КТО ОТВЕЧАЕТ ЗА НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП К УСЛУГАМ СВЯЗИ В ИНТЕРНЕТЕ?

Комментарий к Постановлению Президиума ВАС РФ от 18.09.2012 № 3933/12 по делу «ОАО „Южная телекоммуникационная компания" против ИП Перцовкиной Т.Ф.»

ОАО «Ростелеком» (правопреемник ОАО «Южная телекоммуникационная компания») и ИП Перцовкина Т.Ф. заключили возмездный договор о предоставлении доступа в Интернет по технологии *ADSL*. Поскольку услуги не были оплачены в полном объеме, ОАО «Ростелеком» обратилось в арбитражный суд с иском о взыскании задолженности в сумме около 224 тыс. руб. Предприниматель, возражая против иска, отметил, что указанная задолженность образовалась в связи с противоправным доступом к его логину и паролю.

Арбитражные суды Северо-Кавказского округа удовлетворили исковые требования ОАО «Ростелеком», посчитав, что несанкционированный доступ к логину и паролю не освобождает предпринимателя от оплаты услуг. При этом суды исходили из условий договора, согласно которым предприниматель был обязан сохранить логин и пароль от хищения, а также нести ответственность за услуги, полученные с использованием его данных.

Коллегия судей ВАС РФ, передавая дело в Президиум, с позицией нижестоящих судов не согласилась. Суды, отметив обязанность предпринимателя по защите логина и пароля от доступа третьих лиц, при этом не указали, какие конкретные действия он был обязан совершить. Судьи ВАС РФ пришли к выводу, что вынесенные по делу судебные акты возложили на предпринимателя обязанность по оплате услуг, которыми он не пользовался. Однако, отметила коллегия, в судебной практике сложился и иной подход, согласно которому незаконное использование логина и пароля абонента освобождает последнего от обязанности оплаты неоказанных услуг.

Президиум ВАС РФ решения нижестоящих судов отменил и направил дело на новое рассмотрение. В Постановлении от 18.09.2012 № 3933/12 (далее – Постановление № 3933/12) Президиум ВАС РФ отметил, что нижестоящие суды в своих решениях не указали, какие конкретно действия, предусмотренные законом или договором, должен был совершить и не совершил абонент. При этом согласно Правилам оказания телематических услуг связи (утверждены Постановлением Правительства РФ от 10.09.2007 № 575; далее – Правила) меры по защите абонентского терминала от воздействия вредоносного программного обеспечения возложены как на абонента, так и на оператора. Федеральный за-

кон от 07.07.2003 № 126-ФЗ «О связи» (далее — Закон о связи) также возлагает на операторов связи обязанность обеспечивать защиту средств связи и сооружений связи от несанкционированного доступа к ним. Президиум ВАС РФ отметил, что данные обстоятельства нижестоящими судами не исследовались.

Юрий Александрович Воробьев,
руководитель практики разрешения споров и медиации «Пепеляев Групп»

В данном деле ВАС РФ рассмотрел достаточно болезненный аспект предоставления телематических услуг связи — вопрос о несанкционированном доступе к этим услугам третьих лиц.

При рассмотрении дела судами трех уровней было установлено, что обязанность по оплате услуг связи возникает вне зависимости от доказанности факта доступа и факта получения этих услуг (несанкционированного) третьими лицами. В рамках данного дела факт хищения идентификатора (логин и пароль) клиента был подтвержден вступившим в законную силу приговором суда. Позиция судов при этом сводилась к тому, что клиент обязан принять меры к обеспечению сохранности собственной информации и несет материальную ответственность за услуги, полученные с использованием его данных третьими лицами до момента письменного обращения к оператору о блокировке. Оператор же не несет ответственности за ущерб, причиненный клиенту третьими лицами.

Президиум ВАС РФ направил дело на новое рассмотрение, указав, что и из нормативных актов, и из договора следует, что защита средств связи и сооружений связи от несанкционированного доступа возложена на операторов связи. Оператор связи обладает техническими средствами, позволяющими обеспечить мониторинг «подозрительной» сигнальной нагрузки, и это одна из мер по предотвращению несанкционированного доступа. В такой ситуации на основании ст. 312 ГК РФ оператор связи был обязан потребовать доказательства того, что исполнение принимается самим клиентом или уполномоченным им лицом (риск последствий непредъявления таких требований ложится на оператора связи).

Не менее важен и вывод Президиума ВАС РФ относительно разграничения понятий ответственности по договору и оплаты оказанных услуг. Так, занимая позицию операторов связи, суды сослались (как указано выше) на положения договора, устанавливающие ответственность за необеспечение сохранности идентифицирующей информации. Президиум ВАС РФ же объявил, что вопрос договорной ответственности нельзя смешивать с оплатой услуги (исполнением самого обязательства клиентом).

Таким образом, Президиум ВАС РФ, направив дело на новое рассмотрение, дал указание судам исследовать фактические обстоятельства дела с учетом этих правовых позиций.

Однако значение Постановления № 3933/12 состоит в том, что содержащиеся в нем правовые позиции и подходы могут быть применены к куда более широкому кругу отношений (использование банковских карт, систем интернет-оплаты и пр.), при разрешении споров, в отношении которых ранее применялся более формальный подход.

Яна Андреевна Чирко,
юрист международной юридической фирмы *Dentons*

Вопрос ограничения обязательств и ответственности владельца или оператора авторизационных данных (*ID*) в связи с хищением и неправомерным использованием *ID* кибермошенниками, затронутый в Постановлении № 3933/12, является весьма актуальным. Ни в России, ни в США и Европе не сложилось единого подхода к разрешению данной проблемы. Согласно концепции *identity theft*, а также законодательству, принятому множеством иностранных государств в развитие данной концепции (к примеру, *US Identity Theft and Assumption Deterrence Act, US FTC Safeguards Rule, UK Theft Act* 1968), при разрешении споров между владельцем и оператором *ID* в связи с убытками, возникшими вследствие киберхищений *ID*, суды, как правило, принимают сторону владельца *ID* (потребителя).

При разрешении таких споров анализируются следующие вопросы:

- предпринял ли оператор *ID* все необходимые и достаточные меры для обеспечения компьютерной безопасности своих систем, в том числе для обеспечения безопасности баз данных *ID*;
- известил ли пользователей о мероприятиях, которые необходимо предпринять для защиты *ID* от несанкционированного доступа;
- предпринял ли надлежащие технические меры в отношении безопасности обработки *ID* как персональных данных,

и др.

При этом само киберхищение *ID* по отношению к владельцу *ID* рассматривается как непредвиденное обстоятельство, а обязательства владельца *ID* по обеспечению его сохранности, как правило, имеют исключительно договорную природу (кроме киберхищений *ID* в банковской сфере).

Сходные принципы разграничения обязательств и ответственности владельца или оператора *ID* заложены и в российском законодательстве, нормы которого анализировались Президиумом ВАС РФ при вынесении комментируемого Постановления, а также принимались во внимание судами при разрешении иных аналогичных споров (Определения ВАС РФ от 08.04.2011 № ВАС-3978/11 по делу № А75-4446/2010, от 20.09.2012 № ВАС-8496/12 по делу № А19-8988/2011 и др.).

Так, п. 28 Правил в качестве обязательства пользователя предусматривает лишь совершение действий, препятствующих распространению вредоносного программного обеспечения с его абонентского терминала, что неприменимо

для рассматриваемого спора. При этом в обязательства оператора входит целый перечень мероприятий по информированию абонента и предотвращению несанкционированного доступа к линиям и средствам связи оператора.

Признавая, что меры по защите абонентского терминала возложены как на абонента, так и на оператора, но при этом констатируя необоснованность взимания платы за услуги оператора в рассматриваемом случае, Президиум ВАС РФ не анализирует причины киберхищения *ID*, возможности абонента предвидеть и предотвратить такое хищение, а также не оценивает факт несообщения абонентом оператору о несанкционированном доступе к *ID* на протяжении полутора лет.

Отметим, что в силу ст. 401 ГК РФ лицо признается невиновным, если при той степени заботливости и осмотрительности, какая от него требовалась по характеру обязательства, оно приняло все меры для надлежащего исполнения обязательства. Следовательно, если *ID* абонента были похищены в связи с неосторожностью самого абонента, этот факт может существенно повлиять на вывод об ограничении обязательства абонента по оплате услуг оператора. Своевременность извещения оператора о том, что услуги абоненту не оказаны (но при этом учтены и требуют оплаты), является значительным фактором для целей предотвращения или уменьшения убытков, которые могут быть причинены как абоненту, так и оператору в связи с неоказанием услуги.

В соответствии с положениями Закона о связи претензии абонентов по неисполнению или ненадлежащему исполнению обязательств, вытекающих из договора об оказании услуг связи, предъявляются оператору в досудебном порядке в течение шести месяцев со дня выставления счета за неоказанную или ненадлежащим образом оказанную услугу связи. Также для решения вопроса о степени ограничения обязательств абонента по оплате услуг в связи с киберхищением *ID* необходимо учитывать положения п. 3 ст. 781 ГК РФ, в соответствии с которыми риск невозможности исполнения договора (оплаты) по обстоятельствам, за которые не отвечает ни одна из сторон, возлагается на заказчика. При этом заказчик услуги обязан возместить исполнителю фактически понесенные им расходы.

Вопрос о том, может ли и если да, то до какой степени владелец *ID* освобождаться от обязательств и ответственности в связи с киберхищением *ID*, имеет большое практическое значение. В случае если факт несанкционированного доступа третьего лица к *ID* владельца будет сам по себе достаточен для освобождения владельца *ID* от обязательств перед контрагентами, данное обстоятельство может привести к тому, что владельцы *ID* (потребители услуг) получат обоснованную свободу не уделять надлежащего внимания защите своих *ID*, а операторы *ID* (провайдеры услуг) будут нести в связи с этим неоправданные убытки.

Очевидно, что решение аналогичных споров, связанных с киберхищением *ID*, должно основываться на определенном балансе интересов субъектов спора, который будет способствовать адекватной защите *ID* абонентов операторами, но при этом не будет препятствовать нормальной практике использования интернет-технологий в рамках оказания услуг потребителям.

Многое в таких конфликтах будет зависеть от того объема взаимных прав и обязанностей и характера их детальной проработки, которые будут связаны с конкретными организационно-техническими мерами по обеспечению адекватного отношениям уровня защиты информации.