и нажать кнопку далее…».
- На страницах 29, 31, 32, 33, 34, 35, 36, 37, 39, 40, 41 руководства указывается на необходимость нажатия кнопки «Оплатить». В действительности в ДБО указана кнопка «Перевести».
- На странице 58 руководства указано, что плата за приостановление действия карты в соответствии с тарифами Банка не взимается. Вместе с тем, в предыдущем абзаце этого речь идет о блокировке карты. Если речь идет об одном и том же действии, то данная информация противоречит вышеприведенной, где указывается о взимании платы за блокировку. Если же приостановление представляет собой отдельную операцию, то о ней можно ничего не говорить, поскольку такая функция в ДБО отсутствует.
- На странице 66 опечатка: «Снять денежный средства Вы сможете с учетом доступной суммы к снятию».

Рекомендации:

Устранить замечания, указанные выше.

ОЦЕНКА ДБО И ПРОЦЕССОВ

Защита информации

Документом, которым установлены критерии защиты информации ДБО, является Положение о требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств (далее – «Положение»).

Из п. 2.15.1 данного Положения следует, что банк обеспечивает проведение оценки выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств (далее – «оценка соответствия»). Такая оценка осуществляется банком самостоятельно или с привлечением сторонних организаций не реже 1 раза в 2 года, либо по требованию ЦБ РФ.

Организация, ставшая оператором по переводу денежных средств, оператором платежной системы, оператором услуг платежной инфраструктуры, должна провести первую оценку соответствия в течение шести месяцев после получения соответствующего статуса. Порядок проведения оценки системы ДБО и документирования результатов определен в приложении 1 к Положению.

Требований очень много, для наглядности можно привести некоторые из них:

N	Номер пункта	Оператор обеспечивает
П.2	2.4.1	регистрацию лиц, обладающих правами по управлению криптографическими ключами
П.3	2.4.1	регистрацию лиц, обладающих правами по воздействию на объекты информационной инфраструктуры, которое может привести к нарушению предоставления услуг по осуществлению переводов денежных средств, за исключением банкоматов, платежных терминалов и электронных средств платежа
П.4	2.4.1	регистрацию своих работников, обладающих правами по формированию электронных сообщений
П.5	2.4.2	реализацию запрета выполнения одним лицом в один момент времени ролей, связанных с созданием (модернизацией) объекта информационной инфраструктуры и эксплуатацией объекта информационной инфраструктуры
П.8	2.5.1	включение в технические задания на создание (модернизацию) объектов информационной инфраструктуры требований к обеспечению защиты информации при осуществлении переводов денежных средств
П.11	2.5.4	наличие эксплуатационной документации на используемые технические средства защиты информации
П.13	2.5.4	восстановление функционирования технических средств защиты информации, используемых при осуществлении переводов денежных средств, в случаях сбоев и (или) отказов в их работе
П.16	2.5.6	защиту резервных копий защищаемой информации
П.20	2.6.2	применение некриптографических средств защиты информации от несанкционированного доступа, в том числе прошедших в установленном порядке процедуру оценки соответствия
П.29.1	2.6.3	При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных в подпункте 2.6.1 пункта 2.6 настоящего Положения, оператор по переводу денежных средств, банковский платежный агент (субагент) обеспечивает регистрацию следующей информации о действиях клиентов, выполняемых с использованием автоматизированной системы, программного обеспечения: дата (день, месяц, год) и время (часы, минуты, секунды) осуществления действия клиента; идентификатор клиента; код, соответствующий выполняемому действию; идентификатор устройства
П.57.7	2.8.6	при распространении систем мобильного банкинга с использованием репозиториев осуществляет размещение установочных файлов системы мобильного банкинга в репозитории с указанием в качестве разработчика данной системы оператора по переводу денежных средств либо уполномоченного им разработчика (при этом оператор по переводу денежных средств обеспечивает информирование клиентов об уполномоченных им разработчиках по каналу, альтернативному репозиторию)

Как мы видим, некоторые из требований носят технический характер. В связи с этим такую оценку можно провести только совместно с разработчиками программного обеспечения и системным администратором ДБО.

При проведении оценки осуществляется подсчет количественных показателей $EV1_{пс}$ и $EV1_{пс}$. Затем считается общий показатель $R_{пс}$ путем суммирования $EV1_{пс}$ и $EV1_{пс}$. По результатам полученного показателя оценивается его значение и делается вывод о защите системы ДБО. Причем некоторые из показателей должны были учитываться на этапе формирования технического задания по созданию системы ДБО.

Показатель $R_{пс}$	**Значение показателя**
0,85 и выше	Защита обеспечена (хорошая)
0,70-0,85 и выше	Защита в целом обеспечена (удовлетворительная)
0,5 до 0,7 и выше	Защита обеспечена не в полной мере (удовлетворительная)
меньше 0,5	Защита не обеспечена не в полной мере (неудовлетворительная)

Рекомендации.

Большинство требований носят юридический характер и могут быть выполнены банком путем формирования необходимой документации. К ним можно отнести:

N	Формулировка требования	Как реализовать
П.8	Оператор обеспечивает включение в технические задания на создание (модернизацию) объектов информационной инфраструктуры требований к обеспечению защиты информации при осуществлении переводов денежных средств	Проверить ТЗ к договору на создание ДБО (в нем должны быть требования к обеспечению защиты информации). При необходимости внести правки в ТЗ.
П.9	Оператор обеспечивает участие службы информационной безопасности в разработке и согласовании технических заданий на создание (модернизацию) объектов информационной инфраструктуры	Поставить резолюцию службы безопасности на ТЗ.
П.10	Оператор обеспечивает контроль со стороны службы информационной безопасности соответствия создаваемых (модернизируемых) объектов информационной инфраструктуры требованиям технических заданий	Добавить в положение о службе безопасности о необходимости контроля за созданием ДБО
П.11	Оператор обеспечивает наличие эксплуатационной документации на используемые технические средства защиты информации	Иметь и хранить документацию на ДБО
П.12	Оператор обеспечивает контроль выполнения требований эксплуатационной документации на используемые технические средства защиты информации в течение всего срока их эксплуатации	Назначить лиц, ответственных за контроль выполнения требований документации на ДБО. Указать на такую обязанность в положении о технической поддержке ДБО (далее – «положение о ДБО»).
П.13	Оператор обеспечивает восстановление функционирования технических средств защиты информации, используемых при осуществлении переводов денежных средств, в случаях сбоев и (или) отказов в их работе	Включить данное условие в положение о ДБО, назначить ответственных лиц.
П.14	Оператор обеспечивает реализацию запрета использования защищаемой информации на стадии создания объектов информационной инфраструктуры	Приказом довести данную информацию до сведения программистов.
П.17	Оператор на стадиях эксплуатации и снятия с эксплуатации объектов информационной инфраструктуры обеспечивает уничтожение защищаемой информации в случаях, когда указанная информация больше не используется, за исключением защищаемой информации, перемещенной в архивы, ведение и сохранность которых предусмотрены законодательными актами Российской Федерации, нормативными актами Банка России, правилами платежной системы и (или) договорами, заключенными оператором по переводу денежных средств, банковским платежным агентом (субагентом), оператором платежной системы, оператором услуг платежной инфраструктуры	Приказом довести данную информацию до сведения программистов, назначить ответственных лиц.
П.18	Оператор на стадиях эксплуатации и снятия с эксплуатации объектов информационной инфраструктуры обеспечивает уничтожение защищаемой информации, в том числе содержащейся в архивах, способом, обеспечивающим невозможность ее восстановления	Приказом довести данную информацию до сведения программистов, назначить ответственных лиц.
П.18.3	В случае если программное обеспечение, используемое клиентом при осуществлении переводов денежных средств, разрабатывалось оператором по переводу денежных средств самостоятельно	Включить данное условие в положение о ДБО, назначить ответственных лиц.

	или с привлечением сторонних организаций: оператор по переводу денежных средств обеспечивает распространение изменений, вносимых в указанное программное обеспечение, направленных на устранение ставших известными оператору по переводу денежных средств уязвимостей указанного программного обеспечения; оператор по переводу денежных средств определяет являющиеся актуальными версии указанного программного обеспечения и обеспечивает контроль использования клиентом актуальных версий указанного программного обеспечения	
П.18.4	В случае распространения программного обеспечения, используемого клиентом при осуществлении переводов денежных средств, оператор по переводу денежных средств доводит до клиента инструкцию по эксплуатации (эксплуатационную документацию) данного программного обеспечения и информацию об условиях его эксплуатации либо указывает общедоступный ресурс, с использованием которого клиент имеет возможность получить указанную инструкцию (эксплуатационную документацию) и информацию об условиях эксплуатации данного программного обеспечения	Разместить на сайте инструкцию по эксплуатации ДБО
П.18.5	В случае распространения изменений программного обеспечения, используемого клиентом при осуществлении переводов денежных средств, оператор по переводу денежных средств вносит соответствующие им изменения в инструкцию по эксплуатации (эксплуатационную документацию) данного программного обеспечения	Включить данное условие в положение о ДБО, назначить ответственных лиц.
П.18.6	Оператор по переводу денежных средств регламентирует и контролирует внесение изменений в программное обеспечение, средства вычислительной техники в составе объектов информационной инфраструктуры, а также в программное обеспечение, используемое клиентом при осуществлении переводов денежных средств; при этом в обязательном порядке должны вноситься изменения, направленные на устранение ставших известными оператору по переводу денежных средств уязвимостей программного обеспечения, средств вычислительной техники	Включить данное условие в положение о ДБО, назначить ответственных лиц.
П.19	Оператор обеспечивает учет объектов информационной инфраструктуры, используемых для обработки, хранения и (или) передачи защищаемой информации, в том числе банкоматов и платежных терминалов	Создать и вести журнал учета банкоматов, терминалов и иных объектов информационной инфраструктуры
П.23	При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных в подпункте 2.6.1 пункта 2.6 настоящего Положения, Оператор обеспечивает определение порядка использования информации, необходимой для выполнения аутентификации	Включить данное условие в положение о ДБО, назначить ответственных лиц.
П.29.2	Оператор по переводу денежных средств обеспечивает хранение информации, указанной в абзацах тринадцатом - шестнадцатом подпункта 2.6.3 пункта 2.6 настоящего Положения, не менее пяти лет, начиная с даты осуществления клиентом действия, выполняемого с использованием автоматизированной системы, программного обеспечения	Включить данное условие в положение о ДБО, назначить ответственных лиц.
П.29.3	Оператор по переводу денежных средств определяет во внутренних документах: порядок формирования уникального идентификатора клиента в автоматизированной системе, программном обеспечении; перечень кодов действий клиентов, выполняемых при осуществлении переводов денежных средств с использованием автоматизированной системы, программного обеспечения; подлежащий регистрации идентификатор устройства; порядок регистрации и хранения информации, указанной в абзацах тринадцатом - шестнадцатом подпункта 2.6.3 пункта 2.6 настоящего Положения	Включить данное условие в положение о ДБО, определить порядок формирования УИК, кодов, ИД, назначить ответственных лиц.
П.29.4	Оператор по переводу денежных средств определяет требования к порядку, форме и срокам передачи ему информации о действиях клиентов, выполняемых с использованием автоматизированных систем, программного обеспечения, регистрируемой банковскими платежными агентами (субагентами)	Определить в положении о ДБО порядок, форму и срок передачи информации о действиях клиентов.
П.33	Оператор принимает и фиксируют во внутренних документах решения о необходимости применения организационных мер защиты информации и (или) использования технических средств защиты информации, предназначенных для контроля физического доступа к объектам информационной инфраструктуры (за исключением банкоматов, платежных терминалов и электронных средств платежа), сбои и (или) отказы в работе которых приводят к невозможности предоставления услуг по переводу денежных средств или к несвоевременности осуществления переводов денежных средств, а также доступа в здания и помещения, в которых они размещаются	Определить в положении о ДБО необходимость применения мер защиты информации и технических средств, предназначенных для контроля физического доступа к объектам информационной инфраструктуры.
П.34	Оператор принимает и фиксируют во внутренних документах решения о необходимости применения организационных мер защиты информации и (или) использования технических средств защиты информации, предназначенных для предотвращения физического воздействия на средства вычислительной техники и телекоммуникационное оборудование, сбои и (или) отказы в работе которых приводят к невозможности предоставления услуг по переводу денежных средств или к несвоевременности осуществления переводов денежных средств, за исключением банкоматов, платежных терминалов и электронных средств платежа	Определить в положении о ДБО необходимость применения мер защиты информации и технических средств, предназначенных для предотвращения физического воздействия на оборудование и ВТ.
П.35	Оператор принимает и фиксируют во внутренних документах решения о необходимости применения организационных мер защиты информации и (или) использования технических	Определить в положении о ДБО необходимость принятия

	средств защиты информации, предназначенных для регистрации доступа к банкоматам, в том числе с использованием систем видеонаблюдения	организационных мер защиты информации, предназначенной для доступа к банкоматам и системам видеонаблюдения, назначить ответственных лиц.
П.38	Оператор обеспечивает принятие мер, направленных на предотвращение хищений носителей защищаемой информации	Определить в положении о ДБО необходимость принятия мер по предотвращению хищения носителей информации, назначить ответственных лиц.
П.41	Оператор обеспечивает регулярное обновление версий технических средств защиты информации от воздействия вредоносного кода и баз данных, используемых в работе технических средств защиты информации от воздействия вредоносного кода и содержащих описание вредоносных кодов и способы их обезвреживания	Определить в положении о ДБО необходимость обновления ДБО, назначить ответственных лиц.
П.43	Оператор по переводу денежных средств обеспечивает формирование для клиентов рекомендаций по защите информации от воздействия вредоносного кода	Определить в положении о ДБО необходимость доведения до сведения клиентов информации по безопасности (в части защиты от воздействия вредоносного кода) и последующей актуализации данной и информации, назначить ответственных лиц.
П.48	В случае обнаружения вредоносного кода или факта воздействия вредоносного кода оператор по переводу денежных средств, банковский платежный агент (субагент), Оператор услуг платежной инфраструктуры обеспечивает принятие мер, направленных на устранение последствий воздействия вредоносного кода	Определить в положении о ДБО порядок действий при обнаружении вредоносного кода, назначить ответственных лиц.
П.50	В случае обнаружения вредоносного кода или факта воздействия вредоносного кода Оператор обеспечивает информирование оператора платежной системы	Определить в положении о ДБО порядок действий при обнаружении вредоносного кода, назначить ответственных лиц.
П.51	В случае обнаружения вредоносного кода или факта воздействия вредоносного кода оператор платежной системы обеспечивает информирование операторов услуг платежной инфраструктуры и участников платежной системы	Определить в положении о ДБО порядок действий при обнаружении вредоносного кода, назначить ответственных лиц.
П.52	При использовании сети "Интернет" для осуществления переводов денежных средств Оператор обеспечивает применение организационных мер защиты информации и (или) использование технических средств защиты информации, предназначенных для предотвращения несанкционированного доступа к защищаемой информации, передаваемой по сети "Интернет"	Включить данное условие в положение о ДБО, назначить ответственных лиц.
П.53	При использовании сети "Интернет" для осуществления переводов денежных средств Оператор обеспечивает применение организационных мер защиты информации и (или) использование технических средств защиты информации, предназначенных для предотвращения несанкционированного доступа к защищаемой информации на объектах информационной инфраструктуры с использованием сети "Интернет"	Включить данное условие в положение о ДБО, назначить ответственных лиц.
П.54	При использовании сети "Интернет" для осуществления переводов денежных средств Оператор обеспечивает применение организационных мер защиты информации и (или) использование технических средств защиты информации, предназначенных для предотвращения несанкционированного доступа к защищаемой информации путем использования уязвимостей программного обеспечения	Включить данное условие в положение о ДБО, назначить ответственных лиц.
П.55	При использовании сети "Интернет" для осуществления переводов денежных средств Оператор обеспечивает минимизацию негативных последствий, связанных с несвоевременностью осуществления переводов денежных средств, сбоями или отказами в работе объекта информационной инфраструктуры	Включить данное условие в положение о ДБО, назначить ответственных лиц.
П.57.1	Оператор по переводу денежных средств принимает и фиксирует во внутренних документах решения о необходимости использования пароля многоразового действия и одноразового кода подтверждения в целях аутентификации клиента при осуществлении переводов денежных средств с использованием системы Интернет-банкинга, а также при подтверждении клиентом права доступа к системе Интернет-банкинга	Определить в положении о ДБО необходимость использования многоразовых и одноразовых кодов подтверждения.
П.57.2	В случае принятия решения о необходимости использования одноразового кода подтверждения в целях аутентификации клиента при осуществлении переводов денежных средств с использованием системы Интернет-банкинга, а также при подтверждении клиентом права доступа к системе Интернет-банкинга, оператор по переводу денежных средств формирует и доводит до клиента информацию, необходимую для генерации одноразового кода подтверждения, или одноразовый код подтверждения, который: действителен на протяжении ограниченного периода времени, установленного оператором по переводу денежных средств; используется для подтверждения клиентом права доступа к системе Интернет-банкинга или для подтверждения распоряжения (нескольких распоряжений) о разовом переводе (разовых	Довести до сведения клиента информацию о действительности паролей в ДБО.

	переводах) денежных средств или распоряжения (договора) о периодических переводах денежных средств в определенную дату и (или) период, при наступлении определенных распоряжением (договором) условий; однозначно соответствует сеансу использования системы Интернет-банкинга или распоряжению (распоряжениям, договору), подтверждаемому (подтверждаемым) клиентом с использованием системы Интернет-банкинга; доводится до клиента по альтернативному системе Интернет-банкинга каналу связи, или входит в набор возможных одноразовых кодов подтверждения, который доводится до клиента оператором по переводу денежных средств на материальном носителе, или создается клиентом с использованием технического средства, предназначенного для генерации одноразовых кодов подтверждения	
П.57.3	Оператор по переводу денежных средств принимает и фиксирует во внутренних документах решения о необходимости направления клиенту по альтернативному системе Интернет-банкинга каналу связи сообщения, содержащего сведения о сформированном с использованием системы Интернет-банкинга распоряжении о переводе денежных средств, включая сумму и получателя денежных средств, до подтверждения клиентом указанного распоряжения с использованием одноразового кода подтверждения	Определить в положении о ДБО необходимость направления клиенту сообщений, содержащих сведения о распоряжении на перевод денежных средств, созданном при помощи ДБО.
П.57.4	Оператор по переводу денежных средств на основании заявления клиента, переданного способом, определенным договором оператора по переводу денежных средств с клиентом, определяет параметры операций, которые могут осуществляться клиентом с использованием системы Интернет-банкинга, в том числе устанавливает: максимальную сумму перевода денежных средств с использованием системы Интернет-банкинга за одну операцию и (или) за определенный период времени (например, один день, один месяц); перечень возможных получателей денежных средств, в адрес которых могут быть совершены переводы денежных средств с использованием системы Интернет-банкинга; перечень устройств, с использованием которых может осуществляться доступ к системе Интернет-банкинга с целью осуществления переводов денежных средств, на основе идентификаторов указанных устройств; перечень услуг, предоставляемых с использованием системы Интернет-банкинга; временной период, в который могут быть совершены переводы денежных средств с использованием системы Интернет-банкинга	Включить данное условие в положение о ДБО. Внести изменения в Условия предоставления услуги Интернет-банк ххх.
П.57.10	Оператор по переводу денежных средств обеспечивает приостановление пересылки клиенту извещений (подтверждений) о принятии к исполнению распоряжений и иной защищаемой информации и осуществления перевода денежных средств на основании сообщений (кодов), отправленных с номера телефона, указанного в договоре с клиентом, в случае если оператору по переводу денежных средств стало известно о признаках, указывающих на изменение: получателя информации, направленной оператором по переводу денежных средств и используемой при аутентификации клиента; отправителя сообщений (кодов) с номера телефона, указанного в договоре с клиентом, на основании которых осуществляется перевод денежных средств. К указанным признакам может быть отнесена информация о замене SIM-карты клиента, прекращении обслуживания или смене номера телефона, указанного в договоре с клиентом	Включить данное условие в положение о ДБО, назначить ответственных лиц.
П.63	В случае применения СКЗИ Оператор определяет во внутренних документах и выполняет порядок применения СКЗИ, включающий порядок ввода в действие, включая процедуры встраивания СКЗИ в автоматизированные системы, используемые для осуществления переводов денежных средств	Определить в положении о ДБО порядок применения и использования СКЗИ.
П.64	В случае применения СКЗИ Оператор определяет во внутренних документах и выполняет порядок применения СКЗИ, включающий порядок эксплуатации СКЗИ	Определить в положении о ДБО порядок эксплуатации СКЗИ.
П.65	В случае применения СКЗИ Оператор определяет во внутренних документах и выполняет порядок применения СКЗИ, включающий порядок восстановления работоспособности СКЗИ в случаях сбоев и (или) отказов в их работе	Определить в положении о ДБО порядок восстановления работоспособности СКЗИ.
П.66	В случае применения СКЗИ Оператор определяет во внутренних документах и выполняет порядок применения СКЗИ, включающий порядок внесения изменений в программное обеспечение СКЗИ и техническую документацию на СКЗИ	Определить в положении о ДБО порядок внесения изменений в программное обеспечение СКЗИ.
П.67	В случае применения СКЗИ Оператор определяет во внутренних документах и выполняет порядок применения СКЗИ, включающий порядок снятия с эксплуатации СКЗИ	Определить в положении о ДБО порядок снятия с эксплуатации СКЗИ
П.68	В случае применения СКЗИ Оператор определяет во внутренних документах и выполняет порядок применения СКЗИ, включающий порядок управления ключевой системой	Определить в положении о ДБО порядок управления ключевой системой
П.69	В случае применения СКЗИ Оператор определяет во внутренних документах и выполняет порядок применения СКЗИ, включающий порядок обращения с носителями криптографических ключей, включая порядок применения организационных мер защиты информации и использования технических средств защиты информации, предназначенных для предотвращения несанкционированного использования криптографических ключей, и порядок действий при смене и компрометации ключей	Определить в положении о ДБО порядок обращения с носителями криптографических ключей

П.70	Оператор платежной системы определяет необходимость использования СКЗИ, если иное не предусмотрено федеральными законами и иными нормативными правовыми актами Российской Федерации	Определить в положении о ДБО необходимость применения СКЗИ
П.71	Оператор обеспечивает учет и контроль состава установленного и (или) используемого на средствах вычислительной техники программного обеспечения	Определить в положении о ДБО необходимость учета и контроля, назначить ответственных лиц.
П.72	Оператор платежной системы определяет порядок применения организационных мер защиты информации и (или) использования технических средств защиты информации, используемых при проведении операций обмена электронными сообщениями и другой информацией при осуществлении переводов денежных средств	Включить данное условие в положение о ДБО.
П.76	При эксплуатации объектов информационной инфраструктуры Оператор обеспечивает контроль (мониторинг) соблюдения установленной технологии подготовки, обработки, передачи и хранения электронных сообщений и защищаемой информации на объектах информационной инфраструктуры	Включить данное условие в положение о ДБО, назначить ответственных лиц.
П.81	При эксплуатации объектов информационной инфраструктуры Оператор обеспечивает выявление фальсифицированных электронных сообщений, в том числе имитацию третьими лицами действий клиентов при использовании электронных средств платежа, и осуществление операций, связанных с осуществлением переводов денежных средств, злоумышленником от имени авторизованного клиента (подмена авторизованного клиента) после выполнения процедуры авторизации	Включить данное условие в положение о ДБО, назначить ответственных лиц.
П.82	Оператор обеспечивает формирование службы информационной безопасности, а также определяет во внутренних документах цели и задачи деятельности этой службы	Включить данное условие в положение о ДБО. Сформировать службу безопасности, назначить ответственных лиц по контролю и мониторингу за ДБО.
П.83	Оператор предоставляет полномочия и выделяют ресурсы, необходимые для выполнения службой информационной безопасности установленных целей и задач	Включить данное условие в положение о ДБО.
П.84	Оператор назначают куратора службы информационной безопасности из состава своего органа управления и определяет его полномочия	Назначить куратора СБ
П.85	Служба информационной безопасности и служба информатизации (автоматизации) не должны иметь общего куратора	Назначить разных кураторов в СБ и СИ
П.86	Оператор по переводу денежных средств, имеющий филиалы, обеспечивает формирование служб информационной безопасности в указанных филиалах, определяет для них необходимые полномочия и выделяет необходимые ресурсы	Включить данное условие в положение о ДБО. Сформировать службу безопасности, назначить ответственных лиц по контролю и мониторингу за ДБО в каждом филиале.
П.87	Оператор по переводу денежных средств, имеющий филиалы, обеспечивает взаимодействие и координацию работ служб информационной безопасности	Обеспечить взаимодействие СБ и СИ
П.88	Служба информационной безопасности осуществляет планирование и контроль обеспечения защиты информации при осуществлении переводов денежных средств, для чего наделяется полномочиями осуществлять контроль (мониторинг) выполнения порядка обеспечения защиты информации при осуществлении переводов денежных средств	Включить данное условие в положение о ДБО.
П.89	Служба информационной безопасности осуществляет планирование и контроль обеспечения защиты информации при осуществлении переводов денежных средств, для чего наделяется полномочиями определять требования к техническим средствам защиты информации и организационным мерам защиты информации	Включить данное условие в положение о ДБО.
П.90	Служба информационной безопасности осуществляет планирование и контроль обеспечения защиты информации при осуществлении переводов денежных средств, для чего наделяется полномочиями контролировать выполнение работниками требований к обеспечению защиты информации при осуществлении переводов денежных средств	Включить данное условие в положение о ДБО.
П.91	Служба информационной безопасности осуществляет планирование и контроль обеспечения защиты информации при осуществлении переводов денежных средств, для чего наделяется полномочиями участвовать в разбирательствах инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, и предлагать применение дисциплинарных взысканий, а также направлять предложения по совершенствованию защиты информации	Включить данное условие в положение о ДБО.
П.92	Служба информационной безопасности осуществляет планирование и контроль обеспечения защиты информации при осуществлении переводов денежных средств, для чего наделяется полномочиями участвовать в действиях, связанных с выполнением требований к обеспечению защиты информации при осуществлении переводов денежных средств, применяемых при восстановлении предоставления услуг платежной системы после сбоев и отказов в работе	Включить данное условие в положение о ДБО.

	объектов информационной инфраструктуры	
П.93	Оператор обеспечивает повышение осведомленности работников в области обеспечения защиты информации по порядку применения организационных мер защиты информации	Включить данное условие в положение о ДБО, приказом ознакомить работников с положением о ДБО, информировать лиц, связанных с ДБО, об изменении мер защиты информации.
П.94	Оператор обеспечивает повышение осведомленности работников в области обеспечения защиты информации по порядку использования технических средств защиты информации	Включить данное условие в положение о ДБО, назначить ответственных лиц.
П.95	Оператор обеспечивает повышение осведомленности работников, получивших новую роль, связанную с применением организационных мер защиты информации или использованием технических средств защиты информации	Включить данное условие в положение о ДБО, назначить ответственных лиц.
П.96	Оператор по переводу денежных средств обеспечивает доведение до клиентов информации о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами, и рекомендуемых мерах по их снижению, в том числе информации о: рекомендуемых мерах по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) устройства, с использованием которого клиентом осуществлялся перевод денежных средств; рекомендуемых мерах по контролю конфигурации устройства, с использованием которого клиентом осуществляется перевод денежных средств, и своевременному обнаружению воздействия вредоносного кода; появлении в сети "Интернет" ложных (фальсифицированных) ресурсов и программного обеспечения, имитирующих программный интерфейс используемых оператором по переводу денежных средств систем Интернет-банкинга, и (или) использующих зарегистрированные товарные знаки и наименование оператора по переводу денежных средств, и рекомендуемых мерах по обнаружению указанных ресурсов и программного обеспечения	Включить данное условие в положение о ДБО, назначить ответственных лиц. Добавить соответствующую информацию на сайте.
П.97	Оператор платежной системы определяет требования к порядку, форме и срокам информирования о выявленных в платежной системе инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств	Включить данное условие в положение о ДБО, назначить ответственных лиц.
П.98	Информирование оператора платежной системы о выявленных инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, осуществляется ежемесячно	Включить данное условие в положение о ДБО, назначить ответственных лиц.
П.99	Оператор платежной системы определяет требования к взаимодействию оператора платежной системы, операторов по переводу денежных средств и операторов услуг платежной инфраструктуры в случае выявления в платежной системе инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств	Определить в положении о ДБО порядок действий при выявлении инцидентов, связанных с нарушением информационной безопасности.
П.101	Оператор обеспечивает применение организационных мер защиты информации и (или) использование технических средств защиты информации, предназначенных для выявления инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств	Включить данное условие в положение о ДБО, назначить ответственных лиц.
П.102	Оператор обеспечивает информирование службы информационной безопасности, в случае ее наличия, о выявлении инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств	Включить данное условие в положение о ДБО.
П.103	Оператор обеспечивает реагирование на выявленные инциденты, связанные с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств	Включить данное условие в положение о ДБО, назначить ответственных лиц.
П.104	Оператор обеспечивает анализ причин выявленных инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, проведение оценки результатов реагирования на такие инциденты	Включить данное условие в положение о ДБО, назначить ответственных лиц.
П.105	Оператор платежной системы обеспечивает учет и доступность информации о выявленных в платежной системе инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств	Включить данное условие в положение о ДБО, обеспечить доступность, назначить ответственных лиц.
П.106	Оператор платежной системы обеспечивает учет и доступность информации о методиках анализа и реагирования на инциденты, связанные с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств	Включить данное условие в положение о ДБО, обеспечить доступность, назначить ответственных лиц.
П.106. 1	Оператор обеспечивает регистрацию самостоятельно выявленных инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств.	Включить данное условие в положение о ДБО, обеспечить регистрацию инцидентов, назначить ответственных

	Оператор по переводу денежных средств обеспечивает регистрацию ставших ему известными инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств, выявленных клиентами данного оператора по переводу денежных средств. Оператор по переводу денежных средств обеспечивает регистрацию ставших ему известными инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств, выявленных банковскими платежными агентами (субагентами)	лиц.
П.106. 2	Оператор определяет во внутренних документах порядок регистрации и хранения сведений об инцидентах, указанных в абзацах первом - третьем подпункта 2.13.4 пункта 2.13 настоящего Положения	Положением о ДБО определить порядок регистрации и хранения сведений об инцидентов, назначить ответственных лиц.
П.107	Оператор платежной системы устанавливает распределение обязанностей по определению порядка обеспечения защиты информации при осуществлении переводов денежных средств путем: самостоятельного определения оператором платежной системы порядка обеспечения защиты информации при осуществлении переводов денежных средств; распределения обязанностей по определению порядка обеспечения защиты информации при осуществлении переводов денежных средств между оператором платежной системы, операторами услуг платежной инфраструктуры и участниками платежной системы; передачи функций по определению порядка обеспечения защиты информации при осуществлении переводов денежных средств оператором платежной системы, не являющимся кредитной организацией, расчетному центру	Положением о ДБО определить порядок определения ролей и возможность передачи функций третьим лицам, назначить ответственных лиц.
П.108	Оператор обеспечивает определение порядка обеспечения защиты информации при осуществлении переводов денежных средств в рамках распределения обязанностей, установленных оператором платежной системы	Положением о ДБО определить порядок защиты информации при распределении обязанностей.
П.109	Оператор обеспечивает выполнение порядка обеспечения защиты информации при осуществлении переводов денежных средств	Положением о ДБО определить порядок защиты информации
П.110	Оператор обеспечивает назначение лиц, ответственных за выполнение порядка обеспечения защиты информации при осуществлении переводов денежных средств	Назначить лиц, ответственных за исполнение Положения о ДБО.
П.111	Служба информационной безопасности оператора по переводу денежных средств, оператора услуг платежной инфраструктуры осуществляет контроль (мониторинг) применения организационных мер защиты информации	Включить данное условие в положение о ДБО, назначить ответственных лиц из числа СБ.
П.112	Служба информационной безопасности оператора по переводу денежных средств, оператора услуг платежной инфраструктуры осуществляет контроль (мониторинг) использования технических средств защиты информации	Включить данное условие в положение о ДБО, назначить ответственных лиц из числа СБ.
П.113	Оператор по переводу денежных средств, Оператор услуг платежной инфраструктуры обеспечивает проведение оценки соответствия не реже одного раза в два года, а также по требованию Банка России	Провести оценку и сформировать отчет, который утверждается единоличным исполнительным органом. Осуществлять хранение отчета.
П.113. 1	Организация, ставшая оператором по переводу денежных средств, оператором платежной системы, оператором услуг платежной инфраструктуры, должна провести первую оценку соответствия в течение шести месяцев после получения соответствующего статуса	Провести оценку и сформировать отчет не позднее 6 месяцев с момента получения соответствующего статуса.
П.113. 2	Оператор по переводу денежных средств, Оператор услуг платежной инфраструктуры по результатам оценки соответствия в целях ее документального подтверждения формируют отчет, который утверждается исполнительными органами управления и хранится в порядке, установленном соответствующим оператором. Отчет включает сведения о проведении оценки соответствия, в том числе: заполненную форму 1, установленную приложением 1 к настоящему Положению и содержащую оценки выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств; заполненную форму 2, установленную приложением 1 к настоящему Положению и содержащую оценки выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств; сроки проведения оценки соответствия; сведения о сторонней организации (наименование и местонахождение) в случае ее привлечения оператором по переводу денежных средств, оператором платежной системы, оператором услуг платежной инфраструктуры для проведения оценки соответствия	Проверить соответствие отчета требованиям данного пункта.
П.114	Оператор платежной системы устанавливает требования к содержанию, форме и периодичности представления информации, направляемой операторами по переводу денежных средств и операторами услуг платежной инфраструктуры оператору платежной системы для целей анализа обеспечения в платежной системе защиты информации при осуществлении переводов денежных средств	Положением о ДБО установить требования к информации, предоставляемой для целей анализа.
П.116	Информация, направляемая операторами по переводу денежных средств и операторами услуг	Включить данное условие в положение о

	платежной инфраструктуры, за исключением операционных центров, находящихся за пределами Российской Федерации, оператору платежной системы для целей анализа обеспечения в платежной системе защиты информации при осуществлении переводов денежных средств, включает информацию о степени выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств	ДБО.
П.117	Информация, направляемая операторами по переводу денежных средств и операторами услуг платежной инфраструктуры, за исключением операционных центров, находящихся за пределами Российской Федерации, оператору платежной системы для целей анализа обеспечения в платежной системе защиты информации при осуществлении переводов денежных средств, включает информацию о реализации порядка обеспечения защиты информации при осуществлении переводов денежных средств	Включить данное условие в положение о ДБО.
П.118	Информация, направляемая операторами по переводу денежных средств и операторами услуг платежной инфраструктуры, за исключением операционных центров, находящихся за пределами Российской Федерации, оператору платежной системы для целей анализа обеспечения в платежной системе защиты информации при осуществлении переводов денежных средств, включает информацию о выявленных инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств	Включить данное условие в положение о ДБО.
П.119	Информация, направляемая операторами по переводу денежных средств и операторами услуг платежной инфраструктуры, за исключением операционных центров, находящихся за пределами Российской Федерации, оператору платежной системы для целей анализа обеспечения в платежной системе защиты информации при осуществлении переводов денежных средств, включает информацию о результатах проведенных оценок соответствия	Включить данное условие в положение о ДБО.
П.120	Информация, направляемая операторами по переводу денежных средств и операторами услуг платежной инфраструктуры, за исключением операционных центров, находящихся за пределами Российской Федерации, оператору платежной системы для целей анализа обеспечения в платежной системе защиты информации при осуществлении переводов денежных средств, включает информацию о выявленных угрозах и уязвимостях в обеспечении защиты информации	Включить данное условие в положение о ДБО.
П.121	Оператор регламентируют пересмотр порядка обеспечения защиты информации при осуществлении переводов денежных средств в рамках обязанностей, установленных оператором платежной системы, в связи с изменениями требований к защите информации, определенных правилами платежной системы	Включить данное условие в положение о ДБО, описав порядок пересмотра мер защиты.
П.122	Оператор регламентируют пересмотр порядка обеспечения защиты информации при осуществлении переводов денежных средств в рамках обязанностей, установленных оператором платежной системы, в связи с изменениями, внесенными в законодательные акты Российской Федерации, нормативные акты Банка России, регулирующие отношения в национальной платежной системе	Включить данное условие в положение о ДБО, описав порядок пересмотра мер защиты.
П.123	Оператор регламентируют порядок принятия мер, направленных на совершенствование защиты информации при осуществлении переводов денежных средств, в случаях изменения требований к защите информации, определенных правилами платежной системы	Включить данное условие в положение о ДБО, описать порядок принятия мер.
П.124	Оператор регламентируют порядок принятия мер, направленных на совершенствование защиты информации при осуществлении переводов денежных средств, в случаях изменений, внесенных в законодательные акты Российской Федерации, нормативные акты Банка России, регулирующих отношения в национальной платежной системе	Включить данное условие в положение о ДБО, описав порядок принятия мер.
П.125	Оператор регламентируют порядок принятия мер, направленных на совершенствование защиты информации при осуществлении переводов денежных средств, в случаях изменения порядка обеспечения защиты информации при осуществлении переводов денежных средств	Включить данное условие в положение о ДБО, описать порядок принятия мер.
П.126	Оператор регламентируют порядок принятия мер, направленных на совершенствование защиты информации при осуществлении переводов денежных средств, в случаях выявления угроз, рисков и уязвимостей в обеспечении защиты информации при осуществлении переводов денежных средств	Включить данное условие в положение о ДБО, описав порядок принятия мер.
П.127	Оператор регламентируют порядок принятия мер, направленных на совершенствование защиты информации при осуществлении переводов денежных средств, в случаях выявления недостатков при осуществлении контроля (мониторинга) выполнения порядка обеспечения защиты информации при осуществлении переводов денежных средств	Включить данное условие в положение о ДБО, описав порядок принятия мер.
П.128	Оператор регламентируют порядок принятия мер, направленных на совершенствование защиты информации при осуществлении переводов денежных средств, в случаях выявления недостатков при проведении оценки соответствия	Включить данное условие в положение о ДБО, описав порядок принятия мер.
П.129	Принятие решений оператора по переводу денежных средств, оператора услуг платежной инфраструктуры по совершенствованию защиты информации при осуществлении переводов денежных средств согласуется со службой информационной безопасности	Включить данное условие в положение о ДБО.
П.130	Оператор по переводу денежных средств обеспечивает проведение классификации	Провести оценку ТУ ДБО.

	терминальных устройств (ТУ) ДБО, с учетом следующего: возможностей несанкционированного получения информации, необходимой для осуществления переводов денежных средств; возможностей осуществления воздействия, приводящего к сбоям, отказам, повреждению ТУ ДБО; особенностей конструкции ТУ ДБО; места установки ТУ ДБО	
П.131	Оператор по переводу денежных средств фиксирует во внутренних документах результаты классификации ТУ ДБО и проводит пересмотр результатов классификации ТУ ДБО при изменении факторов, влияющих на классификацию ТУ ДБО	Документально зафиксировать результаты оценки ТУ ДБО, включать в положение о ДБО условие о необходимости пересмотра результатов ТУ ДБО при изменении факторов, влияющих на их работу.
П.132	Оператор по переводу денежных средств, наряду с факторами, указанными в абзаце первом пункта 2.3 настоящего Положения, учитывает результаты классификации ТУ ДБО при выборе организационных мер защиты информации, технических средств защиты информации, а также функциональных и конструктивных особенностей ТУ ДБО, связанных с обеспечением защиты информации при осуществлении переводов денежных средств, с целью выполнения требований подпунктов 2.18.3 - 2.18.8 пункта 2.18 настоящего Положения	Включить данное условие в положение о ДБО.
П.133	Оператор по переводу денежных средств принимает и фиксирует во внутренних документах решения о необходимости установки на (в) ТУ ДБО технических средств, предназначенных для обнаружения и (или) предотвращения (затруднения) работы несанкционированно установленного оборудования	Включить данное условие в положение о ДБО.
П.134	Оператор по переводу денежных средств обеспечивает контроль состава объектов информационной инфраструктуры в сегментах информационно-телекоммуникационных сетей, в составе которых присутствуют ТУ ДБО, за исключением случая использования услуг радиотелефонной подвижной связи	Включить данное условие в положение о ДБО.
П.136	Оператор по переводу денежных средств определяет во внутренних документах порядок работы с заявлениями клиентов о выявленных событиях, связанных с нарушением обеспечения защиты информации при осуществлении переводов денежных средств с применением ТУ ДБО, и обеспечивает выполнение указанного порядка	В положении о ДБО определить порядок работы с заявлениями.
П.137	Оператор по переводу денежных средств определяет порядок настройки программного обеспечения, средств вычислительной техники в составе ТУ ДБО, включая информацию о конфигурации, определяющей параметры работы технических средств защиты информации, и обеспечивает выполнение указанного порядка	В положении о ДБО определить порядок настройки ПО и ВТ в составе ТУ ДБО.
П.138	Оператор по переводу денежных средств обеспечивает периодический контроль состояния ТУ ДБО с целью выявления событий, влияющих на обеспечение защиты информации при осуществлении переводов денежных средств. К таким событиям, в том числе, относятся: несанкционированное внесение изменений в программное обеспечение ТУ ДБО, включая внедрение вредоносного кода; несанкционированное внесение изменений в аппаратное обеспечение ТУ ДБО (установка несанкционированного оборудования на (в) ТУ ДБО), включая несанкционированное использование коммуникационных портов; сбои и отказы в работе технических средств защиты информации, устройств приема платежных карт (при наличии данных устройств), устройств приема наличных денежных средств (при наличии данных устройств), устройств выдачи наличных денежных средств (при наличии данных устройств)	Включить данное условие в положение о ДБО.
П.139	В случае выявления событий, указанных в подпункте 2.18.6 пункта 2.18 настоящего Положения, оператор по переводу денежных средств обеспечивает приведение ТУ ДБО в такое состояние, при котором обслуживание клиентов невозможно, до минимизации возможности наступления негативных последствий выявленных событий или устранения несанкционированных изменений в программном и аппаратном обеспечении ТУ ДБО	Включить данное условие в положение о ДБО.
П.140	Оператор по переводу денежных средств определяет во внутренних документах и обеспечивает выполнение порядка проведения контроля, предусмотренного подпунктом 2.18.6 пункта 2.18 настоящего Положения, включая его периодичность, в зависимости от факторов, указанных в абзаце первом пункта 2.3 настоящего Положения, а также в зависимости от: использования систем удаленного мониторинга состояния ТУ ДБО, применения в соответствии с подпунктом 2.18.2 пункта 2.18 настоящего Положения технических средств, предназначенных для обнаружения и (или) предотвращения (затруднения) работы несанкционированно установленного на (в) ТУ ДБО оборудования; результатов классификации ТУ ДБО в соответствии с подпунктом 2.18.1 пункта 2.18 настоящего Положения	В положении о ДБО определить периодичность контроля за состоянием ТУ ДБО.
П.141	Оператор по переводу денежных средств определяет требования к обеспечению привлеченными к деятельности по оказанию услуг по переводу денежных средств банковскими платежными агентами (субагентами) защиты информации при использовании ТУ ДБО	Включить данное условие в положение о ДБО.

*Голубым цветом обозначены требования, фактически исполненные на дату оценки.

Таким образом, все правовые требования можно свести к следующему:

- должно быть принято положение о ДБО, в котором будут учтены все вышеперечисленные требования.
- с положением о ДБО необходимо ознакомить всех лиц, ответственных за работу и использование ДБО;
- приказами нужно назначить ответственных лиц за функционирование и безопасность ДБО из числа программистов (служба информатизации), назначить куратора СИ.
- приказами нужно назначить ответственных лиц за контроль и мониторинг безопасности ДБО из числа службы безопасности (служба информационной безопасности), назначить куратора СБ.
- провести оценку терминальных устройство ДБО, задокументировав полученные результаты.
- провести оценку системы ДБО самостоятельно, либо с привлечением экспертных организаций, программистов, системных администраторов, задокументировав полученные результаты в форме отчета.
- Создать и вести журнал учета банкоматов, терминалов и иных объектов информационной инфраструктуры;
- Иметь и хранить документацию на ДБО.
- Проверить техническое задание (ТЗ) к договору на создание ДБО (в нем должны быть требования к обеспечению защиты информации). При необходимости внести правки в ранее подготовленное ТЗ.
- Поставить резолюцию службы безопасности на ТЗ.

Иные требования, не включенные в вышеуказанную таблицу, носят технический характер и должны быть реализованы программистами, системными администраторами и не связаны с разработкой внутренних документов и(или) иной документации.

Информация для клиентов и отчетность

При использовании системы ДБО необходимо учитывать, что в силу ст. 25 Федерального закона от 27.06.2011 N 161-ФЗ «О национальной платежной системе» банк до заключения договора с физическим лицом обязан предоставить ему информацию:

- о наименовании и месте нахождения банка, номере лицензии;
- об условиях использования ДБО, в том числе в автономном режиме;
- о способах и местах осуществления перевода;
- о способах и местах предоставления денежных средств физическим лицом банку;
- о размере и порядке взимания банком вознаграждения с физического лица (если предусмотрено)
- о способах подачи претензий и порядке их рассмотрения, включая информацию для связи с оператором электронных денежных средств.

Соответственно, такая информация должна быть размещена на сайте в отдельном блоке и(или) в самих документах, регламентирующих использование ДБО, имеющихся в публичном доступе.

Не позднее 30 дней после проведения оценки системы ДБО банк должен предоставить в ЦБ РФ отчетность по форме 0403202 «Сведения о выполнении операторами платежных систем, операторами услуг платежной инфраструктуры, операторами по переводу денежных средств требований к обеспечению защиты информации при осуществлении переводов денежных средств».

В дальнейшем предоставляется отчетность по форме 0403203 «Сведения о выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств» в сроки, установленные Указанием Банка России от 09.06.2012 N 2831-У. Указание содержит подробное описание о порядке, форме составления отчетности и способах ее предоставления.

ЗАКЛЮЧЕНИЕ

Выводы

Если резюмировать комментарии, указания и выводы, содержащиеся в настоящей правовой оценке, то можно говорить о следующем:

- Необходимо скорректировать уже имеющуюся документацию, связанную с использованием и функционированием системы ДБО. Конкретные формулировки изменений предложены во втором разделе отчета.
- Требуется разработка локальных нормативных актов (ЛНА, связанных с использованием системы ДБО (при их отсутствии), установление контроля за работой ДБО и сохранностью информации. С ЛНА должны быть ознакомлены сотрудники, вовлеченные в контроль за работой системы ДБО. Приказами следует назначить лиц, ответственных за обеспечение информационной безопасности. Иными словами, должны быть реализованы требования Положения N 382-П, утв. Банком России 09.06.2012 г.
- До момента начала использования системы ДБО должна быть проведена оценка, которая фиксируется в форме отчета. Результаты такой оценки должны быть представлены в ЦБ РФ по установленной форме. Конкретные рекомендации представлены в третьем разделе отчета.

Без соблюдения представленных выше указаний использование системы ДБО будет осуществляться в нарушение требований ЦБ РФ и законодательства РФ. Пренебрежение рекомендациями, содержащимися во втором разделе отчета может также повлечь негативные финансовые и правовые последствия для банка, что подтверждается представленной судебной практикой.

Отчет

1.1. Период времени выполнения работ.

Подготовка отчета осуществлялась с 17 по 24 августа 2017 года.

1.2. Цель.

Целью формирования и составления отчета являлась проверка законности использования и функционирования системы ДБО БАНК «XXX», процессов связанных с данной системой, с позиции законодательства Российской Федерации, в том числе требований Центрального банка РФ.

1.3. Объем, характер и география распространения предмета работ, запланированные и фактически полученные данные.

При выполнении работы оценка проводилась только в отношении самой системы ДБО и предоставленной документации, связанной с ней. В предмет исследования не вошли технические показатели системы ДБО, положения документов, не связанные с использованием системы ДБО.

При проведении оценки и формировании рекомендаций предполагалось, что заказчиком представлены все имеющиеся у него документы, при этом остальные документы, на которые не содержалось ссылок в представленных документах, признавались отсутствующими.

Правовая оценка системы ДБО может применяться на дату ее составления на всей территории Российской Федерации. При формировании правовой оценки планирование не осуществлялось. Из представленных результатов следует, что для использования системы ДБО необходимо скорректировать имеющуюся документацию, а также разработать дополнительную документацию, связанную с информационной защитой системы ДБО.

1.4. Использованные методы работы, получения информации и методы оценки.

При выполнении работы применялись эмпирико-теоретические методы получения информации, которые включали в себя: сбор, классификацию, обобщение и анализ информации, а также сравнение выводов, содержащихся в судебной практике, с положениями законодательства РФ, с последующей вероятностной оценкой рисков при использовании системы ДБО.

Кроме того, были соотнесены руководство ДБО с самой системой ДБО за счет сравнения описания из личного кабинета пользователя системы ДБО. При формировании рекомендаций учитывался проведенный поверхностный сравнительный анализ и оценка систем ДБО, используемых другими банками.

1.5. Указание источников информации.

Основным источником информации является Справочно-правовая система «Консультант Плюс».