

Секция «Особенности аудита организации с цифровыми ресурсами: угрозы и информационная безопасность»

Особенности правового регулирования информационной безопасности национальной платежной системы

Научный руководитель – Полякова Татьяна Анатольевна

Костыря Дмитрий Юрьевич

Студент (магистр)

Российская правовая академия Министерства юстиции Российской Федерации, Москва, Россия

E-mail: rramagistratura@mail.ru

Национальная платежная система - ключевая составляющая экономики страны, т.к. обеспечивает участие всех физических и юридических лиц в финансовых и экономических отношениях, основой которых является движение денежных средств. Эффективное и бесперебойное функционирование субъектов национальной платежной системы (далее НПС) является одним из основных факторов, влияющих на развитие экономики страны, рост ВВП, повышение скорости оборачиваемости средств, реализацию денежно-кредитной политики, финансовую стабильность и независимость, повышение качества и безопасности безналичных платежных услуг, способствует выводу экономических отношений из «серой» зоны.[3]

27 июня 2011 года был подписан Федеральный закон № 161-ФЗ «О национальной платёжной системе» (далее — закон № 161-ФЗ), формализовавший существующее положение вещей, когда проведение платежей обеспечивают не только банки, но и многочисленные организации, не имеющие банковской лицензии.

Время издания этого закона совпало с периодом резкого всплеска преступных посягательств на денежные средства, циркулирующие в платёжной системе. Причём эти посягательства всё чаще выполняются с использованием компьютерных технологий. Налёты на отделения банков уже не приносят преступникам столько денег, сколько приносят интеллектуальные и технологичные способы их отъёма. Резкий рост хищений фиксируется в системах интернет-банкинга.

В законе № 161-ФЗ законодатель посвятил вопросам защиты информации отдельную статью, в которой установлено, что:

1) операторы по переводу денежных средств, банковские платёжные агенты (субагенты), операторы платёжных систем, операторы услуг платёжной инфраструктуры обязаны обеспечивать защиту информации о средствах и методах обеспечения информационной безопасности (далее — ИБ), персональных данных и иной информации, подлежащей обязательной защите в соответствии с законодательством РФ;

2) контроль и надзор за выполнением требований, установленных Правительством РФ, осуществляются Федеральной службой безопасности (ФСБ России) и Федеральной службой по техническому и экспортному контролю (ФСТЭК России) в пределах их полномочий и без права ознакомления с защищаемой информацией;

3) операторы по переводу денежных средств, банковские платёжные агенты (субагенты), операторы платёжных систем, операторы услуг платёжной инфраструктуры обязаны обеспечивать защиту информации при осуществлении переводов денежных средств в соответствии с требованиями, установленными Банком России, согласованными с федеральными органами исполнительной власти.[1]

Контроль за соблюдением установленных требований осуществляется Банком России в рамках надзора в национальной платёжной системе в установленном им порядке, согласованном с ФСБ России и ФСТЭК России.

Таким образом, требования безопасности информации при переводе денежных средств устанавливаются Правительством РФ и Банком России. Они же осуществляют контроль выполнения этих требований.

Центральный Банк РФ занимает важное место в платежной системе страны еще и потому, что, являясь оператором собственной клиринговой системы, координирует и регулирует расчетные отношения, осуществляет мониторинг деятельности частных платежных систем, определяя основные правила их функционирования, устанавливает принципы, формы, сроки и стандарты осуществления безналичных расчетов, а также организует наличное денежное обращение.

В соответствии с указаниями Президента РФ Путина В.В. о публичной отчетности контрольно-надзорных органов об итогах проводимых ими проверок, Банк России каждые полгода публикует отчеты об инцидентах в НПС: обзор о несанкционированных переводах денежных средств, которые, в конечном счете, являются показателями нарушения бесперебойности работы НПС и угрозы финансовой стабильности и безопасности страны в связи с возможным ростом недовольства ее граждан качеством работы и безопасностью НПС. Данные обзоры Банка России позволяют на основе анализа представляемой динамики делать выводы об эффективности/неэффективности применяемых мер и о необходимости направления дополнительных усилий в отношении тех или иных банковских услуг.[4]

Во исполнение закона № 161-ФЗ были изданы три основных документа. Так, Правительство РФ выпустило постановление от 13.06.12 № 584 «Об утверждении Положения о защите информации в платёжной системе», вступившее в силу 1 июля 2012 года.

Банк России издал ряд документов по рассматриваемой тематике: Положение от 09.06.12 № 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» и Указание от 09.06.12 № 2831-У «Об отчётности по обеспечению защиты информации при осуществлении переводов денежных средств операторов платёжных систем, операторов услуг платёжной инфраструктуры, операторов по переводу денежных средств»

В основе вышеизложенных актов стоят СТО БР ИББС — комплекс документов (стандарты Банка России). Ещё в середине 2000-х годов Банк России выступил инициатором создания фактически первого полноценного отраслевого стандарта, относящегося к информационной безопасности банковской системы РФ.

Со временем отдельные документы комплекса СТО БР ИББС обновлялись и актуализировались. С появлением нормативных актов в области защиты персональных данных (далее — ПД) комплекс пополнился отраслевой моделью угроз ПД, требованиями по обеспечению безопасности ПД, а также методическими рекомендациями по выполнению требований законодательства в области персональных данных.[5]

Полезность стандартов заключается в том, что банкам предложен комплексный подход к обеспечению защиты информации и информационных технологий, позволяющий одновременно выполнить требования законодательства. При этом каждый банк может самостоятельно или с использованием внешнего аудитора провести оценку степени выполнения у себя требований СТО БР ИББС и получить численное значение этой оценки. Полученные численные показатели дают возможность понять, насколько банк продвинулся в области обеспечения ИБ и какого уровня он достиг в этом вопросе. Как и любой стандарт, рассматриваемый комплекс не обязателен для выполнения в банках. Он предоставляет банкам лучшие практики. Однако уже больше половины всех российских банков добровольно присоединились к этому комплексу и реализуют его положения. Таким

образом, банкам, которые присоединились к СТО БР ИББС, будет значительно проще выполнять требования (уже обязательные) безопасности информации в НПС.

С появлением закона № 161-ФЗ и иных документов Банка России бытует мнение, что комплекс СТО БР ИББС морально устаревает а его актуальность снижается. Однако, скорее всего это ошибочное мнение. Комплекс был и остаётся сборником лучших практик, который является источником права. При этом, комплекс безусловно требует модернизации и обновления.

Стандарты Банка России обеспечивает информационную безопасность организаций банковской системы Российской Федерации (далее - БС РФ), их активов, к которым в том числе относятся персональные данные и банковские технологические процессы, в рамках которых они обрабатываются.

Введение в действие Стандартов для Центрального Банка было знаковым событием. Регулятору пришлось переступить через многие свои правила. Во-первых, Центральный Банк впервые активно подключился к процессам, направленным на повышение защищенности участников отечественного финансового рынка - обеспечения как их информационной безопасности, так и их клиентов. Во-вторых, признал за банками право не следовать всем требованиям документа, а последовательно развивать свои системы обеспечения информационной безопасности через применение оценки зрелости процессов безопасности, которая была тем выше, чем полнее банк следовал требованиям стандарта. В-третьих, стандарт был добровольным. Несмотря на это Стандарт был положительно воспринят банковским сообществом.[6]

СТО (Стандарт организации) не должны вступать в противоречие с действующими Государственными стандартами. Особенность стандартов в том, что они носят рекомендательный характер, а не обязательный в отличии от законодательных актов. К плюсам можно отнести что они являются источниками права.

В настоящее время Стандарты переходят на новый уровень. На их основе подготовлен проект национального стандарта, предназначенный для применения в соответствии с действующим законодательством (№184-ФЗ от 2002 года «О техническом регулировании» и №162-ФЗ от 2015 года «О стандартизации»).

Действующая платежная система не идеальна. Существует множество уязвимостей, объем хищения денежных средств с каждым годом только возрастает. Представляется необходимым использование криптовалютной платежной системы. Система является инновационным аналогом глобальной платежной системы на основе публичного коллективного регистра всех транзакций, который способен изменить существующие финансовые системы. Внедрение любого инновационного продукта в хозяйственный оборот требует комплексного, всестороннего подхода к системе его финансирования и эффекта от использования. Положительным моментом можно считать способность криптосистем к ускорению расчетов по международным транзакциям и значительная безопасность по сравнению с действующими платежными системами.[7]

Действительно, появились новые субъекты НПС (кроме банков). Практика нарушений ИБ подсказывает, что в будущей редакции стандарта нужно развивать и конкретизировать подходы, связанные с анализом и управлением новыми рисками, которые диктует жизнь. Одно из актуальных направлений развития — это усиление подхода, связанного с управлением рисками, с учётом резкого расширения многообразия технологий платежей и других финансовых операций. Информационная безопасность также должна серьёзно обосноваться на фондовом рынке и у всех новых субъектов НПС. Поэтому комплекс нужно актуализировать. При этом роль его как базиса, на котором основаны обязательные нормы и требования обеспечения ИБ, остаётся прежней.

Источники и литература

- 1) Федеральный закон "О национальной платежной системе" от 27.06.2011 N 161-ФЗ
- 2) Постановление Правительства РФ от 13.06.2012 N 584 "Об утверждении Положения о защите информации в платежной системе"
- 3) Бондарева В.А. Национальная платежная система как направление стабилизации банковской системы России: статья в сборнике трудов XVI Международной межвузовской научно-практической конференции. М.: Дашков и К. – с.394.
- 4) Грушина С.А. «Современное состояние национальной платежной системы». Современные гуманитарные исследования, 2015, № 5 (66) – с.31-34.
- 5) Ложкин П.Э. Закон о Национальной платежной системе: Требования по информационной безопасности. Банковское дело, 2012, №11. – с.70-76.
- 6) Чирков А.В. «Проблемы реализации законодательства о национальной платежной системе в части ответственности банков в расчетных правоотношениях». Банковское право, 2011, №6. – с.61-68.
- 7) Хоменко Е.Г. «Правовое обеспечение инфраструктурного взаимодействия между участниками расчетов в Национальной платежной системе». Предпринимательское право, 2016, № 2. – с.39–42.