Ответы на типовые вопросы, связанные с реализацией Положения Банка России от 9 июня 2012 года № 382-П «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»

1. Вопрос: Какими федеральными законами, нормативными актами следует руководствоваться участникам национальной платежной системы при защите персональных данных при осуществлении переводов денежных средств?

Ответ: Требования к защите персональных данных при осуществлении переводов денежных средств в настоящее время установлены Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также Положением Банка России от 9 июня 2012 года № 382-П «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 № 382-П).

Обращаем внимание на то, что в настоящее время не завершено формирование нормативной базы, предусмотренной Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», поскольку Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю не утверждены все документы, предусмотренные статьей 19 данного закона.

2. Вопрос: Как соотносятся Постановление Правительства Российской Федерации от 13 июня 2012 г. № 584 и Положение № 382-П?

Ответ: В соответствии с частью 1 статьи 27 Федерального закона от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе» (далее – Федеральный закон № 161-ФЗ) Постановление Правительства Российской Федерации от 13 июня 2012 г. № 584 "Положение о защите информации в платежной системе" регулирует общие вопросы защиты информации. В соответствии с частью 3 Федерального закона № 161-ФЗ Положение № 382-П устанавливает требования к защите информации при осуществлении переводов денежных средств.

3. Вопрос: Обязана ли кредитная организация во всех случаях, даже при выявлении ею несущественности определенного риска в соответствии с существующими методиками, принимать меры, предусмотренные Положением № 382-П?

Ответ: Положение № 382-П устанавливает требования, в соответствии с которыми операторы по переводу денежных средств, банковские платежные агенты (субагенты), операторы платежных систем, операторы услуг платежной инфраструктуры обеспечивают защиту информации при осуществлении переводов денежных средств. Выполнение данных требований обеспечивается, в том числе, выбором организационных мер и технических средств защиты информации.

Требования к обеспечению защиты информации при осуществлении переводов денежных средств, установленные Положением № 382-П, обязательны к выполнению, при этом результаты оценки рисков оператор может учитывать при выборе организационных мер и технических средств защиты информации.

4. Вопрос: Относится ли к защищаемой в соответствии с Положением № 382-П информации о совершенных переводах денежных средств (в том числе информации, содержащейся в извещениях (подтверждениях), касающихся приема к исполнению распоряжений участников платежной системы) информация, содержащаяся в уведомлении клиента о совершении каждой операции с использованием электронного средства платежа и в чеке банкомата?

Ответ: Информация, содержащаяся в уведомлении клиента о совершении операций с использованием электронного средства платежа, а также информация о переводах денежных средств, печатаемая на чеке банкомата, относится к информации о совершенных переводах денежных средств.

Обращаем внимание на то, что оператор по переводу денежных средств не несет ответственности за обеспечение защиты информации при обработке, хранении и других действиях, производимых клиентом с переданной ему защищаемой информацией.

5. Вопрос: Требуется ли от оператора по переводу денежных средств, являющегося клиентом Банка России, одновременное исполнение требований к защите информации, установленных договором об обмене электронными сообщениями, заключаемым между Банком России и клиентом Банка России, и требований к защите информации при осуществлении переводов денежных средств, установленных Положением № 382-П?

Ответ: Оператор по переводу денежных средств, являющийся клиентом Банка России, при осуществлении переводов денежных средств с использованием платежной системы Банка России обязан исполнять и требования Положения № 382-П, и требования к защите информации, установленные договором об обмене электронными сообщениями при переводе денежных средств в рамках платежной системы Банка России.

6. Вопрос: В каком порядке, в какой форме и с какой периодичностью оператор по переводу денежных средств должен информировать клиентов о различных угрозах и рисках, а также о мерах их нейтрализации?

Ответ: Оператор по переводу денежных средств самостоятельно принимает решения относительно порядка, формы, периодичности доведения до клиентов информации в соответствии с подпунктами 2.7.2, 2.8.2, 2.12.3 пунктов 2.7, 2.8 и 2.12, соответственно, Положения № 382-П, в частности, в зависимости от особенностей клиентской базы (физические или юридические лица, особенности и масштаб работы с клиентами и др.) и особенностей осуществления переводов денежных средств клиентами (использования электронных средств платежа, различные виды доступа к услугам банка и др.).

7. Вопрос: Необходимо ли оператору по переводу денежных средств уведомлять оператора платежной системы об инцидентах (в частности, об обнаружении вредоносного кода), если оператор платежной системы не установил порядок, форму и сроки такого уведомления? Обязан ли оператор по переводу денежных средств информировать каждого из операторов платежной системы об обнаружении вредоносного кода?

Ответ: Согласно подпункту 2.13.1 пункта 2.13 Положения № 382-П оператор платежной системы обязан определить порядок, форму и сроки информирования его оператором по переводу денежных средств. В противном случае имеет место факт нарушения требований Положения № 382-П.

Пунктом 18 части 1 статьи 20 Федерального закона № 161-ФЗ также предусмотрена необходимость отражения оператором платежной системы в правилах платежной системы порядка взаимодействия в рамках платежной системы в спорных и чрезвычайных ситуациях, включая информирование операторами услуг платежной инфраструктуры, участниками значимой платежной системы оператора значимой платежной системы о событиях, вызвавших операционные сбои, об их причинах и последствиях.

При этом формат информационного сообщения и порядок его направления могут быть определены оператором по переводу денежных средств самостоятельно.

Обращаем внимание на то, что в соответствии с подпунктом 2.13.1 пункта 2.13 Положения № 382-П информирование оператора платежной системы должно производиться не реже, чем один раз в месяц.

8. Вопрос: Возможно ли в настоящее время применение несертифицированных, но официально ввезенных на территорию России средств криптографической защиты информации (далее – СКЗИ) при оказании услуг дистанционного банковского обслуживания?

Ответ: Подпунктом 2.9.1 пункта 2.9 Положения № 382-П введен запрет на использование несертифицированных СКЗИ исключительно российского производства.

9. Вопрос: Предполагается ли нормативная унификация документооборота между операторами по переводу денежных средств и операторами платежных систем при выполнении установленных оператором платежной системы требований к обеспечению защиты информации?

Ответ: В настоящее время Банком России не планируется разработка требований, связанных с унификацией документооборота между операторами по переводу денежных средств и операторами платежных систем.

10. Вопрос: В каких случаях допускается назначение ответственных сотрудников вместо создания службы информационной безопасности?

Ответ: Согласно девятому абзацу пункта 2.2 Положения № 382-П под службой информационной безопасности (далее – служба ИБ) понимается подразделение, ответственное за организацию и контроль обеспечения защиты информации, или работники, ответственные за организацию и контроль обеспечения защиты информации.

При этом решение о формировании службы ИБ или о назначении ответственных лиц принимается оператором по переводу денежных средств, банковским платежным агентом (субагентом), являющимся юридическим лицом, оператором услуг платежной инфраструктуры самостоятельно.

11. Вопрос: Допускается ли возможность включения службы информационной безопасности в состав службы информатизации (автоматизации) при условии назначения двух соответствующих кураторов, или оператором по переводу денежных средств обязательно должно быть сформировано две самостоятельные службы?

Ответ: Положение № 382-П не содержит запрета на включение службы информационной безопасности в состав службы информатизации (автоматизации) при исключении возможности курирования службы информационной безопасности куратором службы информатизации (автоматизации).

12. Вопрос: Распространяются ли требования Положения № 382-П на переводы в рамках всех следующих форм безналичных расчетов: расчетов платежными поручениями, расчетов по аккредитиву, расчетов инкассовыми поручениями, расчетов чеками, расчетов в форме перевода денежных средств по требованию получателя (прямое дебетование) и расчетов в форме перевода электронных денежных средств? Планируется ли в дальнейшем разработка Банком России отдельных нормативных актов, регулирующих вопросы защиты информации в отношении каждой из указанных форм безналичных расчетов?

Ответ: Положение № 382-П устанавливает требования, в соответствии с которыми операторы по переводу денежных средств, банковские платежные агенты (субагенты), операторы услуг платежной инфраструктуры, операторы платежных систем обеспечивают защиту информации при осуществлении переводов денежных средств вне зависимости от формы таких переводов.

Разработка отдельных нормативных актов, устанавливающих требования к обеспечению защиты информации при осуществлении переводов денежных средств в зависимости от формы таких переводов, в настоящее время не планируется.

13. Вопрос: В случае если кредитная организация присоединилась к стандарту СТО БР ИББС, какую самооценку ей необходимо провести в первую очередь: на соответствие требованиям СТО БР ИББС или Положения 382-П?

Ответ: Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (далее – СТО БР ИББС-1.0) имеет рекомендательный характер и рекомендован для применения путем включения ссылок на него и (или) прямого использования устанавливаемых в нем положений во внутренних методических и нормативных документах, а также в договорах.

Проведение кредитной организацией оценки соответствия положениям СТО БР ИББС-1.0 не может заменять проведение оценки выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств, установленных Положением № 382-П (далее – оценка соответствия).

Оценка соответствия, согласно Положению № 382-П, проводится не реже одного раза в два года, а также по требованию Банка России.

14. Вопрос: Какие требования Положения № 382-П необходимо выполнить кредитной организации и компании-аутсорсеру для обеспечения соответствия требованиям Положения № 382-П, в случае если планируется передача на аутсорсинг создания, модернизации, технического обслуживания и ремонта объектов информационной инфраструктуры?

Ответ: Положение № 382-П устанавливает требования, в соответствии с которыми операторы по переводу денежных средств, операторы платежных систем, операторы услуг платежной инфраструктуры (далее при совместном

упоминании – операторы) и банковские платежные агенты (субагенты) обеспечивают защиту информации при осуществлении переводов денежных средств.

Передача создания, модернизации, технического обслуживания и ремонта объектов информационной инфраструктуры операторами на аутсорсинг не запрещена Положением № 382-П. Однако обращаем внимание на то, что такая передача может привести к росту рисков информационной безопасности и нарушению системы управления рисками в целом.

Кроме того, выполнение некоторых требований (к примеру, требования о наличии ответственных за обеспечение защиты информации работников и о наличии службы информационной безопасности) не может быть переложено на компанию-аутсорсера.

Также обращаем внимание на то, что в любом случае ответственность за выполнение требований Положения Банка России № 382-П, связанных с созданием, модернизацией, техническим обслуживанием и ремонтом объектов информационной инфраструктуры оператора по переводу денежных средств, лежит на нем самом.

15. Вопрос: Оценке выполнения требований каких категорий проверки в соответствии с Приложением 1 к Положению № 382-П может быть присвоено значение «н/о»?

Ответ: В соответствии с пунктом 1 Приложения 1 к Положению № 382-П оценке выполнения требования к обеспечению защиты информации при осуществлении переводов денежных средств (далее – требование) присваивается числовое или символьное значение. Пункт 2 Приложения 1 к Положению № 382-П устанавливает правила присвоения числовых значений оценке выполнения требований различных категорий проверки. При этом символьное значение «н/о» (нет оценки) может быть присвоено оценке требования любой категории проверки, если выполнение требования не является обязанностью субъекта платежной системы.

16. Вопрос: В каком порядке и каким образом будет осуществляться проверка являющихся защищаемой информацией средств и методов обеспечения информационной безопасности (часть 1 статьи 27 Федерального закона № 161-ФЗ) при условии, что органы, осуществляющие контроль и надзор за выполнением требований установленных Правительством Российской Федерации, не вправе знакомиться с защищаемой информацией (часть 2 статьи 27 Федерального закона № 161-ФЗ)?

Ответ: В соответствии с частью 2 статьи 27 Федерального закона № 161-ФЗ контроль и надзор за выполнением требований, установленных Правительством Российской Федерации, осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, которым является Федеральная служба безопасности Российской Федерации, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, которым является Федеральная служба по техническому и экспортному контролю. Указанная деятельность не осуществляется Банком России.