5. Бутакова Н.А. Реальный и консенсуальный договор // СПС КонсультантПлюс. 2019.
6. Витрянский В.В. Очередной этап реформы гражданского законодательства: потери и достижения // Хозяйство и право. 2017. № 10. С. 6.
7. Кожокаръ И.П. Аксиологические дефекты нормативной подсистемы механизма гражданско-правового регулирования // Право и экономика. 2016. N 8. С. 4 - 8.
8. Ентаева А.В. Презумпция добросовестности опекуна // Стандарты доказывания по гражданским делам. № 1. 2017. С. 42.
9. Ефимова Л.Г. Договоры банковского вклада и банковского счета: монография. М.: Проспект, 2018. С. 201.
10. Нурмухаметов Р. К. Использование специальных банковских счетов в проектном финансировании // Международный экономический симпозиум. № 1. 2015. С. 157.
11. Писаревский Е.Л. Финансовые гарантии в праве европейских государств. Юрист: М. 2008. С. 8.
12. Яковлева И.А. Теоретические и практические проблемы правового регулирования банковской, налоговой и коммерческой тайны в предпринимательской деятельности // Проблемы экономики и юридической практики. 2014. №5. С. 327. В части регулирования номинальных банковских счетов:
13. Пояснительная записка к проекту федерального закона № 393713-4 «о внесении изменений в некоторые законодательные акты российской федерации» // СПС КонсультантПлюс
14. Пояснительная записка к проекту федерального закона № 47538-6 // СПС КонсультантПлюс
15. Решение Комитета по гражданскому, уголовному, арбитражному и процессуальному законодательству от 13.10.2009 № 76(8) // СПС КонсультантПлюс

Соколова Е.А., Ермошина А.Ю.

Роль Банка России в обеспечении информационной безопасности финансовой системы государства

*Академия права и управления Федеральной службы исполнения наказаний
(Россия, Рязань)*

doi: 10.18411/lj-04-2020-102

idsp: ljjournal-04-2020-102

Аннотация

В статье представлен обзор нормативно-правовых актов, принятых Банком России в течение последних трех лет в целях обеспечения информационной безопасности финансовой системы государства и затрагивающих порядок осуществления банковских операций, работы с биометрическими данными физических лиц и другие вопросы банковской деятельности.

Ключевые слова: подзаконные нормативно-правовые акты, Банк России, информационная безопасность, финансовая система, банковские операции.

Abstract

The article provides an overview of the legal acts adopted by the Bank of Russia over the past three years in order to ensure information security of the financial system of the state. They affect the procedure for conducting banking operations, working with biometric personal data, and other banking issues.

Keywords: legal acts, Bank of Russia, information security, financial system, banking operations.

В современном обществе информация выступает одним из основных факторов производства и, как отмечают ученые, оказывает существенное влияние на экономику, обороноспособность страны, политику, социальную сферу и многое другое, от чего в значительной степени зависят поведение людей, формирование общественно-политических движений и достигаются (или не достигаются) социальная стабильность, правопорядок и безопасность.

Новые вызовы современности ставят перед государством задачи, связанные с совершенствованием информационной безопасности финансовой системы страны. В

России ключевым регулятором в данной сфере является Центральный Банк Российской Федерации (Банк России).

По данным Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России (ФинЦЕРТ), для многих современных кредитно-финансовых учреждений киберриски стали одними из важнейших факторов, сдерживающих развитие, а ущерб от киберпреступлений, в том числе репутационный, в настоящее время существенно выше, чем от «классических» ограблений.

С учетом изложенного основными целями Банка России в разрезе информационной безопасности являются:

- 1) обеспечение киберустойчивости (с помощью контроля показателей риска реализации информационных угроз, обеспечения непрерывности предоставления финансовых и банковских услуг, контроля уровня мошеннических операций);
- 2) защита потребителей финансовых услуг (путем мониторинга и контроля показателей, характеризующих уровень финансовых потерь);
- 3) содействие развитию инновационных финансовых технологий (с помощью контроля риска реализации информационных угроз и реализации необходимого уровня информационной безопасности).

В рамках реализации своих основных целей Банк России ведет активную просветительскую работу с гражданами и организациями по вопросам финансово целесообразного, грамотного и безопасного поведения на рынке финансовых услуг.

Одним из наиболее масштабных направлений работы Центрального банка Российской Федерации в сфере обеспечения финансовой безопасности государства является принятие в пределах своей компетенции подзаконных нормативно-правовых актов, регулирующих вопросы защиты клиентских данных при осуществлении банковских операций.

Общие положения о защите информации в российских банках содержатся в Федеральном законе от 27 июня 2011 г. № 161 «О национальной платежной системе», который 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. Данный федеральный закон регулярно дополняется и изменяется с учетом появления новых угроз и вызовов информационной безопасности финансовой системы.

Во исполнение требований Федерального закона «О национальной платежной системе» Банком России принят ряд документов, детализирующих порядок реализации положений закона в части информационной безопасности финансовой системы государства.

Так, Положение Банка России от 3 октября 2017 г. № 607-П «О требованиях к порядку обеспечения бесперебойности функционирования платежной системы, показателям бесперебойности функционирования платежной системы и методикам анализа рисков в платежной системе, включая профили рисков» регулирует вопросы управления рисками и непрерывности предоставления услуг в платежной системе. Данный документ вводит количественные показатели непрерывности функционирования платежной системы в зависимости от уровня её значимости, регламентирует порядок обработки инцидентов (событий, приведших к нарушению предоставления платежных сервисов, возникших в том числе вследствие нарушений защиты информации) услуг платежной инфраструктуры, включая объем сохраняемых сведений, касающихся таких инцидентов, и срок их хранения – 3 года. Банк России

устанавливает периодичность оценки рисков – не реже 1 раза в год и сроки пересмотра системы риск-менеджмента – не реже 1 раза в 2 года, а также определяет перечень количественных показателей доступности услуг платежной инфраструктуры, бесперебойности функционирования платежной системы и частоты инцидентов, а также методы расчета этих показателей.

Положение Банка России от 16 апреля 2018 г. № 640-П «О порядке осуществления Банком России надзора за соблюдением не являющимися кредитными организациями операторами платежных систем, операторами услуг платежной инфраструктуры требований Федерального закона от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе» и принимаемых в соответствии с ним нормативных актов Банка России» регламентирует права Банка России при осуществлении надзора за соблюдением требований федерального закона «О национальной платежной системе» и устанавливает способы воздействия на операторов для устранения выявленных недостатков.

Указанием Банка России от 8 октября 2018 г. № 4926-У «О форме и порядке направления операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры в Банк России информации обо всех случаях и (или) попытках осуществления переводов денежных средств без согласия клиента и получения ими от Банка России информации, содержащейся в базе данных о случаях и попытках осуществления переводов денежных средств без согласия клиента, а также о порядке реализации операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента» установлен порядок реализации мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента. В данном документе определены форма, порядок и содержание сообщений, отправляемых финансовыми организациями в ФинЦЕРТ Банка России. При этом сам Центральный банк Российской Федерации осуществляет формирование и ведение базы данных обо всех случаях и попытках осуществления переводов денежных средств без согласия клиента.

Положение Банка России от 17 апреля 2019 г. № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента» предъявляет требования по защите электронных сообщений банков и их клиентов, клиентской аутентификационной информации, информации об осуществленных банковских операциях, а также определяет порядок применения средств криптографической защиты информации.

Данное положение определяет разные уровни защиты информации для кредитных организаций в зависимости от их значимости: системно значимые кредитные организации, кредитные организации, выполняющие функции оператора услуг платежной инфраструктуры системно значимых платежных систем, и кредитные организации, значимые на рынке платежных услуг, должны выполнять меры по защите информации в соответствии с усиленным (первым) уровнем защиты, определенным ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер», а иные – в соответствии со стандартным (вторым) уровнем защиты.

Указание Банка России от 23 декабря 2019 года № 5365-У «О порядке осуществления контроля оператором по переводу денежных средств за деятельностью банковских платежных агентов» подробно регламентирует контрольную деятельность оператора за переводами денежных средств. В частности, плановые проверки должны проводиться не реже 1 раза в год, внеплановые – при наличии информации об

осуществлении банковским платежным агентом, привлеченными им банковскими платежными субагентами операций, имеющих запутанный или необычный характер, свидетельствующих об отсутствии очевидного экономического смысла или очевидной законной цели. При наличии таких сведений оператор вправе осуществлять мониторинг операций банковского платежного агента, привлеченных им банковских платежных субагентов, в том числе, с учетом имеющейся информации о движении денежных средств.

В целях нейтрализации угроз безопасности, актуальных при работе с биометрическими персональными данными физических лиц, удаленной идентификации клиентов, Банк России выпустил методические рекомендации от 14 февраля 2020 г. № 4-МР по нейтрализации банками угроз безопасности, актуальных при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации. Документ рекомендует банкам регистрировать инциденты при использовании Единой биометрической системы и сообщать о них в Центральный банк Российской Федерации.

Центральный банк Российской Федерации, реализуя свои задачи в сфере обеспечения информационной безопасности финансовой системы государства, оперативно отреагировал на изменение условий работы в связи с пандемией коронавируса, порекомендовав финансовым компаниям принять меры по обеспечению киберустойчивости и информационной безопасности в условиях распространения новой коронавирусной инфекции (COVID-19) (информационное письмо от 20.03.2020 № ИН-014-56/17). Для минимизации рисков ошибок во время проведения денежных переводов, транзакций, ведения банковских счетов физических и юридических лиц, снятия наличных денег в банкоматах и других операции, Банк России рекомендовал осуществлять банковские операции, не связанные с открытием и ведением счетов и не влияющие на бесперебойность транзакций, в удаленном режиме и применять в целях безопасности технологии виртуальных частных сетей, многофакторной аутентификации, а также организовать мониторинг и контроль действий пользователей удаленного мобильного доступа.

Таким образом, Банк России, являясь мегарегулятором финансовой системы государства, использует широкий спектр инструментов в рамках своей компетенции для регулирования и обеспечения информационной безопасности финансовых операций, борьбы с киберпреступностью, снижения уязвимости и инфраструктуры финансового сектора.

Стрыгина С.В.

Исторические основы формирования принципа справедливости в праве

*Саратовский национальный исследовательский государственный университет
им. Н.Г. Чернышевского
(Россия, Саратов)*

doi: 10.18411/lj-04-2020-103

idsp: ljjournal-04-2020-103

Аннотация

В статье ставится задача проанализировать основные этапы формирования категории справедливости и перехода ее из чисто моральных ценностей к правовым. Целью статьи является показать, что справедливость не может быть однозначной и в разные исторические эпохи она меняет свое содержание. Она зависит от развития общественного бытия и общественного сознания. Говорится, что справедливость в