Клименко С. Н.

К вопросу о юридической ответственности за нарушения законодательства Российской Федерации в области информационной безопасности: проблемы, перспективы

Клименко Сергей Николаевич
Северо-Западный институт управления — филиал РАНХиГС (Санкт-Петербург)
Аспирант кафедры конституционного и административного права
sergklim08@mail.ru

РЕФЕРАТ
В статье автор проводит анализ законодательства Российской Федерации и ряда зарубежных стран, устанавливающего правовую ответственность за нарушения в области информационной безопасности. Исследована динамика правонарушений, выявлены проблемы, изложены перспективы развития законодательства.
В статье использованы теоретические материалы таких авторов, как Д. Н. Бахрах [1], И. Л. Бачило [2], Т. А. Кухаренко [4], диссертационные исследования А. А. Стрельцова [6], а также справочная информация из толкового словаря С. И. Ожегова и Н. Ю. Шведовой [5].

КЛЮЧЕВЫЕ СЛОВА
информационная безопасность, юридическая ответственность

Klimenko S. N.

About Legal Responsibility for Violations of the Low of the Russian Federation in the Field of Information Security: Problems and Prospects

Klimenko Sergey Nikolaevich
North-West Institute of Management — branch of the Russian Presidential Academy of National Economy and Public Administration (Saint-Petersburg, Russian Federation)
Graduate student of the Chair of the Constitutional and Administrative Law
sergklim08@mail.ru

ABSTRACT
The author analyses the legislation of the Russian Federation and foreign countries which establishes legal responsibility for irregularities in the field of information security. The research of crime dynamics has been done, the problems have been revealed and the prospects for the legislation development have been outlined. The article contains theoretical materials by such authors as D. N. Bakhrakh, I. L. Bachilo, T. A. Kukharenko, dissertation research A. A. Streltsov, as well as background information S. I. Ozhegov and N. Yu Shvedova.

KEYWORDS
information security, legal responsibility

Развитие общественных отношений в информационной сфере, возникновение новых вызовов в сфере безопасности информации в значительной степени повышают значимость и остроту проблемы адекватного на них реагирования.

Федеральными органами государственной власти, осуществляющими функции в сфере обеспечения информационной безопасности, в последнее время фиксируется значительное увеличение количества компьютерных атак на информационные системы и информационно-телекоммуникационные сети органов государственной власти, особенно при использовании ими сервисов, расположенных вне юрисдикции Российской Федерации. Кроме того, в информационных системах органов

государственной власти все чаще обнаруживаются программные средства иностранных технических разведок.

Совершенно очевидно, что возникающие угрозы существенным образом увеличивают риски в управлении информационной безопасностью. Как следствие — необходимость принятия действенных мер, направленных на дальнейшее совершенствование системы обеспечения информационной безопасности, важнейшим элементом которой является ее правовое обеспечение, регулируемое не только межгосударственными договорами, конвенциями, декларациями, но и патентами, авторским правом, лицензиями на их защиту, а также государственными и ведомственными нормативными правовыми актами [6, с. 109].

В связи с этим, как представляется, основная проблема противодействия нарушениям в области информационной безопасности находится в плоскости правового регулирования информационных отношений.

Формирование информационного законодательства и права в Российской Федерации осуществляется достаточно быстрыми темпами, что подтверждает значительное количество принятых нормативных правовых актов в этой сфере за последние несколько лет. Тем не менее, приходится констатировать, что становление законодательства в области информации, информационных технологий все еще отстает от развития информационных ресурсов, информационных услуг и средств информационного производства в стране.

Сложность проблемы, в сущности, заключается в том, что правовые нормы в сфере информационной безопасности, существенно влияя на качество регулирования отношений субъектов, практически во всех сферах жизни страны, оказывают безусловное воздействие и на развитие законодательства в этой области.

Система законодательства в сфере обеспечения информационной безопасности, если рассматривать ее в общем виде [3, с. 29], включает в себя, с одной стороны, правовые акты, в той или иной степени направленные на достижение обозначенных целей обеспечения информационной безопасности, образуя при этом основу для формирования целостной системы информационной безопасности.

К указанной категории можно отнести Конституцию Российской Федерации, Гражданский кодекс Российской Федерации, Закон Российской Федерации «О государственной тайне», Федеральные законы Российской Федерации «О безопасности», «Об информации, информационных технологиях и о защите информации», «О связи» и многие другие.

С другой стороны, нормативные правовые акты, закрепляющие меры предупредительно-карательного характера, главным образом, Уголовный кодекс Российской Федерации, Кодекс Российской Федерации об административных правонарушениях, а также ведомственные правовые акты.

Таким образом, одновременно с институтами права на информацию, правового режима информационных ресурсов и информационных технологий, институтов защиты информации, а также информационной безопасности в целом действует и институт ответственности, представляющий собой систему норм и процедур, реализация которых направлена на пресечение правонарушений, а также на установление вида, формы и мер наказания за совершенные и доказанные преступления или иные правонарушения с учетом их социального вреда и вины правонарушителя.

Уголовный кодекс Российской Федерации (далее — УК РФ)[1] включает в себя набор статей, направленных на регулирование правоотношений в области обеспечения информационной безопасности. Речь, в частности, идет о таких пре-

[1] Уголовный кодекс Российской Федерации: Федеральный закон Российской Федерации от 13.06.1996 № 63-ФЗ (в действ. ред.) // Собрание законодательства Российской Федерации. 1996. № 52. Ст. 2954.

ступлениях, как «Нарушение неприкосновенности частной жизни» (ст. 137), «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений» (ст. 138), «Незаконный оборот специальных технических средств, предназначенных для негласного получения информации» (ст. 138.1), «Отказ в предоставлении гражданину информации» (ст. 140), «Разглашении тайны усыновления (удочерения)» (ст. 155), «Мошенничество в сфере компьютерной информации» (ст. 159.6), «Незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну» (ст. 183). К этой категории можно отнести ст. 185.1 «Злостное уклонение от раскрытия или предоставления информации, определенной законодательством Российской Федерации о ценных бумагах», ст. 185.3 «Манипулирование рынком», ст. 185.6 «Неправомерное использование инсайдерской информации», ст. 237 «Сокрытие информации об обстоятельствах, создающих опасность для жизни или здоровья людей».

В отдельную главу Кодекса выделены преступления в сфере компьютерной информации (гл. 28 УК РФ). К таким преступлениям следует отнести «Неправомерный доступ к компьютерной информации» (ст. 272), ст. 273 «Создание, использование и распространение вредоносных компьютерных программ», а также «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» (ст. 274).

Вполне очевидно, что правовое регулирование общественных отношений по поводу использования, распространения и защиты информации в целом и отдельных ее видов в частности представляет наибольший интерес.

Бесспорно, важнейшим элементом общей системы информационной безопасности государства является правовой институт государственной тайны.

Правовой режим государственной тайны в целом включает в себя три составляющие [3, с. 56]. Во-первых, это информация, относимая к государственной тайне, а также принципы и критерии, в соответствии с которыми сведения классифицируются как государственная тайна. Во-вторых, правовой механизм ограничения доступа к государственной тайне. В-третьих, санкции за неправомерное получение, распространение этих сведений.

Объектом правоотношений выступает право на государственную тайну. Правовая охрана прав на государственную тайну наступает с момента отнесения конкретных сведений к государственной тайне и действует в течение всего периода их засекречивания.

Уголовно-правовая защита информации, составляющей государственную тайну, согласно нормам УК РФ, осуществляется с помощью введения уголовно-правового запрета на совершение ряда деяний (действий, бездействия), предметом посягательства которых выступает государственная тайна.

Уголовным кодексом Российской Федерации[1] предусмотрено несколько составов преступлений, объектом которых являются правоотношения, связанные с государственной тайной: выдача государственной тайны, квалифицируемая как государственная измена (ст. 275); шпионаж (ст. 276).

Объективной стороной данного состава являются собирание, хранение, похищение информации, содержащей государственную тайну, в целях выдачи иностранному государству, международной либо иностранной организации или их представителям сведений, составляющих государственную тайну. Оба преступления являются умышленными.

[1] Уголовный кодекс Российской Федерации: Федеральный закон Российской Федерации от 13.06.1996 № 63-ФЗ (в действ. ред.) // Собрание законодательства Российской Федерации. 1996. № 52. Ст. 2954.

Уголовная ответственность предусматривается также за разглашение государственной тайны (при отсутствии признаков государственной измены) (ст. 283), незаконное получение сведений, составляющих государственную тайну (ст. 283.1), и за утрату документов, содержащих государственную тайну (ст. 284). В отличие от первых двух составов эти преступления могут быть с субъективной стороны и неосторожными, а их субъектами — лица, имеющие допуск к государственной тайне.

Институт коммерческой тайны, безусловно являясь одним из важных компонентов системы обеспечения устойчивости рынка, оказывает в определенной степени влияние на социальные отношения в целом.

Представляя собой форму обеспечения безопасности наиболее важной коммерческой информации, коммерческая тайна предполагает ограничение ее распространения. С правовой точки зрения это средство защиты от недобросовестной конкуренции.

Уголовный кодекс Российской Федерации закрепляет ряд положений, устанавливающих защиту прав обладателей сведений, составляющих коммерческую тайну, выделяя несколько составов преступлений, предусматривающих различные наказания в зависимости от тяжести совершенного деяния (ст. 183 УК РФ).

Во-первых, уголовным преступлением признаются действия по собиранию сведений, составляющих коммерческую, налоговую или банковскую тайну, в случае если доказано, что эти сведения собирались путем похищения документов, подкупа или угроз, а равно иным незаконным способом.

Во-вторых, предусмотрено наказание за уголовное преступление, заключающееся в незаконном разглашении или использовании сведений, составляющих коммерческую, налоговую или банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе.

Использование сведений в корыстных целях, а равно причинение крупного ущерба являются квалифицирующими признаками еще одного состава уголовного преступления, предусмотренного ст. 183 УК РФ.

И наконец, в случае наступления более тяжких последствий для виновных в совершении уголовного преступления предусматривается самое серьезное наказание.

Как показала практика, существовавшие минимальные наказания в виде штрафов оказались несущественными и не обладали должной эффективностью для защиты прав и законных интересов обладателей информации, отнесенной к коммерческой, банковской и налоговой тайне.

Так, по информации, представленной Судебным департаментом при Верховном Суде Российской Федерации[1], в 2013 г. было зарегистрировано 317 преступлений, квалифицированных по ст. 183 УК РФ. К различным мерам наказания было привлечено 13 лиц, двое из которых осуждены к лишению свободы, на пять лиц наложен штраф. При этом трем лицам был назначен штраф от 25 до 50 тыс. руб., одному — от 5 до 25 тыс. руб. и одному — до 5 тыс. руб.

В связи с этим заинтересованными федеральными органами исполнительной власти было предложено увеличить предельные размеры штрафов, предусмотренные ст. 183 УК РФ, установив их на уровне, аналогичном уровню, установленному ст. 159.4 УК РФ («Мошенничество в сфере предпринимательской деятельности»).

Государственной Думой 10 июня 2015 г. были приняты поправки в ст. 183 Уголовного кодекса Российской Федерации[2], предусматривающие значительное уве-

---

[1] Паспорт проекта Федерального закона № 653786-6 «О внесении изменений в статью 183 Уголовного кодекса Российской Федерации» [Электронный ресурс] // СПС «КонсультантПлюс». URL: http://http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=PRJ;n=124927;div=LAW;mb=LAW;opt=1;ts=ECC0F2C0262D00773FB0AEC3DE24BD26;rnd=0.9350344331469387 (дата обращения: 01.08.2015).

[2] О внесении изменений в статью 183 Уголовного кодекса Российской Федерации: Федеральный закон Российской Федерации от 29.06.2015 № 193-ФЗ // Российская газета. 2015. № 145.

личение минимального наказания по указанной статье, установленного в виде штрафа в размере до 500 тысяч рублей (с 80 тысяч рублей) в части первой; до 1 миллиона рублей (со 120 тысяч рублей) в части второй и до 1,5 миллиона рублей (с 200 тысяч рублей) в части третьей.

В Кодексе Российской Федерации об административных правонарушениях (далее — КоАП РФ)[1] составы правонарушений, касающиеся информации, так же как и в Уголовном кодексе Российской Федерации, рассредоточены по разным разделам. Действующий КоАП РФ включает информационные правонарушения в разные главы (например, гл. 5–8, 13–17, 19).

Наибольшее число составов в области информации и средств связи сосредоточено в гл. 13 «Административные правонарушения в области связи и информации» (ст. 13.1–13.26).

Среди административных правонарушений в информационной сфере отдельно следует выделить такие, как использование несертифицированных средств связи либо предоставление несертифицированных услуг связи (ст. 13.6); нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) (ст. 13.11); разглашение информации с ограниченным доступом (ст. 13.14).

Статья 19.7 КоАП РФ предусматривает ответственность за непредставление или несвоевременное представление уведомления об обработке персональных данных или иной информации по запросу уполномоченного органа.

Важным условием в регулировании отношений в области обеспечения информационной безопасности, явившимся по существу реализацией положений Доктрины информационной безопасности Российской Федерации[2], несомненно, является включение в КоАП РФ норм, предусматривающих административную ответственность за деятельность в сфере защиты информации, отнесенной к государственной тайне.

В настоящее время административно-правовая ответственность за посягательства на режим сохранения государственной тайны прямо предусматривается ст. 13.12, 13.13 упомянутого Кодекса.

Это может быть нарушение условий, предусмотренных лицензией на проведение работ, связанных с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну (п. 3, ст. 13.12), либо использование несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну (п. 4, ст. 13.12). Административная ответственность также предусмотрена за занятие видами деятельности, связанными с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну, без лицензии (п. 2, ст. 13.13). Субъектами административной ответственности могут быть как физические (должностные), так и юридические лица.

Несомненно, отдельно следует остановиться на нормах, регулирующих отношения, связанные с обработкой персональных данных всеми субъектами правоотношений, как с использованием средств автоматизации, так и без использования таковых.

---

[1] Кодекс Российской Федерации об административных правонарушениях: Закон Российской Федерации от 30.12.2001 № 195-ФЗ (в действ. ред.) // Российская газета. 2001. № 256.

[2] Доктрина информационной безопасности Российской Федерации. Утверждена Президентом Российской Федерации 09.09.2000 № Пр-1895 (в действ. ред.) // Российская газета. 2000. № 187.

Целью правового регулирования является обеспечение защиты прав и законных интересов лиц при обработке персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайны. Основная угроза безопасности этих прав и свобод, как правило, исходит от неправомерного использования собираемых персональных данных государственными органами, органами местного самоуправления, юридическими и физическими лицами.

Принятый в 2006 г. Федеральный закон «О персональных данных»[1] устанавливает общие принципы и условия обработки персональных данных, права субъекта персональных данных, обязанности оператора при сборе персональных данных, а также порядок осуществления контроля и надзора за обработкой персональных данных.

Административная ответственность за совершение правонарушения в области персональных данных предусмотрена ст. 13.11 «Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)» КоАП РФ.

В соответствии с указанной статьей максимальный размер штрафа за нарушение требований законодательства Российской Федерации о персональных данных для юридических лиц составляет 10 тысяч рублей.

Государственной Думой 19 января 2015 г. был рассмотрен законопроект[2], предусматривающий внесение существенных изменений в ст. 13.11 КоАП РФ.

Предлагаемые проектом изменения и дополнения данной статьи обусловлены, прежде всего, низкой эффективностью ее действия в сфере защиты прав и интересов субъектов персональных данных, соблюдения принципа неотвратимости наказания за совершенное правонарушение в области персональных данных, а также интенсивным развитием информационно-телекоммуникационных технологий. Немаловажное значение имеет и принятый курс на сближение правового регулирования в сфере защиты персональных данных с международными стандартами.

К примеру, законодательство Италии предусматривает ответственность за нарушение норм в области персональных данных в виде административного штрафа до 1,5 миллиона евро; Великобритании — до 500 тысяч фунтов. В Германии за нарушение законодательства в области персональных данных устанавливается наказание в виде административного штрафа в размере до 300 тысяч евро и конфискации незаконно полученной прибыли. Также предусматриваются административные санкции за несвоевременное устранение и повторное нарушение, а в ряде случаев — уголовная ответственность за соответствующие правонарушения[3].

Показательно, что, несмотря даже на значительно более высокий уровень жизни в европейских странах, санкции, предусмотренные за нарушение законодательства в области персональных данных, в сравнении с нормами, предусмотренными российским законодательством, впечатляют.

Кроме того, совершенно очевидно, что состав действующей ст. 13.11 КоАП РФ уже не в полной мере учитывает тяжесть негативных последствий совершенных

---

[1] О персональных данных: Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ (в действ. ред.) // Российская газета. 2006. № 165.

[2] О внесении изменений в Кодекс Российской Федерации об административных правонарушениях (в части уточнения положений, устанавливающих ответственность за нарушение законодательства о персональных данных): проект Федерального закона № 683952-6 [Электронный ресурс] // СПС «КонсультантПлюс». URL: http://www. consultant.ru/law/review/lawmaking/program_spring/ (дата обращения: 05.08.2015).

[3] Паспорт проекта Федерального закона № 683952-6 «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» [Электронный ресурс] // СПС «КонсультантПлюс». URL:http://http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=PRJ;n=129000 (дата обращения: 05.08.2015).

правонарушений. Как следствие — значительное увеличение роста количества жалоб и обращений граждан на незаконные действия операторов, осуществляющих обработку персональных данных с нарушением законодательства Российской Федерации в области персональных данных и, соответственно, количества выявленных нарушений.

Так, по информации, представленной Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее — Роскомнадзор)[1], являющейся уполномоченным органом по защите прав субъектов персональных данных, в 2010 г. по сравнению с 2009 г., то есть всего за один год, количество выявленных административных правонарушений в области персональных данных выросло — внимание!!! — в 55 раз, в 2011 г., что тоже впечатляет, в 2 раза в сравнении с показателями 2010 г.

Обращает на себя внимание и динамика роста числа обращений со стороны заинтересованных лиц по поводу нарушений прав в области хранения, обработки и защиты персональных данных. Так, в 2012 г. в адрес Роскомнадзора, а также его территориальных органов поступило 5677 обращений, что на 31% выше показателей 2011 г., в 2013 г. поступило 10 016 обращений граждан и юридических лиц, что по сравнению с 2012 г. составляет рост уже на 43%. Более того, по результатам рассмотрения обращений граждан в деятельности операторов выявлены систематические нарушения, носящие повторяющийся характер.

Законопроектом предусматривается дополнение ст. 13.11 КоАП новыми составами административных правонарушений, установив при этом четкую дифференциацию составов правонарушений в области персональных данных с учетом ущерба, причиненного нарушением, а также существенно увеличивая размеры административных штрафов. При этом диапазон административного штрафа, наложенного на граждан, будет варьироваться в зависимости от состава правонарушения от 700 рублей до 5 тысяч рублей, на должностных лиц — от 3 тысяч рублей до 25 тысяч рублей, на индивидуальных предпринимателей — от 5 тысяч рублей до 100 тысяч рублей и на юридических лиц — от 15 тысяч рублей до 300 тысяч рублей.

Максимальное наказание предусматривается за обработку специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, а также персональных данных о судимости.

Не менее важными являются изменения и дополнения в КоАП РФ, связанные с решением вопросов, касающихся определения органов государственной власти, наделенных полномочиями в области административного производства в рамках осуществления государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных.

В настоящее время в соответствии с подведомственностью собранные материалы направляются в органы прокуратуры для принятия соответствующих мер прокурорского реагирования. Однако длительная во временном аспекте установленная процедура собирания материалов, направления их в органы прокуратуры, рассмотрения органами прокуратуры представленных материалов, а также неделящийся характер правонарушений по ст. 13.11 КоАП РФ, для которых к тому же установлен 3-месячный срок давности, делают затруднительным привлечение операторов к установленной законом административной ответственности.

---

[1] Паспорт проекта Федерального закона № 683952-6 «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» [Электронный ресурс] // СПС «КонсультантПлюс». URL:http://http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=PRJ;n=129000 (дата обращения: 05.08.2015).

Законопроектом предполагается, что достаточно эффективной мерой, направленной на решение проблем в сложившейся ситуации и позволяющей в полной мере обеспечить соблюдение принципа неотвратимости наказания за совершенное правонарушение, будет наделение Роскомнадзора полномочиями по возбуждению дел об административных правонарушениях по ст. 13.11 КоАП РФ.

Таким образом, для адекватного и достаточно эффективного реагирования на существующие проблемы, находящиеся в плоскости правового регулирования информационных отношений, можно выделить несколько способов, заключающихся в повышении эффективности действующих норм права путем дифференцирования составов правонарушений с учетом ущерба, причиненного нарушителем; существенного увеличения размеров штрафных санкций, как в плоскости административной ответственности, так и в качестве уголовного наказания; а также с наделением органов государственной власти дополнительными полномочиями в области административного производства.

Литература

1. *Бахрах Д. Н.* Административное право: учебник для вузов. М.: Эксмо, 2010. 608 с.
2. *Бачило И. Л.* Информационное право: учебник для магистров. М.: Юрайт, 2013. 564 с.
3. *Клименко С. Н.* Правовые основы информационной безопасности в таможенных органах Российской Федерации: монография. СПб.: РИО СПб филиала РТА, 2013. 122 с.
4. *Кухаренко Т. А.* Персональные данные. Кто, что и зачем должен о нас знать. М.: Эксмо, 2010. 224 с.
5. *Ожегов С. И., Шведова Н. Ю.* Толковый словарь русского языка. М.: АЗЪ, 1993. 928 с.
6. *Стрельцов А. А.* Теоретические и методологические основы правового обеспечения информационной безопасности России: дисс. ... д-ра юр. наук. М., 2004. 371 с.

References

1. Bakhrakh D. N. *Administrative law* [Administrativnoe pravo]: textbook for higher education institutions. M.: Eksmo, 2010. 608 p. (rus)
2. Bachilo I. L. *Information law* [Informatsionnoe pravo]: textbook for masters. M.: Urait, 2013. 564 p. (rus)
3. Klimenko S. N. *Legal bases of information security in customs authorities of the Russian Federation* [Pravovye osnovy informatsionnoi bezopasnosti v tamozhennykh organakh Rossiiskoi Federatsii]: monograph. SPb.: Publishing Department of the SPb branch of Russian Customs Academy [RIO SPb filiala RTA], 2013. 122 p. (rus)
4. Kukharenko T. A. *Personal information. Who, as why has to know about us* [Personal'nye dannye. Kto, chto i zachem dolzhen o nas znat']. M.:Ecsmo, 2010. 224 p. (rus)
5. Ozhegov S. I., Shvedova N. Yu. *Explanatory dictionary of Russian* [Tolkovyi slovar' russkogo yazyka]. M.: AZ, 1993. 928 p. (rus)
6. Streltsov A. A. *Theoretical and methodological bases of legal support of information security of Russia: doctoral dissertation* [Teoreticheskie i metodologicheskie osnovy pravovogo obespecheniya informatsionnoi bezopasnosti Rossii]. M, 2004. 371 p. (rus)