Неправомерное воздействие на критическую информационную инфраструктуру: уголовная ответственность ее владельцев и эксплуатантов

ТРУНЦЕВСКИЙ Юрий Владимирович, ведущий научный сотрудник отдела методологии противодействия коррупции Института законодательства и сравнительного правоведения при Правительстве Российской Федерации, доктор юридических наук, профессор
117218, Россия, г. Москва, ул. Большая Черемушkinsкая, 34
E-mail: trunzev@yandex.ru

Федеральным законом от 26 июля 2017 г. № 194-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона “О безопасности критической информационной инфраструктуры Российской Федерации”» была введена статья 274¹ «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации» Уголовного кодекса Российской Федерации, описывающая криминальные угрозы объектам критической информационной инфраструктуры и устанавливающая основания уголовной ответственности ее владельцев и эксплуатантов.

Диспозиция ч. 3 ст. 274¹ УК РФ включает противоправные деяния как в форме активного действия, так и бездействия в отношении соблюдения правил эксплуатации и нарушения правил доступа к объектам критической информационной инфраструктуры Российской Федерации. Обязательным признаком составов рассматриваемых преступлений является наступление общественно опасных последствий: причинение вреда критической информационной инфраструктуре (ч. 3 и 4) и тяжкие последствия, имеющие значение для безопасности данной инфраструктуры (ч. 5). Субъект (исполнитель) данного преступления — специальный (владелец/эксплуатант критической информационной инфраструктуры), имеющий доступ к критической информационной инфраструктуре либо к относящимся к ней объектам в силу выполнения своих служебных полномочий и обязанный исполнять установленные правила эксплуатации и доступа к ним.

В статье даны рекомендации по квалификации соответствующих противоправных деяний.

Ключевые слова: критическая информационная инфраструктура, безопасность, уголовная ответственность, общественно опасные последствия, квалификация преступлений.

Unlawful Impact on Critical Information Infrastructure: The Criminal Liability of Its Owners and Operators

Yu. V. TRUNTSEVSKY, leading research fellow of the Department of methodology of combating corruption of the Institute of Legislation and Comparative Law under the Government of the Russian Federation, doctor of legal sciences, professor

34, Bolshaya Cheremushkinskaya st., Moscow, Russia, 117218

E-mail: trunzev@yandex.ru

Federal Law of July 26, 2017 No. 194-FZ “On Amendments to the Criminal Code of the Russian Federation and the Article 151 of the Criminal Procedure Code of the Russian Federation in connection with the adoption of the Federal Law “On the Security of Critical Information Infrastructure of the Russian Federation” introduced a new article — 274 “Irregular impact on the critical information infrastructure of the Russian Federation”, which describes criminal threats to objects of critical information infrastructure, in parts 3, 4 and 5, i.e. the grounds of criminal responsibility of its owners and operators.

Methodology: dialectics, hermeneutics, synergy, philosophical conceptology.

The disposition of the Article 274 Part 3 of the Criminal Code of the Russian Federation includes unlawful acts, both in the form of active action and inaction regarding compliance with operating rules and violation of the rules for access to critical information infrastructure objects of the Russian Federation. An obligatory sign of the component elements of the considered crimes is the occurrence of socially dangerous consequences: harm to the critical information infrastructure (part 3 and 4) and grave consequences that are important for the safety of this infrastructure (part 5). The subject (performer) of this crime is a special one (the owner / operator of the critical information infrastructure) who has access to the critical information infrastructure or objects related to it due to the fulfillment of his/her official powers and is obliged to fulfill the established rules of operation and access to them.

The article contains recommendations on the qualification of the relevant offenses.

Keywords: critical information infrastructure, security, criminal liability, socially dangerous consequences, qualification of crimes.

DOI: 10.12737/art_2019_5_9

Переход к информационному обществу в России приводит к тому, что значительное число бизнес-процессов и систем управления в стратегических отраслях экономики и государственного управления осуществляется на основе информационных технологий¹. Национальное благополучие во многом сейчас зависит от безопасной и устойчивой критической инфраструктуры (системы и сети, лежащие в основе организации общества). Причинение критической информационной инфраструктуре (далее — КИИ) ущерба может привести к разрушающим и необратимым последствиям для их защищенности, а исходя из того, что КИИ выступает связующим звеном между другими областями национальной инфраструктуры, это неизбежно приведет к негативным для них последствиям.

«Многие киберинциденты становятся возможными из-за отсутствия устойчивости и надежности инфраструктуры частных и общественных сетей, плохо защищенных баз данных и других недостатков в критической информационной инфраструктуре»².

¹ См., например: Хабриева Т. Я. Право перед вызовами цифровой реальности // Журнал российского права. 2018. № 9. С. 5—16; Хабриева Т. Я., Черногор Н. Н. Право в условиях цифровой реальности // Журнал российского права. 2018. № 1. С. 85—102.

² Пункт «Н» Резолюции ЕС О киберзащите (On Cyber Defence) от 25 мая 2018 г. (2018/2004 (INI)). URL: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2018-0189+0+DOC+XML+V0//EN>.

Современное киберпространство характеризуется неадекватностью кибербезопасности³. В последние годы существенно увеличилось число инцидентов, связанных с компьютерными атаками⁴, и злоумышленники постоянно находят новые способы их совершения. По оценкам ФСБ России, в 2016 г. было зафиксировано около 70 млн попыток атак на объекты КИИ России⁵. По наблюдениям экспертов в сфере информационной безопасности, в 2017 г. число АРТ-атак выросло в два раза⁶. Последняя крупная мировая кибератака⁷ произошла в мае 2017 г. — хакеры запустили в сеть вирус WCry, кото-

www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2018-0189+0+DOC+XML+V0//EN.

³ См.: Шувалов И. И., Хабриева Т. Я., Цзинжу Фэн и др. Киберпространство БРИКС: правовое измерение: монография / отв. ред. Д. Руйпин, Т. Я. Хабриева; сост. Жун Фу, Н. М. Бевеликова. М., 2017. 336 с.

⁴ См.: Трунцевский Ю. В. Киберпреступления в корпоративной среде: риски, оценка и меры предупреждения // Российский следователь. 2014. № 21. С. 19—22.

⁵ См.: Российская газета. 2017. 24 янв.

⁶ URL: https://www.automation.siemens.com/solutionpartner/partnerfinder/Home/Index?lang=ru&stc=wwcg115371&s_kwcid=AL462!90!1523820511!search!!!4754229500&ef_id=WRw0ZQAAAGivcRIw:20180813111823:s.

⁷ Подробнее см.: Капустин А. Я. К вопросу о международно-правовой концепции угроз международной информационной безопасности // Журнал зарубежного законо-

рый поразил сначала больницы Великобритании, а потом стал распространяться и на другие страны. Вирус атаковал компьютеры в Бельгии, Германии, во Франции, в Португалии, Испании, Китае, США, Бразилии, Украине, Италии, Индии, Чехии, Турции, Канаде, России и других странах (жертвами стали пользователи 75 стран)⁸.

Согласно ст. 14 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (далее — Закон о безопасности КИИ) «нарушение требований настоящего Федерального закона и принятых в соответствии с ним иных нормативных правовых актов влечет за собой ответственность в соответствии с законодательством Российской Федерации». За нарушение законодательства о безопасности КИИ предусмотрена уголовная ответственность.

«Именно масштабы потенциальной общественной опасности стали поводом для разработки и принятия данного Федерального закона»⁹. В целях формирования нормативной базы в части уголовной ответственности за нарушения Закона о безопасности КИИ был принят Федеральный закон от 26 июля 2017 г. № 194-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона “О безопасности критической информационной инфраструктуры Российской Федерации”», вносящий изменения в УК РФ.

дательства и сравнительного правоведения. 2017. № 6. С. 44—51.

⁸ URL: https://www.itv.ru/news/2017-05-13/325215-virus_atakoval_kompyuternye_seti_po_vsemu_miru.

⁹ Черемисинова М. Е. О формировании системы обеспечения безопасности критической информационной инфраструктуры Российской Федерации. URL: <http://comitasgentium.com/ru/o-формировании-системы-обеспечения-б/>.

В Уголовный кодекс включена специальная ст. 274¹ «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации», подследственность уголовных дел по которой (наряду со ст. 272, 273 и 274) передана ФСБ России, а также следователям органа, выявившего эти преступления (ч. 5 ст. 151 УПК РФ). Данные изменения вступили в силу с 1 января 2018 г., и пока какая-либо судебная практика по преступлениям, описанным в ч. 3—5 ст. 274¹ УК РФ, отсутствует¹⁰.

Части 3—5 ст. 274¹ УК РФ распространяются на владельцев/эксплуатантов КИИ. Санкции за совершение данных деяний предусматривают, с учетом различных квалифицирующих признаков, такие наказания, как штраф, принудительные работы, лишение свободы с лишением права занимать определенные должности или заниматься определенной деятельностью.

Объектом преступления (ч. 3—5 ст. 274¹ УК РФ) выступают общественные отношения по обеспечению правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в вышеуказанных системах, а также правил доступа к указанным объектам

Предметом преступления (ч. 3—5 ст. 274¹ УК РФ) являются КИИ России; информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, сети электросвязи, относящиеся к КИИ Российской Федерации. Под КИИ понимаются ИТ-системы государственных и коммерческих организаций, сбои в которых (в том числе в результате хакерских атак) могут привести к тяжелым социальным, политическим, экологическим и прочим последствиям.

Термин «критическая» относится к инфраструктуре, которая при вы-

¹⁰ См.: URL: <http://sudact.ru/regular/>.

ведении из строя или разрушении приведет к катастрофическому и далеко идущему ущербу. Критическая инфраструктура страны обеспечивает ключевые услуги, которые лежат в основе российского общества.

Понятие критической информационной инфраструктуры Российской Федерации содержится в п. 6 ст. 2 Закона о безопасности КИИ; информационной системы — в ГОСТ Р 50922-2006 «Защита информации»¹¹; информационно-телекоммуникационной сети — в п. 4 ст. 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»; автоматизированной системы управления — в п. 1 ст. 2 Закона о безопасности КИИ; сети электросвязи (средства связи) — в п. 28 ст. 2 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи».

Итак, в составе КИИ выделяются информационная и телекоммуникационная среды.

Информационная среда КИИ представляет собой совокупность вычислительных и информационных ресурсов, образующих автоматизированную систему управления технологическими процессами критически важных объектов (АСУ ТП КВО). При этом вычислительные ресурсы формируются системой локальных вычислительных сетей, других программных средств и средств вычислительной техники и могут быть использованы для организации распределенных вычислений (например, при моделировании сложных социальных и физических процессов, дешифровке зашифрованного кода).

Телекоммуникационная среда КИИ образуется совокупностью телекоммуникационных устройств; линий связи и каналов образующего оборудования; систем открытых протоколов обмена информацией

между телекоммуникационными устройствами; глобальной системы цифровых адресов и доменных имен (цифровых идентификаторов); программного обеспечения, реализующего алгоритмы, методы и процессы телекоммуникационной связи на основе протоколов взаимодействия локальных вычислительных сетей и предоставляющего доступ к ним и иным средствам автоматизированной обработки информации.

Субъектами КИИ согласно п. 98 ст. 2 Закона о безопасности КИИ являются государственные органы и учреждения, российские юридические лица и (или) индивидуальные предприниматели. Данным субъектам на праве собственности, аренды или на ином законном основании должны принадлежать информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления. Такие объекты должны функционировать в следующих сферах: здравоохранение, наука, транспорт, связь, энергетика, банковская и иные сферы финансового рынка, ТЭК, атомная энергия, оборонная, ракетно-космическая, горнодобывающая, металлургическая и химическая промышленность. Субъектами КИИ также являются российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

Объективная сторона рассматриваемых составов преступления (ч. 3—5 ст. 274¹ УК РФ) выражается в неправомерном воздействии на КИИ РФ путем:

нарушения правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в ней, или информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к КИИ РФ;

нарушения правил доступа к указанной информации, информацион-

¹¹ Утв. приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст.

ным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи.

Такие деяния могут совершаться в форме как активного действия, так и бездействия в отношении соблюдения указанных правил эксплуатации или доступа.

Характерный пример преступного бездействия — неустановка обновлений программного обеспечения. Работник субъекта КИИ должен провести анализ угроз и принять дополнительные меры защиты от этих угроз. Если в результате расследования компьютерного инцидента выяснится, что доступ произошел благодаря уязвимости, устраняемой посредством обновления компьютерных программ, которое на тот момент было доступным для соответствующей организации, невыполнение этих требований будет являться признаком объективной стороны преступления, предусмотренного ст. 274¹ УК РФ. Судебная практика по уголовным делам в сфере компьютерных преступлений¹² показывает, что субъектом такого преступления становится ИТ-персонал, если эти нарушения совершены им самовольно в нарушение политики информационной безопасности, принятой в организации, в том числе руководители организации, если ИТ-персонал действовал по их приказу или в его отсутствие при наличии необходимости издания соответствующего распоряжения.

По конструкции состав преступления материальный, предусматривает наступление общественно опасных последствий (как момента окончания преступления) — вреда

критической информационной инфраструктуре Российской Федерации (ч. 3—4 ст. 274¹ УК РФ) и тяжких последствий (ч. 5 ст. 274¹ УК РФ).

То есть законодатель логично ставит ответственность в зависимости от наступления общественно опасных последствий преступления, но при этом не устанавливает правил по определению размера тяжести такого вреда, оставляя данный вопрос на стороне судебной системы, которая, в свою очередь, получает возможность трактовать данное положение уголовного закона довольно широко, самостоятельно определяя порог размера малозначительности причиняемого вреда.

Согласно п. 19 постановления Пленума ВС РФ от 29 ноября 2016 г. № 55 «О судебном приговоре» квалификация преступления по той или иной статье уголовного закона, ее части либо пункту должна быть мотивирована судом. Это относится к признанию подсудимого виновным в совершении преступления по таким оценочным признакам, как существенный вред, тяжкие последствия. При этом суды не могут ограничиваться лишь указанием на подобный признак, а в описательно-мотивировочной части приговора обязаны привести обстоятельства, которые послужили основанием для вывода о наличии в содеянном такого признака. Размер вреда — признак оценочный и определяется судом в каждом конкретном случае. В рассматриваемой статье УК РФ вред причиняется критической информационной инфраструктуре Российской Федерации. В соответствии с п. 6 ст. 2 Закона о безопасности КИИ критическую информационную инфраструктуру составляют ее объекты, а также сети электросвязи, которые используются при организации взаимодействия этих объектов. В связи с этим вред может носить либо материальный (физический), либо организационный (технологически-эксплуатационный) характер, выразившийся в нарушении и (или)

¹² URL: http://sudact.ru/regular/doc/?regular-txt=%D0%98%D0%A2&regular-case_doc=&regular-lawchunkinfo=&regular-doc_type=1008&regular-date_from=&regular-date_to=&regular-workflow_stage=&regular-area=&regular-court=&regular-judge=#searchResult.

прекращении функционирования объекта КИИ, сети электросвязи, которая используется при организации взаимодействия таких объектов, либо в нарушении безопасности информации, обрабатываемой таким объектом, в том числе если это произошло посредством компьютерной атаки (компьютерный инцидент).

Анализ судебной практики по преступлениям, имеющим материальный состав, показывает, что единого подхода к определению понятия «тяжкие последствия» с точки зрения их размера в денежном выражении не выявлено — в каждом случае суд должен установить размер вреда/тяжесть последствий исходя из обстоятельств дела, а также в контексте существующей правоприменительной практики и неопределенности толкования размеров ущерба, точно определить категорию последствия часто представляется крайне сложной задачей.

Исходя из того, что данный признак последствий является особо квалифицированным и помещен в ч. 5 ст. 274¹ УК РФ, можно заключить, что «тяжкие последствия» включают более опасные последствия, чем «вред» КИИ, закрепленный в ч. 3 данной статьи.

Тяжкие последствия (ч. 5) в отличие от вреда (ч. 3) могут распространяться как на объекты КИИ, так и на деятельность субъектов КИИ. Такие последствия могут иметь значение для безопасности КИИ — защищенности, обеспечивающей ее устойчивое функционирование при проведении в отношении ее компьютерных атак, в том числе противоправном нарушении эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты (технические, программные, программно-аппаратные и иные средства для обнаружения (в том числе для поиска признаков компьютерных атак в сетях электросвязи, используемых для орга-

низации взаимодействия объектов критической информационной инфраструктуры), предупреждения, ликвидации последствий компьютерных атак и (или) обмена информацией, необходимой субъектам КИИ при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак, а также криптографические средства защиты такой информации). Например, причинение организации (субъекту КИИ) материального ущерба, репутационного вреда или возникновение иных негативных для нее последствий; нарушение технологических и бизнес-процессов организации.

В случае с КИИ тяжкие последствия не должны ограничиваться материальным ущербом, например при остановке воздушного сообщения можно говорить о наступлении тяжких последствий, учитывая критерий массовости, т. е. когда нарушаются права и свободы большого количества субъектов права, когда в результате компьютерного инцидента появляются пострадавшие люди, которые не смогли вовремя вылететь из аэропорта, лишились билетов, самолеты не смогли сесть на аэродром и т. п. В случае отказа системы и, как следствие, прерывания какого-то технологического процесса (например, атомной электростанции) финансовые и другого рода потери будут исчисляться в миллиардах рублей.

Одновременно с этим к тяжким последствиям можно отнести гибель и серьезные травмы людей, разрушения и уничтожение информационной инфраструктуры, нанесение вреда безопасности государства и т. д. То есть тяжесть последствий должна определяться с учетом причинения (или реальности созданной угрозы) тяжкого вреда здоровью людей или смерти, материального ущерба, серьезного нарушения деятельности предприятий, аварий и катастроф, уничтожения, блокирования, модификации или копиро-

вания привилегированной информации особой ценности¹³.

Субъект (исполнитель) рассматриваемых составов преступлений — специальный: это вменяемое лицо, достигшее возраста 16 лет, имеющее доступ к КИИ РФ либо к относящимся к ней объектам в силу выполнения служебных обязанностей по исполнению установленных правил эксплуатации и доступа к КИИ РФ.

Под лицами, использующими свое служебное положение, в ч. 4 ст. 274¹ УК РФ следует понимать лиц, осуществляющих организационно-распорядительные или административно-хозяйственные обязанности в организации, иных лиц¹⁴. В организации признаками такого лица могут обладать: руководители организации или ее подразделений и работники, уполномоченные на решение задач по информационной безопасности, а также иные лица, выполняющие на основании гражданско-правовых договоров задачи по обеспечению безопасности КИИ.

Исходя из того, что к субъектам КИИ относятся российские юридические лица, которым принадлежат данные системы, в случае передачи ими КИИ на баланс аутсорсинговой компании, сделавшая это, например, нефтяная компания под определение субъекта КИИ не подходит, и поэтому ее сотрудники (руководители) не могут быть исполнителями преступления, предусмотренного ч. 3 ст. 274¹ УК РФ. Вместе с тем, если такая организация передала КИИ на аутсорсинг, но у нее остались ком-

пьютеры, через которые можно удаленно подключаться к КИИ, ее следует считать субъектом КИИ, а ее сотрудников — субъектами рассматриваемых преступлений, несмотря на то, что непосредственно соответствующей КИИ она не владеет.

С *субъективной стороны* деяние, описанное в ч. 3 ст. 274¹ УК РФ, характеризуется виной как в форме умысла, так и неосторожности — невыполнение необходимых мероприятий по обеспечению безопасности объекта КИИ, что повлекло причинение ему вреда. Такая трактовка форм вины связана с тем, что нарушения штатного режима функционирования АСУ ТП КВО могут быть следствием как ошибок в работе ее систем и устройств, так и целенаправленного воздействия на АСУ ТП КВО, т. е. важно учитывать причины возникновения нарушений. Лицо предвидит причинение вреда КИИ в результате нарушения им правил эксплуатации (доступа), но без достаточных к тому оснований самонадеянно рассчитывает на предотвращение возможного наступления последствий, либо не предвидит их, хотя при должной осмотрительности и внимательности это лицо должно было и могло их предвидеть.

Таким образом, анализ признаков составов преступлений, предусмотренных ч. 3—5 ст. 274¹ УК РФ, позволил сформулировать положения по квалификации неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации ее владельцами и эксплуатантами. Так, диспозиция ч. 3 данной статьи включает противоправные деяния в форме как активного действия, так и бездействия в отношении соблюдения правил эксплуатации и доступа к объектам КИИ. Обязательным признаком составов рассматриваемых преступлений является наступление общественно опасных последствий: причинение вреда КИИ РФ (ч. 3 и 4) и тяжкие последствия, имеющие значение

¹³ См.: Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации. URL: <https://genproc.gov.ru/documents/nauka/execution/document-104550/>.

¹⁴ См. п. 10 постановления Пленума ВС РФ от 28 июня 2011 г. № 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности».

для ее безопасности (ч. 5). Субъект (исполнитель) данного преступления — специальный (владелец/эксплуатант КИИ), имеющий доступ к КИИ РФ либо к от-

носящимся к ней объектам в силу исполнения своих служебных обязанностей и обязанный исполнять установленные правила эксплуатации, доступа к КИИ.

Библиографический список

Капустин А. Я. К вопросу о международно-правовой концепции угроз международной информационной безопасности // Журнал зарубежного законодательства и сравнительного правоведения. 2017. № 6.

Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации. URL: <https://genproc.gov.ru/documents/nauka/execution/document-104550/>.

Трунцевский Ю. В. Киберпреступления в корпоративной среде: риски, оценка и меры предупреждения // Российский следователь. 2014. № 21.

Хабриева Т. Я. Право перед вызовами цифровой реальности // Журнал российского права. 2018. № 9.

Хабриева Т. Я., Черногор Н. Н. Право в условиях цифровой реальности // Журнал российского права. 2018. № 1.

Черемисинова М. Е. О формировании системы обеспечения безопасности критической информационной инфраструктуры Российской Федерации. URL: <http://comitasgentium.com/ru/o-формировании-системы-обеспечения-б/>.

Шувалов И. И., Хабриева Т. Я., Цзинжу Фэн и др. Киберпространство БРИКС: правовое измерение: монография / отв. ред. Д. Руйпин, Т. Я. Хабриева; сост. Жун Фу, Н. М. Бевеликова. М., 2017.

References

Cheremisinova M. Ye. About formation of security system of critical information infrastructure of the Russian Federation. Available at: <http://comitasgentium.com/ru/o-formirovani-sistemy-obespecheniya-b/>. (In Russ.)

Guidelines for the implementation of prosecutorial supervision over the implementation of laws in the investigation of crimes in the field of computer information. Available at: <https://genproc.gov.ru/documents/nauka/execution/document-104550/>. (In Russ.)

Kapustin A. Ya. The question of the international legal concept of threats to international information security. *Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniya* = *Journal of Foreign Legislation and Comparative Law*, 2017, no. 6, pp. 44—55. (In Russ.)

Khabrieva T. Y. Law Facing the Challenges of Digital Reality. *Zhurnal rossijskogo prava* = *Journal of Russian Law*, 2018, no. 9, pp. 5—16. (In Russ.)

Khabrieva T. Y., Chernogor N. N. The Law in the Conditions of Digital Reality. *Zhurnal rossijskogo prava* = *Journal of Russian Law*, 2018, no. 1, pp. 85—102. (In Russ.)

Shuvalov I. I., Khabrieva T. Y., Tszinzhu Fen et al. Cyberspace BRICS: legal dimension. Ed. by D. Ruypin, T. Y. Khabrieva, Zhun Fu, N. M. Bevelikova. Moscow, 2017. 336 p. (In Russ.)

Truntsevskiy Yu. V. Cybercrime in corporate sphere: risks, evaluation and measures of prevention. *Rossiyskiy sledovatel*, 2014, no. 21, pp. 19—22. (In Russ.)