

ПРОБЛЕМЫ ТЕХНИКИ НАЛОГОВОГО СТИМУЛИРОВАНИЯ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ ДЛЯ МАЛОГО И СРЕДНЕГО БИЗНЕСА**Екатерина Валерьевна КУДРЯШОВА**

кандидат юридических наук, доцент, старший научный сотрудник Института законодательства и сравнительного правоведения при Правительстве РФ, Москва, Российская Федерация

ev_kudryashova@inbox.ru

<https://orcid.org/0000-0002-7029-5794>

SPIN-код: 7017-2770

История статьи:

Получена 25.12.2018

Получена в доработанном виде 28.01.2019

Одобрена 11.02.2019

Доступна онлайн 29.03.2019

УДК 336.2

JEL: H21, H25, M48

Аннотация**Предмет.** Современные научные и практические подходы к экономическому содержанию и стимулированию кибербезопасности для малого и среднего бизнеса. Разные подходы, понятия и терминология в сфере обеспечения кибербезопасности, а также их соотношение с экономикой организации. Научные исследования в области экономической оценки кибербезопасности. Выдвинутые на сегодня предложения о технике стимулирования обеспечения кибербезопасности.**Цели.** Выявить проблемы, препятствующие внедрению экономических и прежде всего налоговых мер стимулирования обеспечения кибербезопасности, как в России, так и в других государствах. Продемонстрировать варианты техник налогового стимулирования обеспечения кибербезопасности для малого и среднего бизнеса.**Методология.** Использован междисциплинарный подход, сравнительный метод, а также системный подход.**Результаты.** Выявлено, что развитие мер налогового стимулирования обеспечения кибербезопасности серьезно тормозится отсутствием единого подхода к экономическому содержанию кибербезопасности. Указано на возможность дифференцированного подхода к крупным организациям и к организациям малого и среднего бизнеса. Описаны примеры конкретных подходов к налоговой технике стимулирования кибербезопасности для малого и среднего бизнеса.**Выводы.** Стимулирование обеспечения кибербезопасности налоговыми и другими экономическими способами признано необходимым не только в России, но и во многих других развитых государствах. Объективно требуется дифференциация в подходах к крупным организациям и к предприятиям малого и среднего бизнеса. Внедрение и реализация уже предложенных техник налогового стимулирования тормозится за счет отсутствия определенного подхода к экономическому содержанию кибербезопасности. Тормозящим фактором также является несогласованность в выборе понятий информационная безопасность, кибербезопасность, цифровая безопасность, что в итоге влияет на экономические подходы.**Ключевые слова:**

кибербезопасность, информационная безопасность, налог, экономическое стимулирование, цифровая экономика

© Издательский дом ФИНАНСЫ и КРЕДИТ, 2018

Для цитирования: Кудряшова Е.В. Проблемы техники налогового стимулирования обеспечения кибербезопасности для малого и среднего бизнеса // *Финансы и кредит*. — 2019. — Т. 25, № 3. — С. 609 — 617. <https://doi.org/10.24891/fc.25.3.609>**Введение**

Одна из проблем современной цифровой эпохи, которая уже констатирована, но далека от решения — проблема кибербезопасности¹. По данным Института системного анализа

РАН РФ, затраты на обеспечение режима информационной безопасности составляют до 30% всех затрат на информационную систему, и владельцы информационных ресурсов серьезно рассматривают экономические аспекты обеспечения информационной безопасности [1]. Значение кибербезопасности часто определяют еще методом «от

¹ Для целей настоящей статьи остановимся на термине «кибербезопасность», хотя как будет понятно из дальнейшего изложения это не единственно возможный вариант.

противного» — с помощью перечисления количества и качества угроз, с которыми приходится сталкиваться организациям разных секторов экономики [2] и, соответственно, через ущерб от нарушения состояния кибербезопасности, а также затраты на ее восстановление. Лабораторией Касперского была предпринята попытка оценить последствия нарушения кибербезопасности, в результате которого была продемонстрирована значительная разница между угрозами и последствиями кибератак для разных видов бизнеса. Однако был сделан общий вывод о том, что обеспечение кибербезопасности всегда дешевле, чем ликвидация последствий ее нарушения².

Проблема кибербезопасности имеет много аспектов и один из них: следует ли и как следует экономически стимулировать обеспечение кибербезопасности, в частности, с помощью налоговых стимулов.

Ранее в публикациях мы уже привлекали внимание к такому понятию в налоговом праве, как техника налогообложения [3]. В самом общем виде техника налогообложения обеспечивает учет объекта обложения и призвана предотвратить уклонение от налогов [4] и обеспечить реализацию избранной модели налогообложения [5]. Техника налогового стимулирования является частным случаем техники налогообложения. С научной точки зрения техника налогообложения остается широчайшим полем для исследований и имеет наибольшее прикладное значение, поэтому в этой статье избран именно этот аспект.

Мы разберем некоторые варианты предложенных в разных странах налоговых техник, стимулирующих обеспечение кибербезопасности для малого и среднего бизнеса.

Применяя междисциплинарный подход, позволяющий объединить право и экономику, мы выявим факторы, тормозящие реализацию

мер налогового стимулирования обеспечения кибербезопасности. Для исследования нам потребуется переход от общего к частному и восхождение от частного к общему, а также мы прибегнем к системному подходу в следующей оригинальной интерпретации: «В экономической и финансовой науке системный подход применяется двояко: во-первых, посредством исследования экономической и финансовой систем, а также их сфер и звеньев с применением аппарата системного подхода, во-вторых, путем соотнесения экономической и финансовой систем с другими системами — биологическими, техническими, физическими и т.д. И если первый подход более традиционен и исчерпаем, то исследования в рамках второго подхода поражают своим разнообразием и новизной» [6]

Соотношение понятия «кибербезопасность» со смежными понятиями в российской и зарубежной традициях и проблема их экономического содержания

На сегодняшний день понятие «кибербезопасность» применяется чаще других, но оно не окончательно устоялось в международной практике.

В российском контексте большое значение имеет соотношение между понятиями «кибербезопасность» и «информационная безопасность» [7]. Согласно доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 05.12.2016 № 646 информационная безопасность — это состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

В российских публикациях обосновывается, что понятие «кибербезопасность» является по определению более узким, чем понятие

² Damage Control: The Cost of Security Breaches. IT Security Risks Special Report Series. Kaspersky Lab. 2016.
URL: <https://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf>

«информационная безопасность» [8]. Кибербезопасность — это прежде всего защита коммуникационных каналов (в частности Интернета) и аппаратуры. Информационная безопасность распространяется и на контент. Термин «кибербезопасность» используется в западных странах. Россия же активно продвигает понятие «информационная безопасность». Так, внесенная Россией на рассмотрение ООН концепция Конвенции международной информационной безопасности к угрозам относит действия, совершаемые «с целью подрыва политической, экономической и социальной систем другого государства, психологическую обработку населения»³.

Нам представляется, что для целей экономической оценки и последующей реализации в финансовом законодательстве понятие кибербезопасность, исключая контент, более конкретно и более точно очерчивает круг заинтересованных субъектов [9, 10]. Хотя значение кибербезопасности для экономики организации пока также неоднозначно.

В поисках в документах понятия с признанным экономическим содержанием мы должны извлечь из хитросплетений понятий и терминов в этой области еще одно — «цифровая» безопасность. ОЭСР сопоставляет кибербезопасность и цифровую безопасность как целое и часть: цифровая безопасность входит в понятие кибербезопасность. Кибербезопасность включает в себя все аспекты цифровой безопасности из технологической сферы, а также экономические, социальные, правовые, правоприменительные, вопросы прав человека, национальной безопасности, благосостояния, международной стабильности и т.д.⁴. В документах ОЭСР именно цифровая безопасность наиболее четко связывается с экономикой организации. В обновленных

документах окончательно утвердилось мнение, что «цифровой» риск не рассматривается более как некий «электронный риск» и должен рассматриваться как экономический риск и, соответственно, входить в сферу общего управления рисками и составлять часть процесса принятия решений, то есть находиться в орбите экономики предприятия. Мы не можем привести аналогичного прямолинейного заявления относительно кибербезопасности или информационной безопасности из международных или российских документов.

Представляется, что только технологический подход не позволяет оценить значение состояния защищенности — безопасности и последствий его нарушения, которые лежат в экономической, социальной, правовой и иных сферах [11–13]. Несмотря на то что кибербезопасность в основном связывается с техникой и технологией, согласно современным исследованиям гораздо большее значение следует придавать человеческому фактору. Люди, намеренно или по халатности, из-за отсутствия необходимых знаний, несут даже большую угрозу безопасности, чем техника. Ресурс снижения стоимости обеспечения кибербезопасности современные исследователи видят именно в социальных факторах [14, 15].

Очевидно, что отсутствие четкой позиции об экономическом содержании кибербезопасности или, как настаивает Россия — информационной безопасности, а может быть, наиболее ограниченной «цифровой безопасности», предложенной ОЭСР, серьезно тормозит развитие налогового стимулирования в этой области. И в российской доктрине информационной безопасности, и в зарубежных документах о кибербезопасности сказано о мерах государственной поддержки, экономических и, в частности, налоговых стимулах в отношении обеспечения этого вида безопасности, но практически все они остаются не реализованными.

Только в 2015 г. наконец на уровне ОЭСР отказались от надуманного понятия

³ Черненко Е., Иванов М. Концепция кибербезопасности разошлась с государственной стратегией // *Коммерсантъ*. № 220 от 29.11.2013. С. 2.

⁴ Digital Security Risk Management for Economic and Social Prosperity OECD Recommendations and Companion Document. OECD. 2015. P.4. URL: <http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf>

«электронный риск», но значительного продвижения к установлению экономического содержания кибербезопасности пока не отметились.

В научной литературе вносятся предложения о методах оценки кибербезопасности. Ученые, занимающиеся стратегическими исследованиями, задаются вопросом: как определить экономически оправданные затраты на защиту информации? Предлагаются следующие критерии выбора методов оценки: во-первых, метод должен обеспечивать количественную оценку затрат на безопасность, используя качественные показатели оценки вероятностей событий и их последствий. Во-вторых, метод должен быть прозрачен с точки зрения пользователя и давать возможность вводить собственные эмпирические данные. В-третьих, метод должен быть универсален, то есть одинаково применим к оценке затрат на приобретение аппаратных средств, специализированного и универсального программного обеспечения, затрат на услуги, затрат на перемещение персонала и обучение конечных пользователей и т.д. В-четвертых, выбранный метод должен позволять моделировать ситуацию, при которой существует несколько контрмер, направленных на предотвращение определенной угрозы, в разной степени влияющих на сокращение вероятности происшествия [1]. Исходя из этих критериев называют следующие приемлемые методы: прикладной информационный анализ; потребительский индекс; добавленная экономическая стоимость; исходная экономическая стоимость; управление портфелем активов; оценка действительных возможностей; метод жизненного цикла искусственных систем; система сбалансированных показателей; совокупная стоимость владения; функционально-стоимостной анализ [1]. Позиции о том, какой из методов является наилучшим, пока нет и, возможно, такой метод не может быть единым, как будет ясно из дальнейшего изложения.

Еще одна проблема, примыкающая к проблемам экономического содержания кибербезопасности, и которая не решена до

настоящего времени — это проблема разграничения необходимых инвестиций в кибербезопасность и всех прочих [16]. Она также является очень важной для целей налогового стимулирования обеспечения кибербезопасности, поскольку логично предоставлять налоговые льготы и стимулы для оправданных вложений.

Техники налогового стимулирования обеспечения кибербезопасности для малого и среднего бизнеса

Экономическое и в том числе налоговое стимулирование обеспечения кибербезопасности не может быть единым для всех и это обусловлено объективными факторами. Субъекты, вовлеченные и заинтересованные в кибербезопасности крайне неоднородны, интересы их как ни странно зачастую противоречат друг другу и технические аспекты их деятельности отличаются: невозможно говорить о едином подходе к кибербезопасности, так называемой серебряной пуле, для каждой из отраслей. Если функционирование некоторой части отраслей, к примеру финансовой сферы или органов госуправления, основано на классических информационных системах, основной целью которых является управление информацией, то другие — энергетика, транспорт, добыча природных ресурсов и т.д. — работают на основе специализированных промышленных систем, созданных для управления технологическим процессом. В подавляющем большинстве случаев инциденты, которые могут произойти на подобных промышленных объектах, потенциально могут привести к гораздо худшим последствиям, чем потеря информации или денег: к угрозе жизни людей, загрязнению окружающей среды и прочим действительно опасным результатам [17].

В то же время налоговое стимулирование обеспечения кибербезопасности с акцентом на определенную отрасль, нам представляется не совсем логичным. Более того, как раз задачей полноценного обеспечения кибербезопасности является вовлечение возможно большего числа участников из разных отраслей экономики в ее обеспечение.

Скорее различия могут проводиться в зависимости от размеров и значимости организации. Особое внимание уделяется субъектам малого и среднего бизнеса, для которых инвестиции в кибербезопасность весьма обременительны. Есть налоговые техники, стимулирующие крупные компании, но именно для малого и среднего бизнеса меры налогового стимулирования обеспечения кибербезопасности наиболее необходимы.

Традиционной мерой стимулирования обеспечения кибербезопасности субъектами малого и среднего бизнеса являются налоговые каникулы — установление определенного периода времени, когда налоги с дохода (прибыли) уплачиваются по пониженной ставке или вовсе не уплачиваются. Такая льгота реализуется путем объявления добровольной сертификации на предмет обеспечения кибербезопасности и в случае прохождения этой сертификации субъекту малого и среднего бизнеса предоставляются налоговые каникулы. Налоговые каникулы могут также предоставляться в случае безаварийной работы в течение определенного периода времени без введения добровольной сертификации — менее формальный подход, но сложнее реализуется.

Нетрадиционный вариант налоговой техники стимулирования обеспечения кибербезопасности был предложен в Великобритании. В ходе дебатов в Великобритании по поводу налоговых стимулов обеспечения кибербезопасности рассматривался вариант применения специальных купонов (voucher) по аналогии с применявшимися в этом государстве ранее «купонами роста»⁵ — купоны роста выдавались организациям без включения их номинальной стоимости в налогооблагаемую прибыль для последующего погашения в счет услуг по содействию бизнесу (техническое сопровождение, прохождение сертификации и пр.).

Стимулирующие купоны могли бы выдаваться для сертификации базового уровня кибербезопасности (Cyber Essentials Certification) в целях преодоления финансовых

затруднений малого и среднего бизнеса в обеспечении кибербезопасности, но они не должны были покрывать все расходы. Ограниченное число купонов предполагалось выдавать в пределах одного года для их погашения в счет оплаты расходов на обеспечение кибербезопасности. Более важный ожидаемый эффект от купонов — это популяризация процедуры сертификации в сфере кибербезопасности с целью заинтересовать малый и средний бизнес в ее проведении. В Великобритании этот вариант не был реализован, в том числе потому, что не смогли сделать убедительный расчет эффективности таких купонов, что, очевидно, связано с проблемой экономического содержания самой кибербезопасности.

Заключение

Стимулирование обеспечения кибербезопасности налоговыми и другими экономическими способами признано необходимым не только в России, но и во многих других развитых государствах. Практически во всех документах, концепциях, стратегиях и доктринах в разных странах есть упоминание о мерах государственной поддержки обеспечения кибербезопасности. Однако, нам представляется, что внедрение и реализация налогового или любого другого экономического стимулирования сталкивается с тормозящими факторами, ключевым из которых является отсутствие определенного экономического содержания кибербезопасности. Возможно, здесь следует искать дифференцированные подходы, исходя из характеристик организаций.

Отчасти такой дифференцированный подход уже наметился в различии вариантов налогового стимулирования для крупных компаний и для организаций малого и среднего бизнеса, в последнем случае выполняется также задача вовлечения возможно большего круга лиц в обеспечение кибербезопасности.

Варианты налоговых техник стимулирования малого и среднего бизнеса уже предложены, но их реализация тормозится как в России, так и в других государствах. В данном случае мы наблюдаем опережающее развитие конкретной техники налогового стимулирования по отношению к решению ключевых экономических проблем.

⁵ Cyber Security Regulation and Incentives Review, December 2016. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/579442/Cyber_Security_Regulation_and_Incentives_Review.pdf

Список литературы

1. Петренко С.А. Оценка затрат на кибербезопасность // Труды Института системного анализа Российской Академии наук. 2006. Т. 27. С. 234—265.
URL: <http://www.isa.ru/proceedings/images/documents/2006-27/234-265.pdf>
2. Rittinghouse J.W., Hancock W.M. Cybersecurity Operations Handbook. Elsevier Digital Press, 2003, 1287 p.
3. Кудряшова Е.В. Соотношение понятий «способ взимания налога» и «техника обложения» на примере косвенных налогов // Налоги-журнал. 2006. № 2. С. 7—14.
URL: <https://wiselawyer.ru/poleznoe/18069-sootnoshenie-ponyatij-sposob-vzimanija-naloga-tekhnika-oblozheniya>
4. Кучеров И.И. Объект налога как правовое основание налогообложения // Финансовое право. 2009. № 1. С. 6—12. URL: <https://www.lawmix.ru/bux/35803>
5. Шашкова А.В. Переход от доиндустриального к индустриальному обществу: смена модели налоговой политики // Финансовое право. 2017. № 5 С. 39—42.
URL: <http://отрасли-права.рф/article/25449>
6. Кузнецов Н.Г., Кочмола К.В., Евлахова Ю.С., Кошель Н.В. Финансовая термодинамика: новые подходы в исследовании мировой финансовой системы // Финансовые исследования. 2010. № 3. С. 3—9. URL: <https://cyberleninka.ru/article/n/finansovaya-termodinamika-novye-podhody-v-issledovani-mirovoy-finansovoy-sistemy>
7. Ефремов А.А. Формирование концепции информационного суверенитета государства // Право. Журнал Высшей школы экономики. 2017. № 1. С. 201—215.
URL: <https://cyberleninka.ru/article/n/formirovanie-kontseptsii-informatsionnogo-suvereniteta-gosudarstva>
8. Цирлов В.Л. Правовые основы кибербезопасности Российской Федерации // Правовая информатика. 2014. № 3. С. 54—56. URL: <https://cyberleninka.ru/article/n/pravovye-osnovy-kiberbezopasnosti-rossiyskoy-federatsii>
9. Shashkova A.V. Russian Specifics of Combating Corruption. *Kutafin University Law Review*, 2015, vol. 2, no. 1, pp. 51—68. URL: http://archive.kulawr.ru/articles/article_101513.html
10. Shashkova A.V. Pro et Contra Criminalization of Corporate Liability in the Russian Federation. *Kutafin University Law Review*, 2017, vol. 4, no. 2, pp. 544—554.
URL: http://archive.kulawr.ru/netcat_files/521/703/2.2017_KULawR__Anna_V._Shashkova__544_554.pdf
11. Ашмарина Е.М., Кудряшова Е.В., Терехова Е.В. и др. Финансово-правовые аспекты и финансовая политика инновационного развития современной российской экономики. Коллективная монография. М.: Элит, 2011.
12. Поветкина Н.А., Леднева Ю.В. «Финтех» и «регтех»: границы правового регулирования // Право. Журнал Высшей школы экономики. 2018. № 2. С. 46—67.
URL: <https://law-journal.hse.ru/data/2018/08/01/1152219816/%D0%BF%D0%BE%D0%B2%D0%B5%D1%82%D0%BA%D0%B8%D0%BD%D0%B0.pdf>
13. Кучеров И.И., Поветкина Н.А., Акопян О.А. Риски финансовой безопасности: правовой формат: монография. М.: ИЗИСП, Норма, 2018. 304 с.

14. Govender S.G., Loock M., Kritzing E. Enhancing Information Security Culture to Reduce Information Security Cost: A Proposed Framework. In: *Cyberspace Safety and Security. 10th International Symposium, CSS 2018, Amalfi, Italy, October 29–31, 2018, Proceedings*. Springer Nature Switzerland AG, 2018, pp. 281–290. URL: <https://doi.org/10.1007/978-3-030-01689-0>
15. Добробаба М.Б. Служебно-деликтные правоотношения: монография. М.: Юрлитинформ, 2013. 296 с.
16. Петренко С.А. Обоснование инвестиций в кибербезопасность // Труды Института системного анализа Российской Академии наук. 2006. Т. 27. С. 266—276. URL: <http://www.isa.ru/proceedings/images/documents/2006-27/266-276.pdf>
17. Войтов М. Критическая инфраструктура в контексте безопасности // Индекс безопасности. 2016. Т. 22. № 1. С. 137—142.

Информация о конфликте интересов

Я, автор данной статьи, со всей ответственностью заявляю о частичном и полном отсутствии фактического или потенциального конфликта интересов с какой бы то ни было третьей стороной, который может возникнуть вследствие публикации данной статьи. Настоящее заявление относится к проведению научной работы, сбору и обработке данных, написанию и подготовке статьи, принятию решения о публикации рукописи.

**CHALLENGES OF TAX INCENTIVES FOR CYBERSECURITY
IN SMALL AND MEDIUM-SIZED BUSINESSES****Ekaterina V. KUDRYASHOVA**Institute of Legislation and Comparative Law under Government of Russian Federation, Moscow, Russian Federation
ev_kudryashova@inbox.ru
<https://orcid.org/0000-0002-7029-5794>**Article history:**Received 25 December 2018
Received in revised form
28 January 2019
Accepted 11 February 2019
Available online
29 March 2019**JEL classification:** H21,
H25, M48**Keywords:** cybersecurity,
tax incentives, economic
incentives, digital economy**Abstract****Subject** The article deals with modern scientific and practical approaches to the economic substance and tax incentives for cybersecurity in small and medium-sized businesses.**Objectives** The purpose is to unveil problems preventing the implementation of economic and tax incentives to ensure cybersecurity, both in Russia and in other countries, and to demonstrate possible tax incentive schemes for SMEs.**Methods** The study draws on the interdisciplinary approach, the comparative method, and the systems approach.**Results** I show that the development of tax incentives to ensure cybersecurity seriously suffers from the lack of an integrated approach to the economic substance of cybersecurity. It is possible to apply a differentiated approach to large organizations and to small and medium-sized businesses. The paper gives examples of specific approaches to the technology of tax incentives for cybersecurity in SMEs.**Conclusions** Encouraging the cybersecurity through tax and other economic measures is crucial in many developed countries. There is a need to differentiate approaches to large businesses and SMEs. Implementation of proposed tax incentive techniques is impeded by the lack of specific approach to the economic substance of cybersecurity. The inhibiting factor is also the inconsistency in the choice of concepts of information security, cybersecurity, digital security, which eventually affects economic approaches.

© Publishing house FINANCE and CREDIT, 2018

Please cite this article as: Kudryashova E.V. Challenges of Tax Incentives for Cybersecurity in Small and Medium-Sized Businesses. *Finance and Credit*, 2019, vol. 25, iss. 3, pp. 609–617.
<https://doi.org/10.24891/fc.25.3.609>**References**

1. Petrenko S.A. [Cybersecurity cost estimation]. *Trudy Instituta sistemnogo analiza Rossiiskoi Akademii nauk = Proceedings of the Institute for Systems Analysis of the Russian Academy of Sciences*, 2006, vol. 27, pp. 234–265.
URL: <http://www.isa.ru/proceedings/images/documents/2006-27/234-265.pdf> (In Russ.)
2. Rittinghouse J.W., Hancock W.M. *Cybersecurity Operations Handbook*. Elsevier Digital Press, 2003, 1287 p.
3. Kudryashova E.V. [Interrelation of concepts of the method of tax collection and taxation technique through the example of indirect taxes]. *Nalogi-zhurnal = Taxes Journal*, 2006, no. 2, pp. 7–14.
URL: <https://wiselawyer.ru/poleznoe/18069-sootnoshenie-ponyatij-sposob-vzimaniya-naloga-tekhnika-oblozheniya> (In Russ.)
4. Kuchеров I.I. [Taxable item as a legal basis of taxation]. *Finansovoe pravo = Financial Law*, 2009, no. 1, pp. 6–12. URL: <https://www.lawmix.ru/bux/35803> (In Russ.)
5. Shashkova A.V. [Transition from pre-industrial to industrial society: Change of tax policy model]. *Finansovoe pravo = Financial Law*, 2017, no. 5, pp. 39–42.
URL: <http://отрасли-права.пф/article/25449> (In Russ.)

6. Kuznetsov N.G., Kochmola K.V., Evlakhova Yu.S., Koshel' N.V. [Financial thermodynamics: New approaches in the study of the global financial system]. *Finansovye issledovaniya = Financial Research*, 2010, no. 3, pp. 3–9. URL: <https://cyberleninka.ru/article/n/finansovaya-termodinamika-novye-podhody-v-issledova-nii-mirovoy-finansovoy-sistemy> (In Russ.)
7. Efremov A.A. [Formation of the concept of information sovereignty of the State]. *Pravo. Zhurnal Vysshei shkoly ekonomiki = Law. Journal of Higher School of Economics*, 2017, no. 1, pp. 201–215. URL: <https://cyberleninka.ru/article/n/formirovanie-kontseptsii-informatsionnogo-suvereniteta-gosudarstva> (In Russ.)
8. Tsirlov V.L. [Legal foundations of cybersecurity in Russia]. *Pravovaya informatika*, 2014, no. 3, pp. 54–56. URL: <https://cyberleninka.ru/article/n/pravovye-osnovy-kiberbezopasnosti-rossiyskoy-federatsii> (In Russ.)
9. Shashkova A.V. [Russian specifics of combating corruption]. *Kutafin University Law Review*, 2015, vol. 2, no. 1, pp. 51–68. URL: http://archive.kulawr.ru/articles/article_101513.html (In Russ.)
10. Shashkova A.V. [Pro et contra criminalization of corporate liability in the Russian Federation]. *Kutafin Law Review*, 2017, vol. 4, no. 2, pp. 544–554. URL: http://archive.kulawr.ru/netcat_files/521/703/2.2017_KULawR__Anna_V._Shashkova__544_554.pdf (In Russ.)
11. Ashmarina E.M., Kudryashova E.V., Terekhova E.V. et al. *Finansovo-pravovye aspekty i finansovaya politika innovatsionnogo razvitiya sovremennoi rossiiskoi ekonomiki. Kollektivnaya monografiya* [Financial and legal aspects and financial policy of innovation development of the modern Russian economy. A joint monograph]. Moscow, Elit Publ., 2011.
12. Povetkina N.A., Ledneva Yu.V. ['Fintech' and 'Regtech': Boundaries of Legal Regulation]. *Pravo. Zhurnal Vysshei shkoly ekonomiki = Law. Journal of Higher School of Economics*, 2018, no. 2, pp. 46–67. URL: <https://law-journal.hse.ru/data/2018/08/01/1152219816/%D0%BF%D0%BE%D0%B2%D0%B5%D1%82%D0%BA%D0%B8%D0%BD%D0%B0.pdf> (In Russ.)
13. Kucherov I.I., Povetkina N.A., Akopyan O.A. *Riski finansovoi bezopasnosti: pravovoi format: monografiya* [Risks to financial security: Legal format: a monograph]. Moscow, IZISP, Norma Publ., 2018, 304 p.
14. Govender S.G., Looock M., Kritzing E. Enhancing Information Security Culture to Reduce Information Security Cost: A Proposed Framework. In: *Cyberspace Safety and Security. 10th International Symposium, CSS 2018, Amalfi, Italy, October 29–31, 2018, Proceedings*. Springer Nature Switzerland AG, 2018, pp. 281–290. URL: <https://doi.org/10.1007/978-3-030-01689-0>
15. Dobrobaba M.B. *Sluzhebno-deliktnye pravootnosheniya: monografiya* [Official and delictual relations: a monograph]. Moscow, Yurlitinform Publ., 2013, 296 p.
16. Petrenko S.A. [Justifying the investments in cybersecurity]. *Trudy Instituta sistemnogo analiza Rossiiskoi Akademii nauk = Proceedings of the Institute for Systems Analysis of the Russian Academy of Sciences*, 2006, vol. 27, pp. 266–276. URL: <http://www.isa.ru/proceedings/images/documents/2006-27/266-276.pdf> (In Russ.)
17. Voitov M. [Critical infrastructure in the context of security]. *Indeks bezopasnosti = Security Index*, 2016, vol. 22, no. 1, pp. 137–142. (In Russ.)

Conflict-of-interest notification

I, the author of this article, bindingly and explicitly declare of the partial and total lack of actual or potential conflict of interest with any other third party whatsoever, which may arise as a result of the publication of this article. This statement relates to the study, data collection and interpretation, writing and preparation of the article, and the decision to submit the manuscript for publication.