Нормативное регулирование обеспечения защиты информации при осуществлении переводов денежных средств в национальной платежной системе

Начальник отдела
Департамента
регулирования расчетов
Банка России

Харламов В.П.

29 мая 2013 г.
г. Москва

Федеральный закон
от 27 июня 2011 г. № 161-ФЗ
"О национальной платежной системе"

Федеральный закон от 27 июня 2011 г. № 161-ФЗ статья 27 "Обеспечение защиты информации в платежной системе"

Часть 3 статьи 27

"Операторы по переводу денежных средств, банковские платежные агенты (субагенты), операторы платежных систем, операторы услуг платежной инфраструктуры обязаны обеспечивать защиту информации при осуществлении переводов денежных средств в соответствии с требованиями, установленными Банком России, согласованными с федеральными органами исполнительной власти, предусмотренными частью 2 настоящей статьи. Контроль за соблюдением установленных требований осуществляется Банком России в рамках надзора в национальной платежной системе в установленном им порядке, согласованном с федеральными органами исполнительной власти, предусмотренными частью 2 настоящей статьи"

Некоторые исходные положения при формировании требований к обеспечению защиты информации при осуществлении переводов денежных средств

1. Под нормативное регулирование Банка России подпадают все включенные в платежные системы организации как не являющиеся кредитными организациями, так и все кредитные организации Российской Федерации.
2. Значительная часть кредитных организаций присоединилась к Комплексу БР ИББС.
3. Поэтому при формировании требований к обеспечению защиты информации при осуществлении переводов денежных средств за основу был взят Стандарт Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения", СТО БР ИББС-1.0-2010. Это дает уверенность в том, что подходы к обеспечению информационной безопасности не будут революционными для банковского сообщества, т.е. не вызовут резких изменений в создании СОИБ, во всяком случае, в организациях банковской системы РФ.
4. При этом учитывалась предметная область (перевод денежных средств) и нормативный статус разрабатываемого документа.
5. Требования к обеспечению защиты информации при осуществлении переводов денежных средств хорошо коррелируют с опубликованным Постановлением Правительства РФ "Об утверждении Положения о защите информации в платежной системе".

В результате

Положение Банка России от 9.06.2012 **№ 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", (зарегистрировано Мин. юстиции 14.06.2012 **№ 24575**).

Указание Банка России от 9.06.2012 **№ 2831-У** "Об отчетности по обеспечению защиты информации при осуществлении переводов денежных средств операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств", (зарегистрировано Мин. юстиции 14.06.2012 **№ 24573**).

Порядок осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств

Контроль за соблюдением операторами платежных систем, операторами услуг платежной инфраструктуры, операторами по переводу денежных средств требований к обеспечению защиты информации при осуществлении переводов денежных средств осуществляется Банком России в следующем порядке.

Банк России проводит проверки операторов …, являющихся кредитными организациями, и инспекционные проверки операторов, не являющихся кредитными организациями.

Банк России запрашивает и получает у операторов документы и информацию, в том числе содержащую персональные данные, о деятельности операторов, связанной с выполнением требований к обеспечению защиты информации при осуществлении переводов денежных средств; требует разъяснения по полученной информации.

Банк России запрашивает и получает у операторов по переводу денежных средств документы и информацию, в том числе содержащую персональные данные, об их деятельности по обеспечению контроля соблюдения банковскими платежными агентами (субагентами), привлекаемыми к деятельности по оказанию услуг по переводу денежных средств, требований к защите информации при осуществлении переводов денежных средств.

Проверки операторов, являющихся кредитными организациями, проводятся на основании статьи 73 Федерального закона от 10 июля 2002 года № 86-ФЗ "О Центральном банке Российской Федерации (Банке России)" в соответствии с порядком, установленным Инструкцией Банка России от 25 августа 2003 года № 105-И "О порядке проведения проверок кредитных организаций (их филиалов) уполномоченными представителями Центрального банка Российской Федерации".

Указанные проверки могут осуществляться с участием территориального учреждения Банка России (его структурного подразделения, к компетенции которого относятся вопросы защиты информации при осуществлении переводов денежных средств) по местонахождению кредитной организации (ее филиала).

Инспекционные проверки операторов, не являющихся кредитными организациями, проводятся в соответствии с порядком, установленным Банком России на основании Федерального закона № 161-ФЗ.

Указанные инспекционные проверки могут осуществляться с участием территориального учреждения Банка России (его структурного подразделения, к компетенции которого относятся вопросы защиты информации при осуществлении переводов денежных средств) по местонахождению оператора, не являющегося кредитной организацией.

Об Указании Банка России
"О внесении изменений в Положение 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"

Уточнение понятия "инциденты, связанные с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств"

- события, которые возникли вследствие нарушения
- - требований к обеспечению
- защиты информации при
- осуществлении переводов
- денежных средств* и (или)

- условий осуществления (требований к осуществлению) перевода денежных средств, связанных с обеспечением защиты информации при осуществлении переводов денежных средств, *которые установлены оператором по переводу денежных средств и доведены им до клиента*

**Требований, в соответствии с которыми оператор платежной системы, оператор услуг платежной инфраструктуры, оператор по переводу денежных средств, банковский платежный агент (субагент) обеспечивают защиту информации при осуществлении переводов денежных средств (ч.3 ст.27 ФЗ-161) установлены Положением Банка России от 9 июня 2012 года № 382-П.*

(Продолжение)

События, которые

- привели **к несвоевременности** (**к нарушению сроков**, установленных законодательством Российской Федерации, правилами платежных систем и (или) договорами, заключаемыми клиентами, операторами по переводу денежных средств, операторами услуг платежной инфраструктуры, операторами платежных систем, банковскими платежными агентами (субагентами), участниками платежных систем) осуществления переводов денежных средств;
- привели или могут привести **к осуществлению переводов денежных средств по распоряжению лиц, не обладающих правом распоряжения** этими денежными средствами;
- привели **к осуществлению переводов денежных средств с использованием искаженной информации**, содержащейся в распоряжениях клиентов, распоряжениях участников платежной системы, распоряжениях клирингового центра.

Регистрация действий клиентов в системах ДБО (Банк - Клиент)

При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных в подпункте 2.6.1 Положения 382-П, оператор по переводу денежных средств, банковский платежный агент (субагент) обеспечивают регистрацию действий клиентов, выполняемых с использованием:

- автоматизированных систем, входящих в состав объектов информационной инфраструктуры и используемых для осуществления переводов денежных средств;

- программного обеспечения, входящего в состав объектов информационной инфраструктуры и используемом для осуществления переводов денежных средств

(Продолжение)

Регистрации подлежит следующая информация о действиях клиентов, выполняемых с использованием автоматизированных систем, программного обеспечения:

- дата (день, месяц, год) и время (часы, минуты, секунды) осуществления действия клиента;
- идентификатор клиента - набор символов, присвоенный клиенту и позволяющий идентифицировать его в автоматизированной системе, программном обеспечении;
- код, соответствующий выполняемому действию;
- идентификатор устройства - идентификационная информация, используемая для адресации устройства, с использованием которого осуществлен доступ к автоматизированной системе, программному обеспечению с целью осуществления переводов денежных средств, которой в зависимости от технической возможности является IP-адрес, MAC-адрес, номер SIM-карты, номер телефона и (или) иной идентификатор устройства .

(Продолжение)

Оператор по переводу денежных средств обеспечивает хранение информации не менее пяти лет, начиная с даты осуществления клиентом действия, выполняемого с использованием автоматизированной системы, программного обеспечения.

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.

(Продолжение)

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).

Требования к фиксации инцидентов

Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры обеспечивают регистрацию самостоятельно выявленных инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов 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 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).

Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры определяют во внутренних документах порядок регистрации и хранения сведений об инцидентах.

Требования к проведению оценки соответствия (пункт 2.15 Положения 382-П)

2.15.1. Оценка соответствия осуществляется на основе:

- информации на бумажном носителе и (или) в электронном виде, содержащей подтверждения выполнения порядка применения организационных мер защиты информации и использования технических средств защиты информации;
- анализа соответствия порядка применения организационных мер защиты информации и использования технических средств защиты информации требованиям настоящего Положения;
- результатов контроля (мониторинга) выполнения порядка обеспечения защиты информации при осуществлении переводов денежных средств.

Оценка соответствия - самостоятельно или с привлечением сторонних организаций.

2.15.2. Не реже одного раза в два года, а также по требованию Банка России.

2.15.3. Порядок проведения оценки соответствия и документирования ее результатов определен в приложении 1 к Положению № 382-П .

2.15.4. Перечень проверяемых требований определен в приложении 2 Положению № 382-П.

Требования к документированию результатов оценки соответствия

Оператор по переводу денежных средств, оператор платежной системы, 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 Положения 382-П;
- заполненную форму 2, установленную приложением 1 Положения 382-П;
- сроки проведения оценки соответствия;
- сведения о сторонней организации (наименование и местонахождение) в случае ее привлечения для проведения оценки соответствия.

Требования к проведению оценки соответствия

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.

Организация, являющаяся на день вступления в силу настоящего Указания оператором по переводу денежных средств, оператором платежной системы, оператором услуг платежной инфраструктуры, должна провести оценку соответствия в течение шести месяцев со дня вступления в силу Указания.

Перспективы

Внесение изменений в Положение БР № 382-П

Внесение изменений в Указание БР № 2831-У

Выпуск Методических рекомендаций по проведению проверок при осуществлении Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств

Разработка требований к обеспечению защиты информации при осуществлении переводов денежных средств с использованием банкоматов и платежных терминалов (расширение Положения БР № 382-П).

Разработка требований к обеспечению защиты информации при осуществлении переводов денежных средств с применением технологий Интернет-банкинга (расширение Положения БР № 382-П).

Разработка рекомендаций по обеспечению защиты информации при осуществлении переводов денежных средств с применением технологий Мобильного банкинга.

Благодарю за внимание

В.П. Харламов
Банк России

тлф. 771-47-70
e-mail: hvp@cbr.ru