

ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ОСУЩЕСТВЛЕНИИ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ В НАЦИОНАЛЬНОЙ ПЛАТЕЖНОЙ СИСТЕМЕ РОССИИ

Никитина Виктория Леонидовна

*НИЯУ МИФИ, Москва, зам. зав. кафедрой кибербезопасности
op50@mail.ru*

Актуальность, новизна, цель и практическая значимость работы обусловлены проблемами реализации Федерального закона от 27 июня 2011 года N 161-ФЗ "О национальной платежной системе" [1], который преследует триединую задачу: уход от иностранной разведки российских финансовых транзакций – усиление национального финансового мониторинга в интересах противодействия легализации (отмывания) доходов, полученных преступным путем, и финансированию терроризма – уменьшение массы наличных денежных средств.

Основные положения нормативного обеспечения защиты информации при осуществлении переводов денежных средств в национальной платежной системе России приведены в анализируемом ниже Положении Центрального банка России от 9 июня 2012 г. N 382-П

Анализируемое «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» по состоянию на 21 августа 2012 года в целом соответствует требованиям, предъявляемым к подзаконным нормативно-правовым актам. Однако, после вступления России во Всемирную торговую организацию (далее - ВТО) Федеральный закон от 27 июня 2011 года N 161-ФЗ "О национальной платежной системе" и, следовательно, анализируемое Положение требуют дополнений по обязательствам России перед ВТО. В частности, согласно терминологии ВТО банковские операции относятся к банковским услугам. После присоединения к ВТО к оказанию таких банковских услуг в России будут допущены иностранцы из стран – членов ВТО на предусмотренных условиях. Россия присоединилась к ВТО 22 августа 2012 года путем ратификации соответствующих международных соглашений. После ратификации эти тексты стали частью международных со-

глашений России, которые, как известно, имеют большую силу, нежели любые внутренние российские законы. В случае противоречия между этими текстами и внутренними российскими законами в силу ч. 4 ст. 15 Конституции РФ применяться должны будут первые. После вступления России в ВТО в отношении оказания иностранными лицами из членов ВТО финансовых услуг в России / применительно к получателям в России и из России будут действовать правила согласно принятым на себя Россией обязательствам. Кроме того, российские субъекты получают право входить на иностранные рынки финансовых услуг, причем с учетом тех обязательств, которые взяли на себя соответствующие члены ВТО.

В связи с получением Россией статуса члена ВТО для нее начали действовать десятки документов ВТО (как международные соглашения, образующие правовую основу ВТО, так и локальные документы органов ВТО). Важнейший из них — Генеральное соглашение о торговле услугами (General Agreement on Trade in Services), GATS (ГАТС). Сюда же следует отнести Международные стандарты ISO 13335, ISO 13569 (банковские и финансовые услуги), ISO 17799/BS 7799-2, », COBIT, серию стандартов ИСО/МЭК 27000 и др.

Необходимо отметить следующие резервы доработки Положения:

1. Целесообразно дополнить п.1.1. Положения ссылкой на «Положение о защите информации в платежной системе», утвержденное Постановлением Правительства РФ от 13 июля 2012 № 584;

2. Положение не содержит ссылки на ранее принятый Стандарт Банка России СТО БР ИББС-1.0-2010 «ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ» без соблюдения которого, как отметил В. Лукацкий, крайне трудно выполнять требования Федерального закона от 27 июля 2006 г. N 152-ФЗ «О персональных данных», которым после 1 января 2011 года должны соответствовать все системы, обрабатывающие персональные данные. Проблема выполнения технических требований, вытекающих из этого закона ускорила процесс принятия кредитными организациями данного стандарта. Обсуждая вопрос внедрения СТО БР ИББС, стоит упомянуть и об Указании Банка России от 09.06.2012 N 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», в котором установлены формы отчетности по обеспечению защиты информации при осуществлении переводов денежных средств 3 категорий операторов: платежных систем; услуг платежной инфраструктуры; по переводу денежных средств.

3. В соответствии с п. 2.9.1. Положения «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». Однако, никак не урегулирован вопрос применения СКЗИ нероссийского производства. В Приложении 2 приведен перечень требований к СКЗИ без учета происхождения. Например, если длина ключей для симметричных СКЗИ, предназначенных для защиты финансовых транзакций составляет свыше 56 бит, то при наличии нотификации ФСБ, ввозятся такие СКЗИ, что фактически является разрешением и на эксплуатацию. Поэтому получается так, что в НПС могут применяться любые СКЗИ.

4. На оператора платежной системы возлагается большая работа по реагированию на инциденты, разработке методик анализа и реагирования, информирование операторов по переводу и операторов инфраструктуры о выявленных инцидентах и т.д. Оценка соответствия требованиям по ИБ проводится самостоятельно или с приглашением внешних организаций в соответствии с методикой, приведенной в приложении к Положению. При этом никак не урегулирован вопрос о наличии лицензии на техническую защиту конфиденциальной информации у такой организации в соответствии с Постановлением Правительства РФ от 03.02.2012 г №79 «О лицензировании деятельности по технической защите конфиденциальной информации».

5. Перечень отмеченных замечаний не является исчерпывающим. Отдельного анализа требуют Приложения к анализируемому Положению. Особенно это относится к Приложению 1, которое содержит спорные утверждения из области многомерных экспертных оценок и не соотносится с международными моделями уровней зрелости организаций. Отмеченные замечания требуют дальнейшего анализа и доработки.

Список источников

1. Федеральный закон от 27 июня 2011 года N 161-ФЗ «О национальной платежной системе». «Российская газета» от 30 июня 2011 г. N 139.