Обзор нормативной правовой базы в сфере защиты информации в платежных системах

Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» в ч.1 ст.9 определено, что ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Федеральный закон «О национальной платежной системе»

Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платежной системе» (далее – 161-ФЗ) устанавливает правовые и организационные основы национальной платежной системы, регулирует порядок оказания платежных услуг, в том числе осуществления перевода денежных средств, использования электронных средств платежа, деятельность субъектов национальной платежной системы, а также определяет требования к организации и функционированию платежных систем, порядок осуществления надзора и наблюдения в национальной платежной системе.

В соответствии с определением, которое дано в п.1 ст.3 161-ФЗ, национальная платежная система представляет собой совокупность субъектов национальной платежной системы: операторов по переводу денежных средств (включая операторов электронных денежных средств), банковских платежных агентов (субагентов), платежных агентов, организаций федеральной почтовой связи при оказании ими платежных услуг в соответствии с законодательством Российской Федерации, операторов платежных систем, операторов услуг платежной инфраструктуры. В свою очередь, платежная система представляет собой совокупность организаций, взаимодействующих по правилам платежной системы в целях осуществления перевода денежных средств, которая включает оператора платежной системы, операторов услуг платежной инфраструктуры и участников платежной системы, из которых как минимум три организации являются операторами по переводу денежных средств – Банк России, государственная корпорация «Банк развития и внешнеэкономической деятельности (Внешэкономбанк)» и кредитные организации, обладающие правом на осуществление переводов денежных средств. Специального регулирования деятельности таких лиц Закон № 161-ФЗ не предусматривает. Например, согласно ч. 3 ст. 11 161-ФЗ перевод денежных средств кредитные организации должны осуществлять в соответствии с требованиями Федерального закона от 02.12.1990 № 395-1 «О банках и банковской деятельности». Таким образом, в Российской Федерации платежные системы входят в структуру национальной платежной системы посредством субъектов платежных систем: операторов платежной системы и операторов услуг платежной инфраструктуры.

В ст. 27 161-ФЗ вводит специальный правовой режим в отношении обеспечения защиты информации в платежной системе. Согласно ч.ч.1 и 3 ст. 27 161-ФЗ операторы по переводу денежных средств, банковские платежные агенты (субагенты), операторы платежных систем, операторы услуг платежной инфраструктуры обязаны обеспечивать защиту:
1. информации о средствах и методах обеспечения информационной безопасности, персональных данных;
2. информации, подлежащей обязательной защите в соответствии с законодательством Российской Федерации;
3. информации при осуществлении переводов денежных средств.

Особенностью обеспечения защиты вышеуказанных категорий информации является двуединая система установления требований к защите информации и осуществления контроля и надзора за выполнением этих требований.

В отношении первой и второй категорий защищаемой информации требования к защите устанавливает Правительство Российской Федерации – см. постановление Правительства РФ от 13.06.2012 № 584 «Об утверждении Положения о защите информации в платежной системе» (далее - ПП-584). Контроль и надзор за выполнением требований, установленных Правительством Российской Федерации, осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности (Федеральная служба безопасности Российской Федерации), и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации (Федеральная служба по техническому и экспортному контролю Российской Федерации), в пределах их полномочий и без права ознакомления с защищаемой информацией.

В отношении третьей категории защищаемой информации требования к защите устанавливает Банк России по согласованию с федеральными органами исполнительной власти (Федеральной службой безопасности и Федеральной службой по техническому и экспортному контролю) – см. «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 № 382-П). Контроль за соблюдением установленных требований осуществляется Банком России в рамках надзора в национальной платежной системе в установленном им порядке.

Постановление Правительства РФ «Об утверждении Положения о защите информации в платежной системе»

ПП-584 (п.1) устанавливает требования к защите информации о средствах и методах обеспечения информационной безопасности, персональных данных и иной информации, подлежащей обязательной защите в соответствии с законодательством Российской

Федерации, обрабатываемой операторами по переводу денежных средств, банковскими платежными агентами (субагентами), операторами платежных систем и операторами услуг платежной инфраструктуры в платежной системе. Кроме того, п. 2 «Положения о защите информации в платежной системе» закреплено, что защита вышеуказанной информации осуществляется в соответствии с требованиями к защите информации, которые включаются операторами этих платежных систем в правила платежных систем в том числе в соответствии с ПП-584.

Согласно п.3. ПП-584 защита информации обеспечивается путем реализации операторами по переводу денежных средств, банковскими платежными агентами (субагентами), операторами платежных систем и операторами услуг платежной инфраструктуры в платежной системе правовых, организационных и технических мер, направленных:
1. на обеспечение защиты информации от неправомерных доступа, уничтожения, модифицирования, блокирования, копирования, предоставления и распространения, а также от иных неправомерных действий в отношении информации;
2. на соблюдение конфиденциальности информации;
3. на реализацию права на доступ к информации в соответствии с законодательством Российской Федерации.

Правила платежной системы должны предусматривать в том числе следующие требования к защите информации:
– создание и организация функционирования структурного подразделения по защите информации (службы информационной безопасности) или назначение должностного лица (работника), ответственного за организацию защиты информации;
– включение в должностные обязанности работников, участвующих в обработке информации, обязанности по выполнению требований к защите информации;
– осуществление мероприятий, имеющих целью определение угроз безопасности информации и анализ уязвимости информационных систем;
– проведение анализа рисков нарушения требований к защите информации и управление такими рисками;
– разработка и реализация систем защиты информации в информационных системах;
– применение средств защиты информации (шифровальные (криптографические) средства, средства защиты информации от несанкционированного доступа, средства антивирусной защиты, средства межсетевого экранирования, системы обнаружения вторжений, средства контроля (анализа) защищенности);
– выявление инцидентов, связанных с нарушением требований к защите информации, реагирование на них;
– обеспечение защиты информации при использовании информационно-телекоммуникационных сетей общего пользования;
– определение порядка доступа к объектам инфраструктуры платежной системы, обрабатывающим информацию;
– организация и проведение контроля и оценки выполнения требований к защите информации на собственных объектах инфраструктуры не реже 1 раза в 2 года.

Контроль (оценка) соблюдения требований к защите информации осуществляется операторами по переводу денежных средств, банковскими платежными агентами (субагентами), операторами платежных систем и операторами услуг платежной инфраструктуры в платежной системе самостоятельно или с привлечением на договорной основе организации, имеющей лицензию на деятельность по технической защите конфиденциальной информации.

Требования к защите информации реализуются:
1. в случае разработки и создания информационных систем - на всех стадиях (этапах) их создания и эксплуатации;
2. в случае приобретения информационных систем - при вводе их в эксплуатацию и при эксплуатации.

Применение шифровальных (криптографических) средств защиты информации осуществляется в соответствии с законодательством Российской Федерации.

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

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, а также устанавливает порядок осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств в рамках осуществляемого Банком России надзора в национальной платежной системе.

Для проведения работ по обеспечению защиты информации при осуществлении переводов денежных средств операторы по переводу денежных средств, банковские платежные агенты (субагенты), операторы платежных систем, операторы услуг платежной инфраструктуры могут привлекать организации, имеющие лицензии на деятельность по технической защите конфиденциальной информации и (или) на деятельность по разработке и производству средств защиты конфиденциальной информации.

В соответствии с п.2.1 382-П к защищаемой информации относится:
– информации об остатках денежных средств на банковских счетах;
– информации об остатках электронных денежных средств;
– информации о совершенных переводах денежных средств, в том числе информации, содержащейся в извещениях (подтверждениях), касающихся приема к исполнению распоряжений участников платежной системы, а также в извещениях (подтверждениях), касающихся исполнения распоряжений участников платежной системы;
требование об отнесении информации о совершенных переводах денежных средств к защищаемой информации, хранящейся в

операционных центрах платежных систем с использованием платежных карт или находящихся за пределами Российской Федерации, устанавливается оператором платежной системы;
– информации, содержащейся в оформленных в рамках применяемой формы безналичных расчетов распоряжениях клиентов операторов по переводу денежных средств (далее - клиентов), распоряжениях участников платежной системы, распоряжениях платежного клирингового центра;
– информации о платежных клиринговых позициях;
– информации, необходимой для удостоверения клиентами права распоряжения денежными средствами, в том числе данных держателей платежных карт;
– ключевой информации средств криптографической защиты информации (далее - СКЗИ), используемых при осуществлении переводов денежных средств (далее - криптографические ключи);
– информации о конфигурации, определяющей параметры работы автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования, эксплуатация которых обеспечивается оператором по переводу денежных средств, оператором услуг платежной инфраструктуры, банковским платежным агентом (субагентом), и используемых для осуществления переводов денежных средств (далее - объекты информационной инфраструктуры), а также информации о конфигурации, определяющей параметры работы технических средств по защите информации;
– информации ограниченного доступа, в том числе персональных данных и иной информации, подлежащей обязательной защите в соответствии с законодательством Российской Федерации, обрабатываемой при осуществлении переводов денежных средств.

Выполнение требований к обеспечению защиты информации при осуществлении переводов денежных средств (п. 2.3 382-П) обеспечивается путем:
1. выбора организационных мер защиты информации; определения во внутренних документах оператора по переводу денежных средств, банковского платежного агента (субагента), оператора платежных систем, оператора услуг платежной инфраструктуры порядка применения организационных мер защиты информации; определения лиц, ответственных за применение организационных мер защиты информации; применения организационных мер защиты; реализации контроля применения организационных мер защиты информации; выполнения иных необходимых действий, связанных с применением организационных мер защиты информации;
2. выбора технических средств защиты информации; определения во внутренних документах оператора по переводу денежных средств, банковского платежного агента (субагента), оператора платежных систем, оператора услуг платежной инфраструктуры порядка использования технических средств защиты информации, включающего информацию о конфигурации, определяющую параметры работы технических средств защиты информации; назначения лиц, ответственных за использование технических средств защиты информации; использования технических средств защиты информации; реализации контроля за использованием технических средств защиты информации; выполнения иных необходимых действий, связанных с использованием технических средств защиты информации.

В соответствии с п.2.6.2 382-П оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают применение некриптографических средств защиты информации от несанкционированного доступа, в том числе прошедших в установленном порядке процедуру оценки соответствия. Допускается применение некриптографических средств защиты информации от несанкционированного доступа иностранного производства.

В соответствии с п.2.9.1 382-П работы по обеспечению защиты информации с помощью СКЗИ проводятся в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи», Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденным приказом Федеральной службы безопасности Российской Федерации от 9 февраля 2005 года № 66, и технической документацией на СКЗИ. В случае если оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры применяют СКЗИ российского производителя, указанные СКЗИ должны иметь сертификаты уполномоченного государственного органа.

Согласно п.2.15.1 382-П оператор по переводу денежных средств, оператор платежной системы, оператор услуг платежной инфраструктуры обеспечивают проведение оценки выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств (далее - оценка соответствия).

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 382-П;
– результатов контроля (мониторинга) выполнения порядка обеспечения защиты информации при осуществлении переводов денежных средств.

Оценка соответствия осуществляется оператором по переводу денежных средств, оператором платежной системы, оператором услуг платежной инфраструктуры самостоятельно или с привлечением сторонних организаций. Оператор по переводу денежных средств, оператор платежной системы, оператор услуг платежной инфраструктуры обеспечивают проведение оценки соответствия не реже одного раза в два года, а также по требованию Банка России.

защита информации в национальной платежной системе, тайна обеспечения информационной безопасности, аналитика

From:
http://sps-ib.ru/ - **Справочно-правовая система по информационной безопасности**

Permanent link:
http://sps-ib.ru/analitika:obzor_zakonodatelstva_nps

Last update: **2017/05/30 20:39**