Секция «Информационное общество, цифровая экономика и информационная безопасность»

Особенности применения электронного банкинга в России

Научный руководитель – Зуева Анна Сергеевна

Федосеева Виктория Александровна
Студент (магистр)
Московский государственный университет имени М.В.Ломоносова, Высшая школа государственного аудита, Кафедра информационной безопасности и компьютерного права, Москва, Россия
E-mail: victoriafedoseeva98@gmail.com

На сегодняшний день имеется спрос на безналичные формы расчетов, которые обладают определёнными преимуществами, если сравнивать с наличными денежными оборотам, к ним можно отнести, к примеру, высокую скорость, применимость на отдаленных территориях и другие. Так как потребности в использовании возрастают, совершенствуются формы расчетов, один из таких способов - это Интернет-банкинг. Сегодня мы уже не можем представить сферу банковских услуг без Интернет-банкинг.

С помощью Интернет-банкинг предоставляются банковские услуги через интернет, другими словами появляется возможность использовать банковские услуги каждый день круглосуточно в любой точке мира, которая имеет доступ к Интернету. Такой вид предоставления банковских услуг наиболее перспективный и на сегодняшний день развивается, что позволяет коммерческим банкам активно взаимодействовать с клиентами. Центральный Банк даёт следующее определение интернет-банкингу, как «способу дистанционного банковского обслуживания клиентов, который осуществляется кредитными организациями в сети Интернет и включает информационное и операционное взаимодействие с ними».

Преимущества, которые предоставляет Интернет-банкинг: сократить время на совершение операций и их обработку; появляется возможность круглосуточно контролировать состояние счета, проводить онлайн-платежей без задержек; осуществлять операции без личного присутствия владельца счета; нет привязки к определенному местонахождению, чтобы осуществлять операции.

Можно выделить следующие основные характеристики системы Интернет-банкинга: функциональные возможности, которые обеспечивают доступ клиентов к операциям, более широкий доступ к банковским услугам; удобство пользовательского интерфейса, который облегчает использование системы клиентами: более понятные и простые в установке, удобное выполнение определённых операций банковских услуг; уровень обеспечения безопасности передачи и хранения финансовой информации, то есть данные носителей защищены.

Широкое использование интернет-банкинга можно обусловить следующими взаимосвязанными факторами: в эпоху глобализации рынков, повышенной бизнес-конкуренции клиенты банков должны иметь возможность осуществлять мгновенные и удобные финансовые операции, и в виду такого спроса появляются предложения такого способа оказания услуг; не применяя интернет-банкинг на сегодняшний день, банк исключается из конкурентной борьбы в сфере оказания банковских услуг; банки также имеют плюс для себя, потому что сокращаются материальные и временные затраты.

Спектр услуг, который предоставляется банками с помощью Интернета законодательно не ограничивается. Несмотря на то, что специальными законодательными актами российский интернет-банкинг не регулируется, использование интернет-банкинга при оказании

банковских услуг никак не ограничивается. Согласно статье 847 ГК РФ, которая устанавливает порядок распоряжения денежными средствами, предполагается, что Договором может быть предусмотрено удостоверение прав распоряжения денежными суммами, которые находятся на счете, электронными средствами платежа и иными способами с использованием в них аналогов собственноручной подписи, кодов, паролей и других средств, которые подтверждают, что распоряжение даётся уполномоченным на это лицом. Поэтому, чтобы использовать интернет-банкинга, необходима только аутентификация клиента.

Сегодня сфера интернет-банкинга достаточным образом регулируется законодательством РФ. К примеру, «Налоговым кодексом РФ (часть вторая)» от 05.08.2000 № 117-ФЗ статьёй 149 «Операции, не подлежащие налогообложению (освобождённые от налогообложения)». Оказание услуг, связаные с установкой и эксплуатацией системы «клиент-банк», не подлежат налогообложение на территории РФ. К важным регулирующим документам относится «Приложение к письму Банка России от 31.03.2008 № 36-Т», в котором даются рекомендации, чтобы организовывать управление рисками, которые возникают в процессе осуществления кредитными организациями операций с применением систем интернет-банкинга.

Кроме этого документ «Указание Банка России от 12.11.2009 № 2332-У «О перечне, формах и порядке составления и предоставления форм отчётности кредитных организаций в Центральный Банк РФ» определяет порядок по составлению и предоставлению отчётности по форме 0409070 «Сведения об использовании кредитной организацией интернет-технологий».

Несмотря на то, что такой институт перспективный и привлекательный для клиентов, он имеет серьезные недостатки, которые способны заставить клиентов отказаться от услуг банка.

На сегодняшний день банки не могут не использовать интернет-банкинг, однако серьезные риски использования такой системы отрицательно влияют на оказания услуг. Основной проблемой для самого банка являются проблемы DDoS атак. Под DDoS атакой понимается атака на сайт, её основная цель -вывести из строя сайт, используя большое количество ложных запросов. Такая атака приводит к тому, что сервера, которые обслуживают сайт, обрабатывают огромное количество ложных запросов, из-за чего сайт становится недоступен обычному пользователю. Такие атаки чаще всего направлены не для того, чтобы завладеть денежными средствами, а, чтобы испортить репутацию и вывести из строя конкурентоспособность банка: сервера, который не функционируют даже в течение получаса, могут привести к тому, что большая часть клиентов будет отказываться от услуг этого банка.

Данная угроза очень серьезна для банков из-за неудобства для клиентов, которые привыкли иметь доступ к банковским услугам круглосуточно. В виду этого банки затрачивают немалые ресурсы и приобретают альтернативные серверы, чтобы переходить на низ при атаке. Однако не исключается и такая угроза, как хищение персональных данных клиентов, что, помимо морального вреда, который причиняется клиентам, будет негативно отражаться на репутации банка.

Также актуальный недостаток интернет-банкинга - это возможность хищения денежных средств клиента, применяя вирусные программы, фишинговые сайты и другие способы, чтобы завладеть значимой информацией.

Последний случай - частый предмет спора между клиентом и банком. Обычно в таких случаях клиент заявляет банку иск о взыскании денежных средств и компенсации морального вреда. В судебной практике также бывают случаи мошенничества со стороны клиентов, когда ими перечисляются денежные средства на счета знакомых лиц, однако делают запрос о том, что перевод не был ими выполнен и их интернет-банк подвергся взло-

му злоумышленников. В таком случае, клиент должен предъявить, что им был выполнен перевод денежных средств. Поэтому банк настаивает на том, что электронная цифровая подпись принадлежит клиенту, следовательно, по мнению банка, перевод осуществлен клиентом.

Отметим, что отношения между клиентом и банком основываются на договоре оказания услуг, поэтому их отношения законодательно регулируются в том числе ФЗ "О защите прав потребителей". Поэтому истец чаще всего ссылается на несоответствие услуги, которая предоставляется интернет-банкингом и их требованиям безопасности.

Согласно статье 1095 ГК РФ, вред, который причиняется имуществу гражданина из-за конструктивных, рецептурных или иных недостатков услуги, а также из-за недостоверной или недостаточной информации об услуге, должно возмещаться лицом, которое оказывало услугу, то есть исполнителем, вне зависимости виноват он или нет его вины. Можно сделать вывод, хищение денежных средств в сфере интернет-банкинга формально подпадает под вред, который причиняет банк безвиновно.

Но ГК содержатся положения, которые отражаются в статье 1098, по которым исполнитель услуги может быть освобождён от ответственности, если докажет, что вред возник вследствие непреодолимой силы или нарушения потребителем правил пользования, которые были установлены. Поэтому с помощью огромного перечня таких правил, с которыми клиент соглашается, заключая договор с банком, исполнитель услуги, то есть банк, чаще всего выигрывает в таких делах.

Основные правила, чаще всего, выглядят следующим образом: клиент не сообщает третьим лицам, в том числе сотрудникам банка, одноразовые пароли, PIN-коды и CVV-коды, потому что по правилам эту информацию получает только клиент; клиентом используются исключительно официальные сайты и приложения; меняя номер мобильного телефона, клиент сообщает об этом факте банку, чтобы новый владелец номера не смог получать данные клиента, благодаря которым можно получать доступ к онлайн-банку.

Если клиентом нарушены правила, которые устанавливаются банком, этот факт делает невозможным взыскание денежных средств. Но в интересах банка минимизация таких споры, чтобы сохранить репутацию и клиентскую базу. Это, по нашему мнению, можно осуществить следующими способами: обширно информировать население о способах защиты от злоумышленников в сфере интернет-банкинга; технически увеличить безопасное пользование интернет-банкинга. Такой подход находит отражение в п. 4 Письма Банка России № 146-Т. Вторым способом, кроме использования качественных антивирусных программ, может обеспечиваться повышенным уровнем идентификации и аутентификации клиента. Прежде всего, нужно разобраться с разграничением понятий идентификации и аутентификации. Как правильно отмечает В. Ференец, идентификация - процесс определения, что за человек перед нами, а аутентификация - процесс подтверждения, что этот человек именно тот, за кого себя выдает.

Элементами аутентификации являются субъект и его характеристика. Характеристики субъекта делятся на следующие факторы: I know (что я знаю): к данному фактору относятся пароли, ПИН-коды, ключевые слова и т.д.; I have (что у меня есть): это, как правило, смарт-карты, брелки, банковские карты с технологией PayPass; I am (что я есть): в первую очередь, это отпечатки пальцев, рисунок сетчатки глаза, тембр голоса и другие биометрические показатели. Аутентификация только по одному из вышеперечисленных факторов называется однофакторной. Использование первого и второго факторов по одиночке небезопасно для для финансовых организаций, а биометрического - слишком дорогостояще. Поэтому чаще всего в интернет-банкинге используется сочетание фактора "I know" и фактора "I have", что называется двухфакторной или многофакторной аутентификацией. Процесс двухфакторной аутентификации клиента в интернет-банкинге

осуществляется следующим образом: клиент осуществляет вход в личный кабинет посредством ввода пароля (фактор "I know"), после чего клиенту посредством СМС-сообщения высылается одноразовый пароль на мобильный телефон, который, как подразумевается, всегда находится у клиента (фактор "I have").

Поэтому, в отсутствие специального правового регулирования отношений в сфере интернет-банкинга сочетание информационных и технических инструментов поможет банкам сократить случаи неправомерного завладения денежными средствами клиента, и, как следствие, сократить количество судебных споров банков и их клиентов по этому поводу, что благоприятно скажется на репутации банков и безопасности их клиентов.

Помимо всего этого, с технической точки зрения, было бы целесообразно ввести систему подтверждения операции посредством кодов, генерирующихся в интервале одной минуты, на личном переносном устройстве типа брелок, как это применяется в Европе. Данная система поможет предупредить риски возникновения мошеннических операции.

Источники и литература

1) Гражданский кодекс Российской Федерации, часть вторая от 26.01.1996 N 14-ФЗ // Собрание законодательства РФ. 1996. (в ред. от 23.05.2018).
2) Козлов С.В. Некоторые аспекты правового регулирования дистанционного банковского обслуживания // Банковское право. - 2014. - №3. - С.57-65.
3) Письмо Банка России N 36-Т "О Рекомендациях по организации управления рисками, возникающими при осуществлении кредитными организациями операций с применением систем Интернетбанкинга"//Вестник Банка России. 09.04.2008. N 16.
4) Письмо Банка России № 141-Т «О рекомендациях по подходам кредитных организаций к выбору провайдеров и взаимодействию с ними при осуществлении дистанционного банковского обслуживания». // СПС КонсультантПлюс.
5) Письмо Банка России от 05.08.2013 № 146-Т "О рекомендациях по повышению уровня безопасности при предоставлении розничных платежных услуг с использованием информационно-телекоммуникационной сети "Интернет"// СПС КонсультантПлюс.
6) Савельев Д.Б. Гражданско-правовые аспекты распределения рисков в интернет-банкинге//Банковское право. - 2016. - №3. - С. 31-36.
7) Ференец В. Банкинг начинается с аутентификации//Банковское обозрение. - 2017. - №2.
8) Бурмистрова Полина Дмитриевна, Шаталова Елена Петровна Дистанционное банковское обслуживание как средство модернизации банковских услуг // Вестник ГУУ. 2018. №11. URL: https://cyberleninka.ru/article/n/distantsionnoe-bankovskoe-obsluzhivanie-kak-sredstvo-modernizatsii-bankovskih-uslug (дата обращения: 01.03.2020).
9) Ревенков П.В. Электронный банкинг: риск взаимодействия с провайдерами // Финансы и кредит. 2011. №17 (449). URL: https://cyberleninka.ru/article/n/elektronny-banking-risk-vzaimodeystviya-s-provayderami (дата обращения: 01.03.2020).
10) Митрохин В.В., Дьякова О.Н. К вопросу о классификации системы дистанционного банковского обслуживания // Финансы и кредит. 2012. №17 (497). URL: https://cyberleninka.ru/article/n/k-voprosu-o-klassifikatsii-sistemy-distantsionnogo-bankovskogo-obsluzhivaniya (дата обращения: 01.03.2020).
11) Вестник Банка России. 09.04.2008. N 16.