

**РИСКИ В УСЛОВИЯХ ЦИФРОВОГО ОБЩЕСТВА И ТЕНДЕНЦИИ ИХ РАЗВИТИЯ****Анатолий Анатольевич КИЛЯЧКОВ <sup>а\*</sup>, Лариса Алексеевна ЧАЛДАЕВА <sup>б</sup>**

<sup>а</sup> доктор экономических наук, профессор кафедры экономики организации,  
Финансовый университет при Правительстве РФ, Москва, Российская Федерация  
Chaldaeva45@mail.ru  
<https://orcid.org/0000-0001-6203-4968>  
SPIN-код: 6565-5829

<sup>б</sup> независимый исследователь, кандидат технических наук, старший научный сотрудник,  
Москва, Российская Федерация  
AAKil@mail.ru  
<https://orcid.org/0000-0002-6950-4085>  
SPIN-код: 1257-1461

\* Ответственный автор

**История статьи:**

Получена 10.04.2019  
Получена в доработанном  
виде 24.04.2019  
Одобрена 14.05.2019  
Доступна онлайн 28.06.2019

УДК 330.85

JEL: A11, A12, B14

**Аннотация**

**Предмет.** Специфические риски, появившиеся в процессе формирования цифрового общества.

**Цели.** Выработка предложений по противодействию формирующимся угрозам и возникающим вызовам в условиях появления цифровых технологий и всестороннего внедрения новых способов организации экономических процессов.

**Методология.** Проведен анализ инцидентов, произошедших в киберпространстве за последние годы. Определение причин, которые привели к возникновению угроз, позволило выявить тенденции их развития. Последующая экстраполяция выявленных тенденций на ближайшие годы указывает на возможность появления принципиально новых киберугроз.

**Результаты.** Степень ущерба от реализации рисков, порожденных цифровыми технологиями, возрастала, начиная от банального грабежа и мошенничества через шантаж и скрытое использование ресурсов жертвы кибернападения до угрозы диверсионных актов и их совершения. Возможности цифровых технологий порождают не только очевидные и просчитываемые риски, но и принципиально новые угрозы, которые либо не рассматриваются вовсе, либо вероятность которых считается пренебрежимо малой. Ущерб от реализации подобных рисков может быть весьма значительным.

**Выводы.** Для ответа на возникающие риски потребуются создание соответствующего инструментария, важнейшим элементом которого является наличие национального сегмента Интернета. В настоящее время идет процесс осознания Россией своих национальных интересов в виртуальном пространстве, который представляет собой начало формирования виртуального государства.

**Ключевые слова:** риски  
и угрозы, цифровая  
экономика, высокие  
технологии,  
информационное общество,  
противодействие угрозам

© Издательский дом ФИНАНСЫ и КРЕДИТ, 2019

**Для цитирования:** Кильячков А.А., Чалдаева Л.А. Риски в условиях цифрового общества и тенденции их развития // *Финансы и кредит*. — 2019. — Т. 25, № 6. — С. 1444 — 1453.  
<https://doi.org/10.24891/fc.25.6.1444>

Формирование цифрового общества не только предоставляет новые возможности для развития экономики, но и приводит к появлению специфических рисков, обусловленных появлением новых технологий. Поэтому выявление новых рисков, возникающих при построении

информационного общества<sup>1</sup>, и способов их предотвращения является в настоящее время актуальной задачей. Для того чтобы достойно встретить формирующиеся угрозы и

<sup>1</sup> Указ Президента Российской Федерации от 09.05.2017 № 203 «О стратегии развития информационного общества в Российской Федерации на 2017–2030 годы».  
URL: <http://www.garant.ru/products/ipo/prime/doc/71570570/>

возникающие вызовы, необходимо рассмотреть существующие в настоящее время риски в области высоких технологий, выявить тенденции их развития и выработать предложения по противодействию возможным угрозам<sup>2</sup> [1].

На начальном этапе развития информационных технологий порождаемые ими риски были достаточно очевидны и представляли собой действия, больше похожие на банальный грабёж. Для вымогательства денежных средств использовались программы-шифровальщики, которые широко используются и до настоящего времени. Проникая в компьютер, они шифруют содержащиеся в нем файлы, а затем предлагают купить ключ для их расшифровки. При этом совсем нет гарантии того, что этим ключом удастся расшифровать зашифрованные данные. В 2017 г. было зафиксировано две крупнейшие эпидемии шифровальщиков, вызванных известными программами WannaCry и ExPetr (он же Petya, он же NotPetya). К концу 2017 г. появился и новый шифровальщик, Bad Rabbit<sup>3</sup>.

Существуют программы-трояны, которые не вымогают, а самостоятельно крадут деньги у жертвы. Так, троян CryptoShuffler отслеживает все, что попадает в буфер обмена (команды «копировать» и «вставить») компьютера жертвы. Как только CryptoShuffler замечает, что в буфер обмена попадает адрес криптовалютного кошелька, он заменяет его адресом счета злоумышленника<sup>4</sup>. При этом CryptoShuffler не тормозит работу компьютера или смартфона и не требует выкуп. Наоборот, он старается работать как можно более скрытно, так как чем дольше его не найдут, тем больше денег он успеет украсть для своих создателей.

<sup>2</sup> Савина Т.Н. Цифровая экономика как новая парадигма развития: вызовы, возможности и перспективы // *Финансы и кредит*. 2018. Т. 24. № 3. С. 579—590. URL: <https://doi.org/10.24891/fc.24.3.579>

<sup>3</sup> Mamedov O., Sinitsyn F., Ivanov A. Bad Rabbit Ransomware. URL: <https://securelist.com/bad-rabbit-ransomware/82851/>

<sup>4</sup> Юнаковский С. Байки из блокчейна. URL: <https://securelist.ru/tales-from-the-blockchain/87860/>

До последнего времени действия по заражению компьютеров пользователей (кибератаки) носили неизбирательный характер. Однако недавно было обнаружено<sup>5</sup>, что злоумышленники стали уделять особое внимание бухгалтерам в целях кражи финансовых средств со счетов компаний. Для этого используются две программы-трояны: RTM и Buhtrap. Программа RTM распространяется через фишинговые рассылки, которые имитируют деловую переписку. Buhtrap внедряется в главные страницы крупных российских новостных сайтов, откуда попадает к жертвам. В результате заражения злоумышленники изменяют реквизиты получателя финансовых средств в файлах, которые используются для обмена данными между бухгалтерскими и банковскими программными системами.

Более продвинутые технологии грабежа, использующие программу-троян LokiBot, имитируют не только интерфейс мобильного банка, но и интерфейсы мессенджеров WhatsApp, Skype и Outlook, выводя уведомления о транзакциях от имени этих приложений. Эта программа не только подделывает экран банковского сайта, но и заставляет смартфон вибрировать как при получении уведомления о якобы пришедшем переводе. Если же попытаться избавиться от этого трояна, он шифрует данные на смартфоне, блокирует экран и обвиняет жертву в просмотре детской порнографии, требуя выкуп в размере в 100 долл. США, номинированный в биткоинах<sup>6</sup>.

Развитие программ-троянов шло также по пути эксплуатации компьютера жертвы, когда они заставляли его работать на мошенника (зарабатывать криптовалюту, майнить). Для злоумышленника это значительно более выгодно и безопасно, чем шифровать

<sup>5</sup> Шошин П. Киберпреступность фокусируется на бухгалтерях. URL: [https://www.kaspersky.ru/blog/financial-trojans-2019/22301/?utm\\_source=newsletter&utm\\_medium=Email&utm\\_campaign=kd%20weekly%20digest](https://www.kaspersky.ru/blog/financial-trojans-2019/22301/?utm_source=newsletter&utm_medium=Email&utm_campaign=kd%20weekly%20digest)

<sup>6</sup> Kovacs E. Removal Attempt Turns Android Banking Trojan into Ransomware. URL: <https://www.securityweek.com/removal-attempt-turns-android-banking-trojan-ransomware>

компьютеры, так как отсутствует необходимость каким-либо образом раскрывать себя при получении сворованных денег<sup>7</sup>. Дальнейшее развитие данной технологии может заключаться в том, что компьютеры заставят не только майнить криптовалюту, но и полностью работать на злоумышленников: производить вычисления, осуществлять поиск информации в Сети, хранить данные, скрытно следить за пользователем, прослушивать его и т.п. Другими словами, компьютер жертвы будет работать на злоумышленника в виртуальном пространстве, расходуя вполне реальные технические ресурсы, электроэнергию и информационный трафик жертвы, а также собирать о нем персональную информацию, в том числе интимного характера.

В настоящее время в социальных сетях есть все возможности для того, чтобы собрать информацию для целевого фишинга<sup>8</sup>. И если по фотографии жертвы этот процесс осуществляется не очень эффективно (успех в 30% случаев), то по имени и фамилии, особенно если они дополнены иной информацией (возраст, образование, не говоря уже об электронном адресе и телефоне) успешный результат достигается с гарантированной вероятностью. Если принимать во внимание наблюдающуюся тенденцию, можно сделать вывод о том, что в цифровом пространстве существует возможность найти и собрать всю информацию об интересующем человеке, включая компрометирующую.

При этом если негативная информация о человеке или близких ему людях отсутствует, то ее можно создать в виртуальном пространстве, а затем шантажировать жертву. Для этого уже есть все возможности. В 2016 г. на конференции Adobe MAX была

представлена программа, которая, анализируя фрагмент речи человека, может сгенерировать его голос, в том числе со словами, которых не было в исходной записи. Эта программа может стать инструментом для обхода систем голосовой идентификации, используемых в банках. Компании Adobe, Google и Lyrebird создают аналогичные системы, которые, используя минутную запись речи человека, могут научиться произносить его голосом произвольные фразы<sup>9</sup>.

Дальнейшее развитие этой тенденции состоит в подделке не только голоса, но и изображения человека, а также имитации общения с ним. Так китайское государственное информационное агентство «Синьхуа» представило первого виртуального ведущего новостей, который был создан благодаря технологиям машинного обучения<sup>10</sup>. Прототипом виртуального человека стал реальный ведущий новостных телепередач Чжан Чжао, который «подарил» своему цифровому коллеге собственную внешность, голос и даже свою мимику.

Еще дальше продвинулись ученые Вашингтонского университета, которые опубликовали результаты эксперимента по созданию виртуальных двойников знаменитых людей<sup>11</sup>. Разработанная ими программа обрабатывает фотографии и видео с изображением человека, анализирует его мимику и жестикуляцию и на основе собранных данных создает управляемого

<sup>7</sup> Булавас В., Лопатин Е. Майнеры на подъеме. URL: <https://securelist.ru/miners-on-the-rise/80257/>

<sup>8</sup> Гридасова А. Как злоумышленники собирают информацию для целевого фишинга. URL: [https://www.kaspersky.ru/blog/spearphishers-information/22228/?utm\\_source=newsletter&utm\\_medium=Email&utm\\_campaign=kd%20weekly%20digest](https://www.kaspersky.ru/blog/spearphishers-information/22228/?utm_source=newsletter&utm_medium=Email&utm_campaign=kd%20weekly%20digest)

<sup>9</sup> Куксов И. Технологичное телефонное мошенничество. URL: <https://www.kaspersky.ru/blog/synthetic-voice-phone-fraud/18521/>; Consumer Alert: 'Can You Hear Me' Scams. Phone Fraudsters Recording Consumers' Voice Responses. FCC Consumer Alert from the federal Communications Commission. URL: [https://transition.fcc.gov/Daily\\_Releases/Daily\\_Business/2017/db0327/DOC-344083A1.pdf](https://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db0327/DOC-344083A1.pdf); Let's Get Experimental: Behind the Adobe MAX Sneaks. URL: <https://theblog.adobe.com/lets-get-experimental-behind-the-adobe-max-sneaks/>

<sup>10</sup> Коняшин А. В Китае появился первый виртуальный ведущий новостей, созданный с помощью ИИ. URL: <https://gmbbox.ru/materials/38340-v-kitae-poyavilsya-perviy-virtualniy-vedushchiy-novostey-sozdanniy-s-pomoshchyu-ii>

<sup>11</sup> Барышинева В. Ученые создали виртуального двойника для любого человека. URL: <https://birdinflight.com/ru/novosti/hajtek/uchyonnye-sozdali-virtualnogo-dvojnika-dlya-lyubogo-cheloveka.html>; Suwajanakorn S., Kemelmacher-Shlizerman I., Seitz S.M. What Makes Kevin Spacey Look Like Kevin Spacey? URL: <https://arxiv.org/pdf/1506.00752v1.pdf>

виртуального персонажа, который выглядит и двигается в точности как его прототип.

Таким образом, современные цифровые технологии могут быть использованы для тотальной дезинформации жертвы, допустим, путем ее общения с виртуальным знакомым через Skype. Кроме того, возможно создание фейковых видеоматериалов, имеющих высокую степень достоверности в целях компрометации жертвы. Это можно делать как для шантажа и получения выкупа, так и для политической дискредитации публичного лица.

Современные виды мошенничества уже не ограничиваются только областью межличностных отношений и финансов. В настоящее время существует возможность удаленного управления транспортными средствами. Правда, установить полный контроль над автомобилем возможно только при установке нелицензированного программного обеспечения<sup>12</sup>. Так, в прошлом году появилось сообщение о взломе автомобиля марки Jeep Cherokee<sup>13</sup>. Более того, есть информация о том, что удалось получить доступ к внутренним системам самолета Boeing 757. Взлом произвел представитель Министерства внутренней безопасности США Роберт Хайки (Robert Hickey)<sup>14</sup>. Хотя самолет, компьютер которого был взломан, и находился на стоянке в аэропорту, но другие самолеты подобной модели эксплуатируются многими авиакомпаниями, например, Delta, American Airlines и United Airlines. На этом фоне особенно настораживает информация о том, что компания Raytheon разработала

программное обеспечение, которое устанавливается на бортовые компьютеры самолетов для управления запуском ракет с истребителей<sup>15</sup>. Взлом и удаленное управление этой программой может привести к катастрофическим последствиям военного-политического характера.

Существующие цифровые технологии позволяют воздействовать не только на транспортные средства, но и на объекты реального сектора экономики. По всему миру функционируют промышленные роботы, которые осуществляют различные операции по заранее заданной программе. Эти устройства состоят из управляющего компьютера, контроллера и механических манипуляторов. На компьютере работает программа, выполняющая заложенный в нее алгоритм действий. Контроллер преобразует их в последовательность операций, осуществляемых манипулятором. Для этого контроллер использует так называемые конфигурационные файлы, в которых прописана вся информация, необходимая для того, чтобы подать на нужные сервомоторы манипулятора строго определенное напряжение в четко оговоренный момент времени и таким образом правильно выполнить операцию. Однако было обнаружено, что некоторые подобные промышленные роботы подключены напрямую к Интернету или к недостаточно защищенной заводской Wi-Fi сети. Это предоставляет злоумышленнику возможность обнаружить промышленный робот с помощью специализированного сканера и, даже не заменяя программу управляющего компьютера, перезаписать конфигурационные файлы контроллера, изменив логику его работы. В зависимости от целей хакерской атаки такой подход применим как для шпионажа, так и для проведения диверсионных операций при производстве высокоточных изделий. Например, отклоняя манипулятор в процессе электросварки на

<sup>12</sup> Марковская А. Умные машины: комфорт стоит денег... или безопасности. URL: [https://www.kaspersky.ru/blog/dont-hack-your-car/20203/?utm\\_source=newsletter&utm\\_medium=Email&utm\\_campaign=kd%20weekly%20digest](https://www.kaspersky.ru/blog/dont-hack-your-car/20203/?utm_source=newsletter&utm_medium=Email&utm_campaign=kd%20weekly%20digest)

<sup>13</sup> Выступление Чарли Миллера (Charlie Miller) и Криса Валасека (Chris Valasek) на Международной конференции по безопасности Black Hat USA 2015. URL: [https://www.youtube.com/watch?v=Tjvw5fz\\_GuA&list=PLH15HpR5qRsXF78lrpWP2JKpPJs\\_AFnD7](https://www.youtube.com/watch?v=Tjvw5fz_GuA&list=PLH15HpR5qRsXF78lrpWP2JKpPJs_AFnD7)

<sup>14</sup> Van Cleave K. Experts Working with Homeland Security Hacked into Boeing 757. URL: <https://www.cbsnews.com/news/homeland-security-hacked-boeing-757-jetliner/>

<sup>15</sup> WikiLeaks опубликовал документы ЦРУ о системе управления ракетами. URL: <https://ria.ru/20170907/1501993058.html>

доли миллиметра, что совершенно незаметно для глаза, робот будет производить брак. При этом управляющая программа промышленного робота остается совершенно неизменной, а подменяются только параметры на контроллере<sup>16</sup>.

Данная угроза уже была реализована. Специалисты полагают, что с июня 2009 г. по апрель 2010 г. пять промышленных комплексов в Иране подвергались нападениям при помощи программы-диверсанта Stuxnet<sup>17</sup>. Этот вирус был разработан для выведения из строя центрифуг, на которых Иран обогащает уран. Вирусная программа — диверсант увеличила скорость вращения центрифуг выше предельно допустимого значения, что привело к их разрушению. Причем операторы, обслуживающие аппаратуру, этого не заметили, так как контрольные датчики показывали значения скорости вращения центрифуг в пределах нормы.

Кроме того, есть подозрение, что блэкаут в Венесуэле в марте 2019 г. был инициирован кибер-диверсионными действиями США против энергосистемы суверенного государства<sup>18</sup>.

Таким образом, степень ущерба от реализации рисков, порожденных цифровыми технологиями, возростала начиная от банального грабежа и мошенничества через

шантаж и скрытую эксплуатацию объекта до угрозы диверсионных актов, а эта ситуация влечет за собой уже политические риски.

В конце прошлого года в США был принят весьма любопытный документ, получивший название «Стратегия национальной кибербезопасности Соединенных Штатов Америки»<sup>19</sup> [1–10]. В этом документе перед администрацией США были поставлены следующие задачи: защита американского образа жизни, обеспечение процветания США, сохранение мира методом принуждения и продвижение американского влияния. Для решения поставленных задач планируется увеличить возможности США по сдерживанию и наказанию лиц и государств, использующих цифровые инструменты против интересов США, а также расширить американское влияние за рубежом в целях более широкого внедрения принципов открытого, совместимого, надежного и безопасного Интернета.

В документе утверждается, что обеспечение безопасности киберпространства имеет основополагающее значение для реализации американской стратегии и требует как внедрения последних достижений технического прогресса, так и использование широкого набора эффективных мер принуждения. При этом планируется придать этим мерам экстерриториальный характер, включая механизмы привлечения к уголовной ответственности находящихся за рубежом лиц, совершивших преступления с использованием компьютерной техники.

США планируют использовать возможности киберпространства по всем направлениям реализации власти на национальном уровне для выявления, противодействия, обезвреживания и снижения уровня угроз, которые нарушают или противоречат национальным интересам, в целях обеспечения превосходства США в киберпространстве. Для этого США

<sup>16</sup> Quarta D., Pogliani M., Polino M. et al. Breaking the Laws of Robotics Attacking Industrial Robots. URL: <https://www.blackhat.com/docs/us-17/thursday/us-17-Quarta-Breaking-The-Laws-Of-Robotics-Attacking-Industrial-Robots.pdf>; Maggi F., Quarta D., Pogliani M. et al. Rogue Robots: Testing the Limits of an Industrial Robot's Security. URL: <https://www.blackhat.com/docs/us-17/thursday/us-17-Quarta-Breaking-The-Laws-Of-Robotics-Attacking-Industrial-Robots-wp.pdf>

<sup>17</sup> New Русская служба BBC. URL: [https://www.bbc.com/russian/international/2012/12/121225\\_iran\\_stuxnet\\_attack](https://www.bbc.com/russian/international/2012/12/121225_iran_stuxnet_attack). Ахмадинежад: иранские центрифуги подверглись кибератаке. URL: [https://www.bbc.com/russian/mobile/international/2010/11/101129\\_iran\\_cyberattack.shtml#sa-link\\_location=more-story-3&intlink\\_from\\_url=https%3A%2F%2Fwww.bbc.com%2Frussian%2Finternational%2F2012%2F12%2F121225\\_iran\\_stuxnet\\_attack&intlink\\_ts=1550933601223&story\\_slot=1-sa](https://www.bbc.com/russian/mobile/international/2010/11/101129_iran_cyberattack.shtml#sa-link_location=more-story-3&intlink_from_url=https%3A%2F%2Fwww.bbc.com%2Frussian%2Finternational%2F2012%2F12%2F121225_iran_stuxnet_attack&intlink_ts=1550933601223&story_slot=1-sa)

<sup>18</sup> Кто вызвал энергетический коллапс в Венесуэле. URL: <https://www.discred.ru/2019/03/14/kto-vyzval-energeticheskij-kollaps-v-venesuele>

<sup>19</sup> Стратегия национальной кибербезопасности Соединенных Штатов Америки. URL: [http://d-russia.ru/wp-content/uploads/2019/01/National-Cyber-Strategy\\_USA\\_2018.pdf](http://d-russia.ru/wp-content/uploads/2019/01/National-Cyber-Strategy_USA_2018.pdf)

будут использовать дипломатические, информационные, военные, финансовые, разведывательные методы, а также возможности правоохранительных органов.

В целях сохранения долгосрочной открытости, совместимости, безопасности и надежности Интернета США будут активно защищать свою позицию международного лидера для продвижения американского влияния и обеспечения своих интересов. США рассматривают принципы свободы Интернета неразрывно связанными со своей национальной безопасностью и будут продвигать свое видение открытого Интернета в качестве международного стандарта. Это предоставит американским компаниям большие конкурентные преимущества в рамках мировой цифровой экономики. При этом забота других стран о своем национальном суверенитете является неприемлемым для США поведением, угрожающим ее интересам. В качестве противников США в документе названы Россия, Китай, Иран и КНДР.

Причем США уже перешли к практическим действиям, которые реализуют задачи, сформулированные в Стратегии кибербезопасности. Недавно сайт WikiLeaks опубликовал очередную порцию секретных документов ЦРУ о программах-кибершпионах<sup>20</sup>. Из этих документов следует, что в ЦРУ разработаны программные закладки на зараженных компьютерах с операционной системой Windows, которые обеспечивают условия для осуществления слежки, запуск вредоносных приложений, а также хранение используемых хакерами драйверов и программных закладок.

Более того, Пентагон приступил к разработке новой стратегии боевых действий «Троянский конь», которая предполагает активное использование протестного потенциала пятой колонны для дестабилизации обстановки с одновременным нанесением ударов по

наиболее важным объектам<sup>21</sup>. Как показывает история цветных революций при их организации активно использовались возможности цифрового пространства для обмена информацией. Это объясняет ту настойчивость, с которой в Стратегии кибербезопасности США проводится мысль об открытом Интернете в качестве международного стандарта для продвижения американского влияния. Основываясь на подобных фактах, начальник Генерального штаба Вооруженных сил РФ В.В. Герасимов заявил о переносе военных действий в информационную сферу<sup>22</sup>.

Приведенные факты указывают на то, что цифровые технологии достигли такой степени развития, что порождаемые ими риски стали угрожать основам экономики, общества и самого государственного строя России. Это привело к появлению государственных программ управления подобными процессами. В декабре 2016 г. была подписана «Доктрина информационной безопасности Российской Федерации». Основное отличие российской Доктрины от американской киберстратегии состоит в том<sup>23</sup>, что Российская Федерация не заявляет о своём стремлении быть лидером в киберпространстве и никого противником не называет.

Следует отметить, что возможности высоких технологий порождают не только очевидные и просчитываемые риски, но и принципиально новые угрозы, которые либо не рассматриваются вовсе, либо вероятность которых считается пренебрежимо малой. Причем ущерб от реализации подобных рисков может быть весьма значительным. Отмеченные признаки указывают на то, что формирование цифрового общества

<sup>21</sup> Генштаб России объяснил суть американского «Троянского коня».  
URL: <https://ria.ru/20190302/1551501526.html>

<sup>22</sup> Генштаб предупредил о переносе военных действий в информационную сферу.  
URL: <https://ria.ru/20190302/1551498511.html>

<sup>23</sup> Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента РФ от 05.12.2016 № 646. URL: <https://www.garant.ru/products/ipo/prime/doc/71456224>; Ашманов И. Новая киберстратегия США: о мировом господстве прямым текстом.  
URL: <https://ria.ru/20190121/1549627256.html>

<sup>20</sup> WikiLeaks опубликовал новый пакет секретных документов ЦРУ о кибершпионаже.  
URL: <https://ria.ru/20170831/1501474835.html>

сопровождается угрозой реализации рисков типа «черного лебедя». Данное понятие было введено Н. Талебом, сформулировавшим характерные признаки подобных рисков [11]:

- 1) в прошлом не было зафиксировано признаков, предвещающих наступление этого риска, то есть до реализации данного риска он либо вообще не рассматривался, либо вероятность его наступления считалась пренебрежимо малой величиной;
- 2) реализация данного риска приводит к огромным, зачастую катастрофическим последствиям;

3) постфактум возникают различные объяснения произошедшего, которые делают данное событие объяснимым и предсказуемым.

Эти риски потребуют инструментария для ответа на возникающие угрозы, одним из которых является формирование национального сегмента Интернета. В настоящее время происходит формирование национального суверенитета России в виртуальном пространстве<sup>24</sup>, которое по существу представляет собой начало формирования виртуального государства<sup>25</sup>.

<sup>24</sup> Масальцева М. Госдума в первом чтении одобрила закон об автономной работе Рунета.

URL: [https://daily.afisha.ru/news/24092-gosduma-v-pervom-chtenii-odobrila-zakon-ob-avtonomnoy-rabote-runeta/?utm\\_source=yxnews&utm\\_medium=desktop](https://daily.afisha.ru/news/24092-gosduma-v-pervom-chtenii-odobrila-zakon-ob-avtonomnoy-rabote-runeta/?utm_source=yxnews&utm_medium=desktop)

<sup>25</sup> У россиян появится цифровое право.

URL: <https://news.mail.ru/society/36518454/?frommail=1>

## Список литературы

1. Шевченко И.В., Коробейникова М.С. Регулирование инновационно-инвестиционной безопасности России // Национальные интересы: приоритеты и безопасность. 2018. Т. 14. № 9. С. 1693—1730. URL: <https://doi.org/10.24891/ni.14.9.1693>
2. Устюжанина Е.В., Сизгарев А.В., Шеин Р.А. Цифровая экономика как новая парадигма экономического развития // Национальные интересы: приоритеты и безопасность. 2017. Т. 13. № 10. С. 1788—1804. URL: <https://doi.org/10.24891/ni.13.10.1788>
3. Бабанов В.Н. Факторы и проблемы развития цифровой экономики в России // Известия Тульского государственного университета. Экономические и юридические науки. 2017. № 4-1. С. 255—262. URL: <https://cyberleninka.ru/article/n/factory-i-problemy-razvitiya-tsifrovoy-ekonomiki-v-rossii>
4. Chakpitak N., Maneejuk P., Chanaim S., Sriboonchitta S. Thailand in the Era of Digital Economy: How Does Digital Technology Promote Economic Growth? Predictive Econometrics and Big Data: International Conference of the Thailand Econometrics Society. Studies in Computational Intelligence Series, 2018, pp. 350–362. URL: [https://doi.org/10.1007/978-3-319-70942-0\\_25](https://doi.org/10.1007/978-3-319-70942-0_25)
5. Martin-Shields C.P., Bodanac N. Peacekeeping's Digital Economy: The Role of Communication Technologies in Post-Conflict Economic Growth. *International Peacekeeping*, 2018, vol. 25, iss. 3, pp. 420–445. URL: <http://dx.doi.org/10.2139/ssrn.2970923>
6. Goldstein H. Editorial: The Digital Economy Act and Statistical Research. *Journal of the Royal Statistical Society. Series A: Statistics in Society*, 2017, vol. 180, iss. 4, pp. 945–946. URL: <https://doi.org/10.1111/rssa.12317>
7. Pilik M., Juříčková E., Kwarteng M.A. On-line Shopping Behaviour in the Czech Republic under the Digital Transformation of Economy. *Economic Annals-XXI*, 2017, vol. 165, iss. 5-6, pp. 119–123. URL: <https://doi.org/10.21003/ea.V165-24>
8. Tan K.H., Ji G., Lim C.P., Tseng M.-L. Using Big Data to Make Better Decisions in the Digital Economy. *International Journal of Production Research*, 2017, vol. 55, iss. 17, pp. 4998–5000. URL: <https://doi.org/10.1080/00207543.2017.1331051>
9. Milgrom P., Roberts J. The Economics of Modern Manufacturing: Technology, Strategy, and Organization. *The American Economic Review*, 1990, vol. 80, iss. 3, pp. 511–528. URL: [https://www.researchgate.net/publication/4901048\\_The\\_Economics\\_of\\_Modern\\_Manufacturing\\_Technology\\_Strategy\\_and\\_Organization](https://www.researchgate.net/publication/4901048_The_Economics_of_Modern_Manufacturing_Technology_Strategy_and_Organization)
10. Паньшин Б. Цифровая экономика: особенности и тенденции развития // Наука и инновации. 2016. Т. 3. № 157. С. 17—20. URL: <http://innosfera.by/files/2016/3.pdf>
11. Талей Н.Н. Черный лебедь. Под знаком непредсказуемости. М.: Колибри, 2016. 736 с.

## Информация о конфликте интересов

Мы, авторы данной статьи, со всей ответственностью заявляем 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.

**RISK IN TERMS OF DIGITAL SOCIETY AND THE DEVELOPMENT TRENDS****Anatolii A. KILYACHKOV<sup>a,\*</sup>, Larisa A. CHALDAEVA<sup>b</sup>**<sup>a</sup> Financial University under Government of Russian Federation, Moscow, Russian Federation

Chaldaeva45@mail.ru

<https://orcid.org/0000-0001-6203-4968><sup>b</sup> Independent researcher, Moscow, Russian Federation

AAKil@mail.ru

<https://orcid.org/0000-0002-6950-4085>

\* Corresponding author

**Article history:**

Received 10 April 2019

Received in revised form

24 April 2019

Accepted 14 May 2019

Available online

28 June 2019

**JEL classification:** A11, A12,  
B14**Keywords:** risks, threats,  
digital economy, high  
technologies, information  
society, threat countering**Abstract****Subject** This article discusses the specific risks posed by the emergence of new opportunities in the process of digital society formation.**Objectives** The article aims to develop certain proposals to counter threats and challenges emerging under the advent of digital technologies and comprehensive introduction of new ways of economic process organization.**Methods** For the study, we analyzed various incidents and situations occurred in cyberspace in recent years.**Results** The article shows the dynamics of development and the types of threats and risks generated by digital technologies. It describes the causes that led to threats and identifies trends in their development. Extrapolation of the identified trends for the coming years indicates the possibility of fundamentally new cyberthreats emergence.**Conclusions** Responding to emerging risks will require to create appropriate tools, the most important element of which is the availability of the Internet national segment.

© Publishing house FINANCE and CREDIT, 2019

**Please cite this article as:** Kilyachkov A.A., Chaldaeva L.A. Risk in Terms of Digital Society and the Development Trends. *Finance and Credit*, 2019, vol. 25, iss. 6, pp. 1444–1453.<https://doi.org/10.24891/fc.25.6.1444>**References**

1. Shevchenko I.V., Korobeinikova M.S. [Regulating the security of the Russian innovation and investment]. *Natsional'nye interesy: priority i bezopasnost' = National Interests: Priorities and Security*, 2018, vol. 14, iss. 9, pp. 1693–1730. (In Russ.)  
URL: <https://doi.org/10.24891/ni.14.9.1693>
2. Ustyuzhanina E.V., Sigarev A.V., Shein R.A. [Digital economy as a new paradigm of economic development]. *Natsional'nye interesy: priority i bezopasnost' = National Interests: Priorities and Security*, 2017, vol. 13, no. 10, pp. 1788–1804. (In Russ.)  
URL: <https://doi.org/10.24891/ni.13.10.1788>
3. Babanov V.N. [The factors and problems of development of the digital economy in Russia]. *Izvestiya Tul'skogo gosudarstvennogo universiteta. Ekonomicheskie i yuridicheskie nauki = News of Tula State University. Economic and Legal Sciences*, 2017, no. 4-1, pp. 255–262.  
URL: <https://cyberleninka.ru/article/n/factory-i-problemy-razvitiya-tsifrovoy-ekonomiki-v-rossii> (In Russ.)

4. Chakpitak N., Maneejuk P., Chanaim S., Sriboonchitta S. Thailand in the Era of Digital Economy: How Does Digital Technology Promote Economic Growth? Predictive Econometrics and Big Data: International Conference of the Thailand Econometrics Society. *Studies in Computational Intelligence Series*, 2018, pp. 350–362. URL: [https://doi.org/10.1007/978-3-319-70942-0\\_25](https://doi.org/10.1007/978-3-319-70942-0_25)
5. Martin-Shields C.P., Bodanac N. Peacekeeping's Digital Economy: The Role of Communication Technologies in Post-Conflict Economic Growth. *International Peacekeeping*, 2018, vol. 25, iss. 3, pp. 420–445. URL: <http://dx.doi.org/10.2139/ssrn.2970923>
6. Goldstein H. Editorial: The Digital Economy Act and Statistical Research. *Journal of the Royal Statistical Society. Series A: Statistics in Society*, 2017, vol. 180, iss. 4, pp. 945–946. URL: <https://doi.org/10.1111/rssa.12317>
7. Pilik M., Juříčková E., Kwarteng M.A. On-line Shopping Behaviour in the Czech Republic under the Digital Transformation of Economy. *Economic Annals-XXI*, 2017, vol. 165, iss. 5–6, pp. 119–123. URL: <https://doi.org/10.21003/ea.V165-24>
8. Tan K.H., Ji G., Lim C.P., Tseng M.-L. Using Big Data to Make Better Decisions in the Digital Economy. *International Journal of Production Research*, 2017, vol. 55, iss. 17, pp. 4998–5000. URL: <https://doi.org/10.1080/00207543.2017.1331051>
9. Milgrom P., Roberts J. The Economics of Modern Manufacturing: Technology, Strategy, and Organization. *The American Economic Review*, 1990, vol. 80, iss. 3, pp. 511–528. URL: [https://www.researchgate.net/publication/4901048\\_The\\_Economics\\_of\\_Modern\\_Manufacturing\\_Technology\\_Strategy\\_and\\_Organization](https://www.researchgate.net/publication/4901048_The_Economics_of_Modern_Manufacturing_Technology_Strategy_and_Organization)
10. Pan'shin B. [Digital economy: features and development trends]. *Nauka i innovatsii = Science and Innovations*, 2016, vol. 3, no. 157, pp. 17–20. URL: <http://innosfera.by/files/2016/3.pdf> (In Russ.)
11. Taleb N.N. *Chernyi lebed'. Pod znakom nepredskazuemosti* [The Black Swan: The Impact of the Highly Improbable]. Moscow, KoLibri Publ., 2016, 736 p.

### Conflict-of-interest notification

We, the authors 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.