УДК 347.42

Быкова Н.А.,
Студент 3 курса магистратуры
направление «Правовое сопровождение бизнеса (бизнес-юрист)»
Волго-вятский институт (филиал)
университета имени О.Е. Кутафина МГЮА

ОБ ОТДЕЛЬНЫХ ПОЛОЖЕНИЯХ ЗАКОНОДАТЕЛЬСТВА, НАПРАВЛЕННЫХ НА ПРОТИВОДЕЙСТВИЕ ОСУЩЕСТВЛЕНИЯ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ БЕЗ СОГЛАСИЯ КЛИЕНТОВ

Аннотация: *Угрозы безопасности информации представляют особую опасность, поскольку могут привести к развитию системного кризиса финансового рынка страны и национальной платежной системы в целом. В связи с этим банкам необходимо обеспечивать должный уровень защиты информации, связанной с аутентификационными данными клиентов, путем внедрения конкретных организационных и технологических решений. В настоящей статье рассмотрены отдельные положения законодательства, направленные на обеспечение банками защиты информации с целью сокращения количества и объемов операций, проведенных без согласия клиентов.*

Ключевые слова: *несанкционированное списание средств, защита информации, безопасность финансовых операций, системы фрод-мониторинга, информационное взаимодействие.*

Annotation: *Threats to information security are particularly dangerous, as they can lead to the evolution of the crisis in the country's financial market and the national payment system. In this regard, banks need to provide the appropriate level of customer's authentication data protection by introducing specific organizational and technological solutions. This article reviews selected provisions of various acts aimed at ensuring banks' information protection in order to reduce the number and volume of of unauthorized funds transfer.*

Key words: *unauthorized funds transfer, information security, security of financial operations, fraud monitoring systems, exchange of information.*

В связи с распространением использования дистанционных способов расчетов и проведения платежей банки вынуждены непрерывно совершенствовать собственные системы фрод-мониторинга (от англ. fraud – мошенничество). Данные системы отслеживают полный профиль клиентских операций, представленный не только набором персональных данных, но и комплексом характерных приходно-расходных операций со всеми используемыми клиентом устройствами. Обладая соответствующими данными о профиле клиента, банк в случае отклонения от таких показателей может приостановить операцию по счету и уточнить детали и намерение клиента ее совершить. Цель такого взаимодействия – установить, действительно ли клиент совершает данную операцию.

Данные системы в целом могут быть достаточно эффективны, однако для их создания и настройки требуется привлекать разработчиков, имеющих серьезные компетенций в данной области. Кроме того, содержание и развитие подобных технологических решений обходится достаточно дорого в финансовом плане.

Тем не менее, даже при активном использовании таких систем фрод-мониторинга не удается констатировать факт уменьшения количества операций, связанных с получением несанкционированного доступа к счету и списанию денежных средств на счета третьих лиц.

В настоящее время законодательством Российской Федерации в области национальной платежной системы установлена обязанность для операторов по переводу денежных средств до списания денежных средств со счета отправителя осуществлять проверку операции на предмет ее соответствия признакам операций без согласия. Банк России осуществляет формирование и ведение базы данных о случаях и попытках осуществления переводов денежных средств без

согласия клиента в целях обеспечения защиты информации при осуществлении переводов денежных средств[1].

Соответственно, Банк России, будучи основным регулятор финансовой системы страны, осознает реальную необходимость разработки и внедрения конкретных мер участниками рынка по минимизации риска осуществления операций без согласия клиентов, а также необходимость их дальнейшего развития. В общих чертах порядок реализации мер по противодействию переводов средств без согласия клиента описан в Указании Банка России от 08.10.2018 № 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".

Согласно данному Указанию участники информационного обмена (операторы по переводу денежных средств, операторы платежных систем, операторы услуг платежной инфраструктуры) должны направлять в Банк России информацию о переводах без согласия клиента в виде электронных сообщений при наступлении следующих событий:

- при получении уведомлений от клиентов о случаях и (или) попытках переводов средств без согласия клиента;

- при выявлении операций, которые соответствуют признакам осуществления перевода денежных средств без согласия клиента;

[1] Ч. 5 ст. 27 О национальной платежной системе: федер. закон РФ от 27 июня 2011 г. № 161-ФЗ [Электронный ресурс] // Собр. законодательства РФ. – 2011. – № 27, ст. 3872. – Доступ из справ.-правовой системы «КонсультантПлюс».

- при выявлении операций по переводу средств, совершенных в результате несанкционированного доступа к объектам информационной инфраструктуры банка;

- при получении уведомлений от участников платежной системы о списании денежных средств с их корреспондентских счетов без их согласия;

- при обнаружении компьютерных атак.

Другими словами, оператор по переводу денежных средств, получивший уведомление от клиента о выявлении им операции без его согласия, должен в срок, не превышающий одного рабочего дня с даты получения обращения, уведомить Банк России о факте данной операции. Для этого в Банке России на базе Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ) внедрена автоматизированная система «Фид-АнтиФрод». В течение 2019 года соответствующий интерфейс проходил испытания и был доступен для участников в тестовом режиме.

Дополнительно по каждой операции без согласия в рамках промежуточного уведомления оператор по переводу денежных средств, обслуживающий отправителя, имеет возможность на основании сведений, предоставленных клиентом, направить в Банк России информацию о номере обращения клиента в полицию. Таким образом, при должной активности граждан в части защиты своих прав и обращении их в правоохранительные органы в Банке России формируется возможность корреляции фактов обращения граждан в правоохранительные органы по операциям без согласия, сведений о самих операциях и их получателях. Указанную информацию в рамках межведомственного взаимодействия Банк России может направлять в МВД России для повышения уровня раскрываемости преступлений, в случае, когда денежные средства, переводимые в рамках операции без согласия, снимаются получателем.

Согласно Закону о ЦБ РФ целями деятельности Банка России являются укрепление банковской системы РФ, развитие и обеспечение стабильности

финансового рынка страны и национальной платежной системы[2]. Одним из ключевых условий реализации данных целей является обеспечение необходимого и достаточного уровня защиты информации в кредитных организациях, некредитных финансовых организациях РФ, а также субъектах национальной платежной системы.

Так, с непосредственным участием ЦБ РФ для целей обеспечения эффективности и возможности стандартизированного контроля мероприятий по защите информации, проводимых финансовыми организациями, был разработан ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер»[3].

Данный стандарт определяет для финансовых организаций 3 уровня защиты информации (минимальный, стандартный, усиленный) и устанавливает соответствующие требования к их защите.

Так, например, к мерам защиты информации по идентификации и аутентификации клиента относится временная блокировка учетной записи пользователей не менее чем на 30 мин. после выполнения ряда неуспешных попыток аутентификации; автоматическое прерывание сессии доступа по истечении 15 минут с прекращением отображения на мониторе информации, доступ к которой был получен ранее; а также необходимость повторной аутентификации для продолжения работы с системой «Банк-Клиент» после ее принудительного или автоматического прерывания.

К мерам защиты по организации управления и организации защиты идентификационных и аутентификационных данных относятся, например, смена пароля пользователей не реже одного раза в год; использование пользователями

[2] Ст. 3 О Центральном банке Российской Федерации (Банке России): федер. закон РФ от 10 июля 2002 г. № 86-ФЗ [Электронный ресурс]: принят Гос. Думой 27 июня 2002 г. // Собр. законодательства РФ. – 2002. – № 28, ст. 2790. – Доступ из справ.-правовой системы «КонсультантПлюс».

[3] ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» [Электронный ресурс]. М.: Стандартинформ. 2017. Доступ из справ.-правовой системы «КонсультантПлюс».

паролей длиной не менее восьми символов и включение в него букв и цифр; запрет на использование в качестве паролей легко вычисляемых сочетаний (имена, фамилии, общепринятые сокращения, наименования и др.).

В контексте исследования гражданско-правовой ответственности за несанкционированные списания целесообразно будет выделить следующие меры защиты информации, которые, вероятно, позволят сократить количество несанкционированных списаний денежных средств со счетов клиентов:

- контроль отсутствия (выявление) аномальной сетевой активности, связанной с возможным несанкционированным удаленным доступом к аутентификационным данным клиента;

- контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации, использование которых может позволить осуществить несанкционированный доступ к ресурсам, размещенным во внутренних вычислительных сетях финансовой организации;

- выполнение еженедельных операций по проведению проверок на отсутствие вредоносного кода;

- реализация защиты от вредоносного кода на уровне контроля общедоступных объектов доступа (в том числе банкоматов, платежных терминалов).

Согласно данным[4], подготовленным специалистами АО «Консультант Плюс», финансовые организации распределены следующим образом в соответствии с тремя уровнями защиты информации, которые им нужно будет соблюдать:

- Усиленный уровень защиты информации в своей деятельности необходимо будет обеспечить системно значимым кредитным организациям и центральным контрагентам;

- ««обычные» кредитные организации, а также крупные страховые компании (те, активы которых за последние 6 месяцев на 31 декабря года,

[4] ЦБ РФ определил, какие банки и НФО будут соблюдать самые строгие требования защиты от киберугроз [Электронный ресурс]: обзор специалистов АО «КонсультантПлюс». 2019. Доступ из справ.-правовой системы «КонсультантПлюс».

предшествующего дате определения уровня, превышали 20 млрд руб.)» вынуждены будут обеспечивать стандартный уровень защиты;

- Микрофинансовые организации и ламбады - минимальный уровень.

ГОСТ Р 57580.2-2018 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия»[5] был утвержден для оценки соответствия защиты информации финансовых организаций согласно организационным и техническим мерам ГОСТ Р 57580.1-2017. Для оценки полноты реализации процессов защиты информации используют следующую «шкалу оценивания»: нулевой уровень соответствия; первый уровень; второй; третий; четвертый; пятый.

Так, согласно пп. 9.2 Положения Банка России № 683-П[6] кредитные организации должны соответствовать третьему уровню защиты к 1 января 2021 г., который предполагает, что меры защиты информации реализуются *в значительном количестве* на постоянной основе в соответствии с общими подходами (способами), установленными в финансовой организации. Контроль и совершенствование реализации данных мер защиты *осуществляются бессистемно и/или эпизодически*.

Более того, уровень соответствия не ниже четвертого, когда меры защиты информации реализуются в *полном* объеме на постоянной основе в соответствии с общими подходами, установленными в финансовой организации, а контроль и совершенствование реализации данных мер *в основном реализован*, кредитные организации должны обеспечить к 1 января 2023 года.

Итак, в настоящее время перед кредитными организациями стоят амбициозные задачи по формированию и внедрению комплексных систем, направленных на защиту банковской информации и безопасность финансовых

[5] ГОСТ Р 57580.2-2018 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия [Электронный ресурс]. М.: Стандартинформ. 2017. Доступ из справ.-правовой системы «КонсультантПлюс».

[6] 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 [Электронный ресурс]**:** Положение Банка России от 17 апреля 2019 г. № 683-П // Вестник Банка России. – 2019. – № 33. – Доступ из справ.-правовой системы «КонсультантПлюс».

операций. Однако, достаточно противоречивым в данном контексте можно назвать ответ ЦБ РФ[7], который предусматривает следующее: «в качестве причин невозможности технической реализации мер защиты информации полагаем допустимым указывать такие, как: 1) отсутствие на рынке технических решений российского производства, обеспечивающих необходимую эффективность и функциональность; 2) возможные западные санкции и опасность/невозможность использования решений иностранных производителей. При этом такие обоснования должны базироваться на подтвержденных факт, а не на предположениях».

Очевидно ли то, что отдельные информационные кластеры могут остаться без должного внимания и уровня защиты в связи с ранее упомянутыми причинами – утверждать сложно. Тем не менее, остается лишь надеяться на то, что, соответствуя данным ГОСТам, кредитным организациям удастся обеспечить достойный уровень информационной безопасности своих систем, что позволит в ближайшем будущем значительно сократить количество инцидентов, связанных с получением несанкционированного доступа третьими лицами к счетам клиентов и последующего списания денежных средств.

Использованные источники:

1. Федеральный закон от 27.06.2011 г. № 161-ФЗ «О национальной платежной системе» [Электронный ресурс] // Собр. законодательства РФ. – 2011. – № 27, ст. 3872. – Доступ из справ.-правовой системы «КонсультантПлюс».

2. Федеральный закон от 10.07.2002 г. № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» [Электронный ресурс]: принят Гос. Думой 27 июня 2002 г. // Собр. законодательства РФ. – 2002. – № 28, ст. 2790. – Доступ из справ.-правовой системы «КонсультантПлюс».

3. Положение Банка России от 17.04.2019 г. № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты

[7] Об отдельных вопросах, связанных с защитой информации финансовых организаций. (Письмо Банка России от 22.05.2020 № 56-1-11/265 [Электронный ресурс]. Документ опубликован не был. Доступ из справ.-правовой системы «КонсультантПлюс».

информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента» [Электронный ресурс]**:** // Вестник Банка России. – 2019. – № 33. – Доступ из справ.-правовой системы «КонсультантПлюс».

4. Указание Банка России от 08.10.2018 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» [Электронный ресурс]: // Вестник Банка России. – 2018. – № 98. – Доступ из справ.-правовой системы «КонсультантПлюс».

5. ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» [Электронный ресурс]. М.: Стандартинформ. 2017. Доступ из справ.-правовой системы «КонсультантПлюс».

6. ГОСТ Р 57580.2-2018 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия [Электронный ресурс]. М.: Стандартинформ. 2017. Доступ из справ.-правовой системы «КонсультантПлюс».

7. Письмо Банка России от 22.05.2020 г. № 56-1-11/265 «Об отдельных вопросах, связанных с защитой информации финансовых организаций» [Электронный ресурс]. Документ опубликован не был. Доступ из справ.-правовой системы «КонсультантПлюс».

8. Обзор специалистов АО «КонсультантПлюс» 2019 г. «ЦБ РФ определил, какие банки и НФО будут соблюдать самые строгие требования защиты от киберугроз» [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».