

РИСКИ КИБЕРПРОСТРАНСТВА И ИХ ВЛИЯНИЕ НА ЭФФЕКТИВНОСТЬ ВЗАИМОДЕЙСТВИЯ ХОЗЯЙСТВУЮЩИХ СУБЪЕКТОВ

Лариса Алексеевна ЧАЛДАЕВА

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

История статьи:

Рег. № 516/2019
Получена 23.07.2019
Получена в доработанном
виде 10.08.2019
Одобрена 30.08.2019
Доступна онлайн
15.11.2019

УДК 004.056
JEL: L81, L86, M15

Ключевые слова:

риски и угрозы,
киберпространство,
цифровая экономика,
кибербезопасность,
киберпреступления

Аннотация

Тема. Статья посвящена рискам киберпространства, оказывающим влияние на результаты деятельности хозяйствующих субъектов, формирующих киберугрозы и провоцирующих необходимость разработки стратегии противодействия и отстаивания национальных интересов.

Цели. Выявление в ходе исследования проблем, связанных с освоением киберпространства и современным состоянием экономики страны. Рассмотрение возможности их решения на основе предложений, представленных в Доктрине информационной безопасности Российской Федерации. Формулирование предложений по снижению степени влияния рисков киберпространства на эффективность деятельности хозяйствующих субъектов.

Методология. Использованы методы системного анализа, сравнительного, структурного и логического анализа, контент-анализ СМИ.

Результаты. Выявлены проблемы освоения киберпространства, связанные с экономикой страны, рассмотрены возможности их решения с учетом предложений, представленных в Доктрине информационной безопасности Российской Федерации. Показано, что хозяйствующим субъектам, занятым различными видами экономической деятельности, следует разработать и внедрить программу кибербезопасности и защиты от различных видов посягательств от сторонних организаций и стран, а также предпринять меры по минимизации рисков.

Выводы. В настоящее время остается актуальным активное противодействие рискам и угрозам киберпространства, оказывающим влияние на результаты деятельности хозяйствующих субъектов. Для оперативного реагирования на указанные риски киберпространства и их минимизации следует, в частности: эффективно и постоянно сотрудничать с государственными органами управления и компаниями по программе кибербезопасности и противодействия угрозам в киберпространстве; организовать диверсификацию валютных транзакций, осуществляя их не только в долларах США, но и в валюте других стран; использовать в расчетах различные международные и национальные платежные системы; ориентировать клиентов на использование конкурентных отечественных разработок и изобретений при предоставлении коммерческих кредитов; обеспечить оплату работ, выполненных специалистами коммерческих банков по кибербезопасности в соответствии с существующими принципами организации оплаты труда.

© Издательский дом ФИНАНСЫ и КРЕДИТ, 2019

Для цитирования: Чалдаева Л.А. Риски киберпространства и их влияние на эффективность взаимодействия хозяйствующих субъектов // *Национальные интересы: приоритеты и безопасность*. – 2019. – Т. 15, № 11. – С. 2029 – 2041.
<https://doi.org/10.24891/ni.15.11.2029>

В январе 2019 г. в Давосе прошла ежегодная площадкой, где обсуждаются основные сессия Всемирного экономического форума тенденции и перспективы глобальной (ВЭФ), который является главной мировой экономики и бизнеса. В преддверии форума

ВЭФ опубликовал последнее издание своего доклада о глобальных рисках¹, характеризуя представление о том, какие задачи являются первоочередными в глобальной экономике и геополитике. В частности, в числе пяти глобальных рисков с точки зрения вероятности их реализации были названы кибератаки, мошенничество или хищение информации. Отмечено, что по мере того, как влияние технологий проникает в повседневную жизнь, кибератаки и уязвимые протоколы кибербезопасности становятся все более серьезными проблемами. Причем реализация стратегий борьбы с киберугрозами отстает от жизни: она, увы, скорее реагирующая, чем превентивная.

Так, яростная атака Ransomware 2017 г. показала, что она быстро стала одной из самых опасных угроз кибербезопасности. Атака WannaCry Ransomware началась весной 2017 г. и затронула более 300 тыс. компьютеров в более чем 150 странах. Эксперты Cybersecurity Ventures отметили, что общая стоимость ущерба от выкупа за 2017 г. составляет более 5 млрд долл. США. И это в 15 раз больше, чем 325 млн долл. США в результате ущерба, нанесенного в 2015 г. В качестве одного из ярких примеров хищения информации можно привести и многочисленные нарушения государственной идентификационной базы данных в Индии, которые привели к разглашению персональной информации более одного млрд зарегистрированных граждан. Причем в 2019 г., по оценкам экспертов ВЭФ, следует ожидать еще активации риска кражи данных компании, либо денег (82%), нарушение функционирования компании или ее инфраструктуры (80%), увеличения риска кражи личных данных (64%)². Таким образом, подтверждается особая актуальность темы кибербезопасности в настоящий период.

¹ Топ-5 глобальных рисков в 2019 г. по мнению Всемирного экономического форума. URL: <https://bcs-express.ru/novosti-i-analitika/top-5-global-nykh-riskov-v-2019-godu-po-mneniiu-vsemirnogo-ekonomicheskogo-foruma>

² Там же.

Тема исследования широко представлена в научной и специальной литературе. Иностранные авторы в своих работах ставят на первый план исследование возникающих злободневных проблем и поиск возможных практических рекомендаций³ [1–6]. Активно ведут анализ причин возникновения киберугроз и выработку рекомендаций по их нейтрализации отечественные исследователи [7–10]. Так, В.М. Матюшок и В.А. Красавина ставят в своей работе проблему широко – как ситуация на мировом рынке новейших ИТ-технологий затрагивает национальные интересы России. Л.В. Юрьева, М.В. Тумбинская и Л.Ю. Овсяницкая рассматривают вопросы безопасности конкретно – в приложении к металлургическим холдингам и предприятиям [11–13]. Совершенно справедливо поднимает проблему М.Н. Власенко – с точки зрения обеспеченности компаний персоналом: и сегодня кадры специалистов решают успех дела, то есть остро нужны профессионалы в области кибербезопасности [14]. Наконец, вопросы кибербезопасности актуальны еще и по той причине, что уже долгие годы не утихают информационные войны [15]. Нельзя не учитывать и того очевидного факта, что киберпространство активно освоили и продолжают использовать международные криминальные структуры и организованная преступность [16].

Также следует отметить и то, что в современном киберпространстве взаимодействие хозяйствующих субъектов осложняется не только указанными проблемами и рисками цифрового характера, но и принципиально новыми угрозами, которые сопровождают и влияют на результативность данного процесса. Суть вопроса состоит в том, что глобализация в стадии формирования цифрового общества содействовала появлению и развитию специфических угроз в киберпространстве, что, в свою очередь, вызвало необходимость

³ Semenova K.D., Tarasova K.I. Statistical Research of Global Cyber-Risks: The Cost of Cyber-Crime. Topical Questions of Contemporary Science: Collection of scientific articles. 2017, pp. 315–320.

разработки и внедрения приемов и методов кибербезопасности⁴.

Основной причиной появления киберугроз является неизбежное столкновение коренных интересов различных стран в киберпространстве. Естественно, проблема заключается в создании доверия и безопасности при использовании информационных и коммуникационных технологий. Фундаментальная роль здесь принадлежит Международному союзу электросвязи (ведущее агентство Организации Объединенных Наций по вопросам информационных и коммуникационных технологий). Точкой отсчета в борьбе с киберугрозами принято считать Всемирную встречу на высшем уровне по вопросам информационного общества и Полномочную конференцию МСЭ в 2006 г.⁵. Именно там решено было предпринять конкретные шаги к сдерживанию угроз и опасностей, связанных с информационным обществом. Так, в 2007 г. объявлено о начале Глобальной программы кибербезопасности (ГКП) как основы международного сотрудничества. Цель ГКП – повысить доверие и безопасность в информационном обществе. Она разрабатывается для взаимодействия и эффективного стимулирования сотрудничества между всеми заинтересованными сторонами и строится на пяти стратегических принципах (рис. 1). ГКП – это первый действительно глобально многосторонний альянс частного и государственного секторов против киберугроз. В 2008 г. МСЭ и Международное многостороннее партнерство против киберугроз (ИМРАСТ) официально подписали Меморандум о взаимопонимании. В результате налаженного взаимодействия

странам-участникам предоставляются опыт, оборудование и ресурсы для эффективного увеличения возможностей глобального сообщества по предотвращению, защите и противодействию киберугрозам. С самого своего начала ГКП получила поддержку и признание лидеров и экспертов в области кибербезопасности всего мира.

Для того чтобы снизить риски в области кибербезопасности и исключить возможные угрозы, в разных странах были разработаны и приняты документы, формулирующие правила, в соответствии с которыми государствам предоставляется возможность взаимодействовать друг с другом в киберпространстве. К числу таких документов относится и Стратегия национальной кибербезопасности Соединенных Штатов Америки⁶ (далее – Стратегия), которая была принята высшим органом управления страны в сентябре 2018 г. Целевая направленность данного документа сводится к укреплению доминирующего положения страны в киберпространстве в настоящем и будущем, поскольку ее основными конкурентными противниками являются Россия, Иран и Северная Корея, а также Китай, который достаточно своеобразно использует возможности киберпространства в свою пользу.

Однако кроме этого, террористические группировки также используют киберпространство для популяризации своих идей и агитации присоединения к ним в целях завоевания лидирующих позиций в мировом пространстве и в частности США.

Кроме этих мер для поддержания своего статуса в киберпространстве и обеспечения экономической безопасности Соединенные Штаты Америки намерены воспользоваться всеми возможными приемами, как-то – информационными, финансовыми, дипломатическими и иными способами вплоть до применения силы. К тому же

⁴ Доктрина информационной безопасности Российской Федерации: утв. Указом Президента РФ от 05.12.2016 № 646; О Стратегии развития информационного общества в Российской Федерации на 2017–2030 гг.: Указ Президента РФ от 09.05.2017 № 203; Об утверждении программы «Цифровая экономика Российской Федерации»: расп. Правительства РФ от 28.07.2017 № 1632-р; Независимый экспертный доклад «Модернизация экономики как построение нового государства». URL: <http://apn.ru/publications/article22100.htm>

⁵ Глобальная программа кибербезопасности МСЭ. URL: <http://psihdocs.ru/mejdunarodnij-soyuz-elektrosvyazi-v-poiskah-kibernira.html?page=18>

⁶ Стратегия национальной кибербезопасности Соединенных Штатов Америки. URL: http://d-russia.ru/wp-content/uploads/2019/01/National-Cyber-Strategy_USA_2018.pdf

разведывательные службы США, вероятнее всего, сохранят преимущественные позиции по использованию цифровых данных в целях выявления действий, угрожающих национальным интересам государства, а страна проявит активность в обеспечении интернет-связи для продвижения своего влияния и продолжит совместную работу с представителями гражданского общества различных стран по защите прав индивидуума и свободы слова в интернет-пространстве.

Иными словами, США декларируют таким образом явное намерение и в дальнейшем использовать возможности Интернета для совершения «цветных» революций и защиты собственных интересов.

Для достижения поставленных целей Соединенные Штаты Америки проектируют и последовательно реализуют проекты привлечения к уголовной ответственности лиц, находящихся за рубежом и совершивших в свое время киберпреступления против этой страны, а далее, безусловно, придавая этим мерам экстерриториальный характер, требуют от иностранных правоохранительных органов наличия технических возможностей для эффективного оказания помощи правоохранительным органам по их первому требованию.

Кроме того, Соединенные Штаты Америки и их соответствующие органы планируют разработать программу привлечения иностранных специалистов по кибербезопасности. В этих целях администрация намерена провести своеобразную «иммиграционную» реформу, а также предоставить образовательные и карьерные возможности для закрепления перспективных специалистов в области кибербезопасности в своей стране.

В то же время правительство США не намерено «предоставлять» странам-противникам преимуществ в использовании результатов исследований и разработок американских ученых и практиков.

Также необходимо отметить и то, что в Стратегии утверждается: принципы «свободы» Интернета неразрывно связаны с национальной безопасностью Соединенных Штатов Америки, а поэтому для продвижения государственного влияния и реализации собственных интересов страна намерена целенаправленно обеспечивать открытость, совместимость, безопасность и надежность Интернета, что предоставит американским компаниям высокие конкурентные преимущества.

Далее развитие событий направлено на «завоевание» зарубежных рынков американскими разработками и технологиями, что может оказать решающее значение на поддержку американского влияния в целях противодействия глобальным конкурентам.

Анализируя основные положения Стратегии национальной кибербезопасности Соединенных Штатов Америки, можно выявить и другие факторы, которые способствуют возникновению принципиально новых угроз для хозяйствующих субъектов зарубежных стран, среди которых следует выделить следующие:

- 1) правительство Соединенных Штатов Америки окажет решительное сопротивление получению странами-противниками преимуществ за счет использования результатов американских исследований и разработок;
- 2) для поддержания американского влияния и в целях противодействия глобальным конкурентам правительство Соединенных Штатов Америки намерено насыщать зарубежные рынки американскими разработками и технологиями;
- 3) правительство Соединенных Штатов Америки также «планирует» привлекать ценных специалистов в области кибербезопасности, используя все возможные средства.

Таким образом, результат анализа Стратегии национальной кибербезопасности

Соединенных Штатов Америки позволяет выявить факторы, провоцирующие появление ряда рисков, которые естественным образом могут трансформироваться в риски сотрудничающих с ними хозяйствующих субъектов и организаций.

1. Риск санкционного давления. Если хозяйствующий субъект использует в своей деятельности американские разработки и при этом получает преимущество над американскими компаниями, то против него возможно применение различных санкций. При этом, как показывает опыт последних лет, наряду с первичными санкциями против какого-либо хозяйствующего субъекта возможны вторичные санкции против партнеров данного субъекта. Причем очевидной цели вторичных санкций подвержены те организации, которые обслуживают финансовые потоки компаний, попавших под первичные санкции. Принимая во внимание то обстоятельство, что практически все хозяйствующие субъекты используют вычислительное и телекоммуникационное оборудование, а также программное обеспечение, например, операционную систему Windows, основанную на применении американских технологий, то данному риску подвержены практически все хозяйствующие субъекты. При этом, например, коммерческий банк может оказаться перед выбором: следовать санкционным требованиям и занять позицию, противоречащую интересам своей страны, или защитить национальные интересы и быть при этом подвергнутым вторичным санкциям⁷.

2. Риск коммерческого шпионажа. Насыщение американскими разработками и технологиями зарубежных рынков с учетом того, что разведывательное сообщество Соединенных Штатов Америки имеет право использовать все цифровые данные, полученные из любых источников, повышает вероятность появления так называемых

«закладок». «Закладки» – это аппаратные элементы устройства или фрагменты программного обеспечения, необходимого для его функционирования, которые позволяют осуществлять несанкционированный доступ к информации, содержащейся в устройстве. В связи с этим обращает на себя внимание сообщение WikiLeaks⁸ о том, что в ЦРУ разработаны программные закладки на «зараженных» компьютерах с операционной системой Windows, которые обеспечивают возможности для осуществления отслеживания и запуска вредоносных приложений, а также хранения используемых драйверов и программных закладок. В результате коммерческая информация, принадлежащая хозяйствующим субъектам, станет в полном объеме доступной информационной разведке США, а значит, и конкурирующим американским компаниям, и финансовым институтам.

3. Риск «вербовки» специалистов по кибербезопасности. Почти 2/3, например, российских онлайн-банков уязвимы для хищения денег хакерами⁹. Основной причиной этого является недостаточно высокий уровень квалификации разработчиков программного обеспечения, которые не проводят всестороннего тестирования программного обеспечения. Таким образом, дефицит квалифицированных кадров по кибербезопасности уже является актуальным для российских хозяйствующих субъектов, а при наличии высококонкурентных предложений со стороны Соединенных Штатов Америки, он может стать еще более критичным не только для хозяйствующих субъектов и финансовых учреждений, но и для безопасности страны в целом.

4. Риск экстрадиции в Соединенные Штаты Америки специалистов и руководителей, что позволяет правительству этой страны

⁸ WikiLeaks опубликовал новый пакет секретных документов ЦРУ о кибершпионаже.
URL: <https://ria.ru/20170831/1501474835.html>

⁹ Горячева В. Хакеры начали издавать. Эксперты назвали главные уязвимости онлайн-банков.
URL: <https://kommersant.ru/doc/3933113>

⁷ Елагин М. Следователи проверяют российские банки за отказ работать в Крыму.
URL: https://tsargrad.tv/articles/sledovатели-proverjat-vtb-i-drugie-rossijskie-banki-za-otkaz-rabotat-v-krymu_137431

инициировать экстрадиции «интересующего» его объекта, начиная от специалиста и до руководителя компании. Примером реализации данного риска-угрозы является задержание в Канаде финансового директора компании Huawei Technologies Мэн Ванчжоу за то, что китайская компания не соблюдает антииранских санкций, введенных Вашингтоном¹⁰. Задержание произошло по запросу Соединенных Штатов Америки, где директор компании предстанет перед судом.

В перспективе следует ожидать увеличения количества запросов министерства юстиции Соединенных Штатов Америки на арест и экстрадицию специалистов и руководителей различных компаний из разных стран. Причем и коммерческие банки не застрахованы от подобного развития событий. В частности, ведущим специалистам по кибербезопасности могут быть предъявлены вымышленные обвинения, а после экстрадиции в Соединенные Штаты Америки их, возможно, попытаются склонить к сделке со следствием заманчивым предложением остаться в стране на привлекательных условиях.

Однако следует отметить, что защищать национальные интересы и интересы отечественных компаний в виртуальном пространстве от кибернападения субъектов другого государства должны в первую очередь соответствующие государственные органы, службы и управления. Высшее руководство Российской Федерации осознает возникшую угрозу. Доказательством тому являются принципы и правила, которыми руководствуются органы государственной власти и управления Российской Федерацией в области защиты национальных интересов в киберпространстве и которые нашли свое отражение в Доктрине информационной безопасности Российской Федерации (далее – Доктрина), утвержденной еще в декабре 2016 г.¹¹.

¹⁰ Герасюкова М. Ответит за Иран: в Америке арестовали директора Huawei.

URL: https://gazeta.ru/tech/2018/12/06/12084979/cfo_arrested.shtml

¹¹ Доктрина информационной безопасности Российской Федерации: утв. Указом Президента РФ от 05.12.2016 № 646. URL: <http://base.garant.ru/71556224/>

Хотя Доктрина информационной безопасности Российской Федерации и заявила о себе ранее, чем Стратегия национальной кибербезопасности Соединенных Штатов Америки, тем не менее, она содержит адекватное понимание возможностей Российской Федерации в вопросах противодействия угрозам в информационном пространстве со стороны других государств, а также тех мер, которые необходимо предпринять для защиты жизненно важных интересов личности, общества и государства в целом.

Однако в Доктрине не учтены риски, порожденные самой Стратегией и касающиеся человеческого фактора. Это прежде всего риск привлечения иностранных специалистов по кибербезопасности и риск экстрадиции специалистов и руководителей. Как свидетельствует результат апрельских событий 2019 г.¹², защита российских граждан институтами государственной власти России от экстерриториальных претензий со стороны Соединенных Штатов Америки носит проблематичный характер.

С другой стороны, целесообразно обратиться к изучению полезного опыта тех компаний, которые успешно решают проблемы кибербезопасности и управления возникающими рисками. Так, Сбербанк России планирует войти в число мировых лидеров по управлению рисками кибербезопасности¹³. Известно, что на сегодняшний день Сбербанк лидирует в данной области по стране с большим отрывом. Подтверждение тому – независимая международная оценка.

На основе проведенного анализа можно прийти к следующим выводам. Хозяйствующим субъектам, занятым

¹² Греческий суд объявил о перерыве по делу россиянина Винника.

URL: https://gazeta.ru/social/news/2019/04/05/n_12832303.shtml

¹³ Греф рассказал о планах Сбербанка войти в топ-5 мировых лидеров по управлению рисками кибербезопасности. URL: <https://rns.online/finance/Gref-rasskazal-o-planah-Sberbanka-voiti-v-top-5--mirovih-liderov-po-upravleniyu-riskami-kiberbezopasnosti--2017-04-20/>

различными видами экономической деятельности, следует разработать и внедрить программу кибербезопасности и защиты от различных видов посягательств от сторонних организаций и стран, а также предпринять комплексные меры по минимизации рисков, а именно:

- 1) эффективно и на постоянно действующей основе следует сотрудничать с государственными органами управления и компаниями по программе кибербезопасности и противодействия угрозам в киберпространстве. Необходимость таких мер более всего соответствует требованиям Доктрины, в которой одними из участников системы информационной безопасности являются «организации денежно-кредитной, валютной, банковской и иных сфер финансового рынка»¹⁴;
- 2) организовать диверсификацию валютных транзакций, осуществляя их не только

в долларах США, но и в валюте других стран;

- 3) использовать в расчетах различные международные и национальные платежные системы;
- 4) ориентировать своих клиентов на использование конкурентных отечественных разработок и изобретений при предоставлении коммерческих кредитов;
- 5) обеспечить оплату выполненных работ специалистами коммерческих банков по кибербезопасности в соответствии с существующими принципами организации оплаты труда;
- 6) при выезде за границу – как в деловые поездки, так и в других целях необходимо реально оценивать риски предъявления экстерриториальных претензий со стороны министерства юстиции Соединенных Штатов Америки.

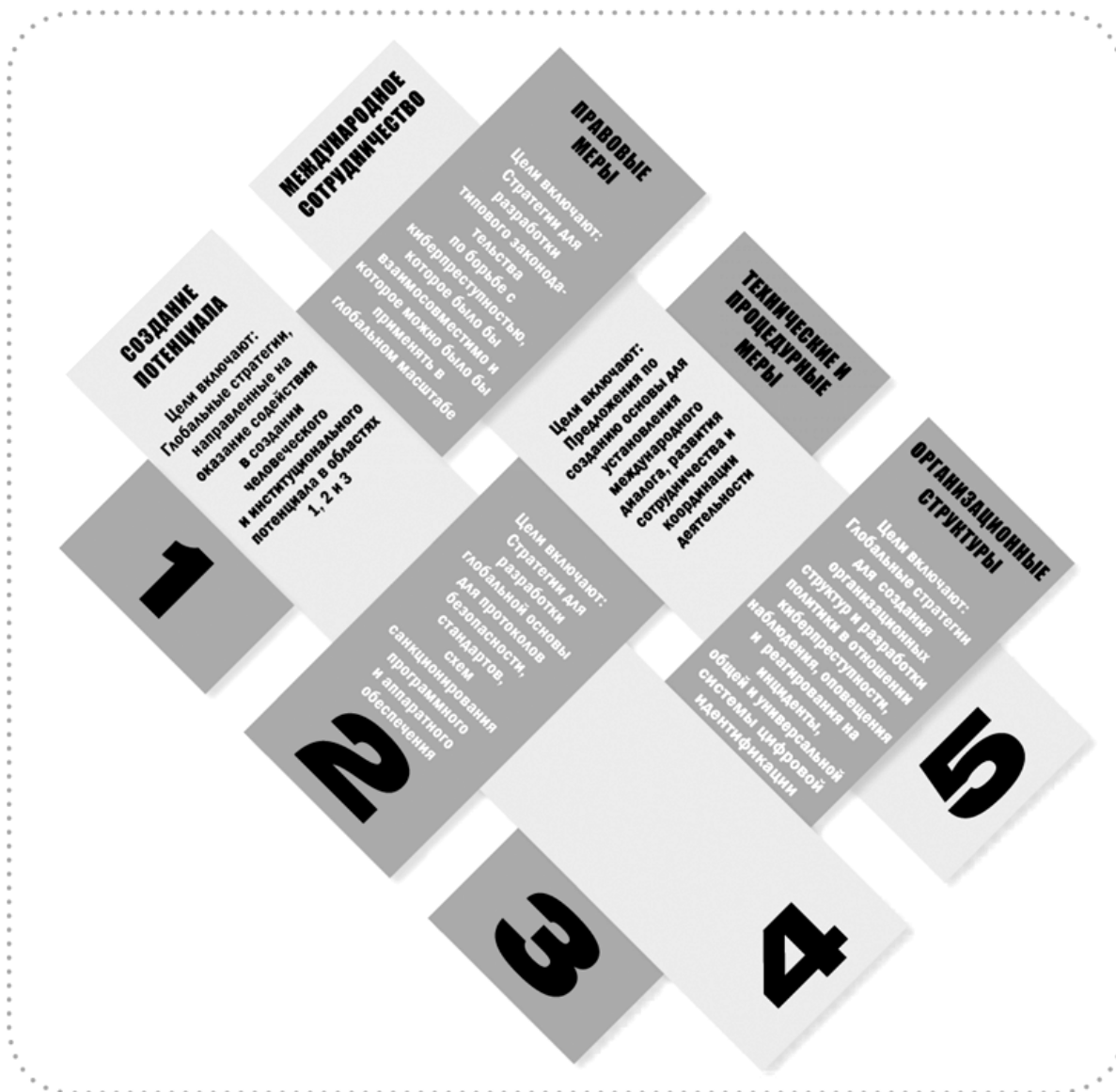
¹⁴ Доктрина информационной безопасности Российской Федерации (разд. V, п. 33): утв. Указом Президента РФ от 05.12.2016 № 646. URL: <http://base.garant.ru/71556224/>

Рисунок 1

Глобальная программа кибербезопасности: пять стратегических принципов

Figure 1

Global Cybersecurity Agenda: The Five Strategic Principles



Источник: Глобальная программа кибербезопасности МСЭ.

URL: <http://psihdocs.ru/mejdunarodnij-soyuz-elektrosvyazi-v-poiskah-kibermira.html?page=18>

Source: ITU Global Cybersecurity Program.

URL: <http://psihdocs.ru/mejdunarodnij-soyuz-elektrosvyazi-v-poiskah-kibermira.html?page=18> (In Russ.)

Список литературы

1. Alosaimi R., Alnuem M. Risk Management Frameworks for Cloud Computing: A Critical Review. *International Journal of Computer Science & Information Technology*, 2016, vol. 8, iss. 4. URL: <https://doi.org/10.5121/ijcsit.2016.8401>
2. Green I.S. *Cyber Security: An Introduction for Non-Technical Managers*. Routledge, 2015, 264 p.
3. LeClair J., Keeley G. *Cybersecurity in Our Digital Lives*. Hudson Whitman/Excelsior College Press, 2015, 262 p.
4. Dalziel H. *Introduction to US Cybersecurity Careers*. Syngress, 2014, 68 p.
5. Митник К. Искусство обмана. М.: Компания АйТи, 2004. 40 с.
6. Саймон В.Л., Митник К.Д. Искусство вторжения. М.: ДМК-Пресс, Компания АйТи, 2005. 138 с.
7. Хрусталёв Е.Ю., Костюрин Г.А. Киберугрозы: причины возникновения и рекомендации по предупреждению // *Национальные интересы: приоритеты и безопасность*. 2019. Т. 15. Вып. 6. С. 1185–1194. URL: <https://doi.org/10.24891/ni.15.6.1185>
8. Матюшок В.М., Красавина В.А. Мировой рынок новейших ИТ-технологий и национальные интересы // *Национальные интересы: приоритеты и безопасность*. 2017. Т. 13. Вып. 11. С. 1988–2004. URL: <https://doi.org/10.24891/ni.13.11.1988>
9. Ревенков П.В., Бердюгин А.А. Кибербезопасность в условиях Интернета вещей и электронного банкинга // *Национальные интересы: приоритеты и безопасность*. 2016. Т. 12. Вып. 11. С. 158–169. URL: <https://cyberleninka.ru/article/v/kiberbezopasnost-v-usloviyah-interneta-veschey-i-elektronnogo-bankinga>
10. Кудряшова Е.В. Проблемы техники налогового стимулирования обеспечения кибербезопасности для малого и среднего бизнеса // *Финансы и кредит*. 2019. Т. 25. Вып. 3. С. 609–617. URL: <https://doi.org/10.24891/fc.25.3.609>
11. Юрьева Л.В. Особенности и проблемы системы информационной безопасности в металлургических холдингах // *Национальные интересы: приоритеты и безопасность*. 2008. Т. 4. Вып. 10. С. 74–80. URL: <https://cyberleninka.ru/article/v/osobennosti-i-problemy-sistemy-informatsionnoy-bezopasnosti-v-metallurgicheskikh-holdingah>
12. Тумбинская М.В. Организационное обеспечение процесса управления ИТ-инфраструктурой в системе защиты информации на предприятии // *Национальные интересы: приоритеты и безопасность*. 2015. Т. 11. Вып. 1. С. 31–41. URL: <https://cyberleninka.ru/article/v/organizatsionnoe-obespechenie-protssessa-upravleniya-it-infrastrukturoy-v-sisteme-zaschity-informatsii-na-predpriyatii>
13. Овсянницкая Л.Ю. Актуальные вопросы защиты информации (на примере промышленных предприятий и учреждений здравоохранения г. Челябинска) // *Национальные интересы: приоритеты и безопасность*. 2013. Т. 9. Вып. 21. С. 54–60. URL: <https://cyberleninka.ru/article/v/aktualnye-voprosy-zaschity-informatsii-na-primere-promyshlennyh-predpriyatij-i-uchrezhdeniy-zdravoohraneniya-g-chelyabinska>

14. *Власенко М.Н.* Организационные аспекты и проблемы кадрового обеспечения хозяйствующих субъектов специалистами сферы информационной безопасности в современных условиях рыночной экономики России // *Национальные интересы: приоритеты и безопасность*. 2011. Т. 7. Вып. 24. С. 64–71.
URL: <https://cyberleninka.ru/article/v/organizatsionnye-aspekty-i-problemy-kadrovogo-obespecheniya-hozyaystvuyuschih-subektov-spetsialistami-sfery-informatsionnoy>
15. *Крошилин С.В.* Информационные войны на микро- и макроуровне и их влияние на экономическую безопасность // *Национальные интересы: приоритеты и безопасность*. 2011. Т. 7. Вып. 7. С. 46–51. URL: <https://cyberleninka.ru/article/v/informatsionnye-voyny-na-mikro-i-makrourovne-i-ih-vliyanie-na-ekonomicheskuyu-bezopasnost>
16. *Глотина И.М.* Киберпреступность как теневой бизнес // *Вестник Челябинского государственного университета*. 2016. № 6. С. 51–57.
URL: <https://cyberleninka.ru/article/v/kiberprestupnost-kak-tenevoy-biznes>

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.

CYBERSPACE RISKS AND THEIR IMPACT ON THE EFFICIENCY OF THE INTERACTION OF ECONOMIC AGENTS

Larisa A. CHALDAEVA

Financial University under Government of Russia, Moscow, Russian Federation
Chaldaeava45@mail.ru
<https://orcid.org/0000-0001-6203-4968>

Article history:

Received 23 July 2019
Received in revised form
10 August 2019
Accepted 30 August 2019
Available online
15 November 2019

JEL classification: L81, L86,
M15

Keywords: risk, threat,
cyberspace, digital economy,
cybersecurity, cybercrime

Abstract

Subject The article discusses cyberspace risks that influence the performance of economic agents and engender cyberthreats and urge to articulate strategies for countering them and protecting national interests.

Objectives The study is to identify what difficulties arise from the cyberspace and current economic situation in the country. I review whether such issues can be solved through proposals set out in the Doctrine of Information Security of the Russian Federation. The article formulates my ideas for reducing the extent to which cyberspace risks influence the performance of economic agents.

Methods The study is based on methods of a systems analysis, comparative, structural and logic analysis, content analysis of mass media.

Results I discovered what impedes the cyberspace exploration concerning the national economy and reviewed if such issues can be resolved in accordance with the Doctrine of Information Security of the Russian Federation. Economic agents are showed to lack a cybersecurity program, protect various types of activities from third parties and countries, and undertake risk mitigation measures.

Conclusions and Relevance Currently, it is still important to actively counteract cyberspace risks and threats, which affect business performance. To promptly respond to such cyberspace risks, businesses should cooperate effectively and constantly with governmental authorities and businesses under the auspices of the cybersecurity program, diversify foreign exchange transactions and use other currencies, other than USD, use various international and national payment systems, persuade customers to enjoy competitive domestic products and inventions as part of wholesale lending practices, pay for work done by cybersecurity teams of commercial banks in accordance with the existing remuneration principles.

© Publishing house FINANCE and CREDIT, 2019

Please cite this article as: Chaldaeava L.A. Cyberspace Risks and Their Impact on the Efficiency of the Interaction of Economic Agents. *National Interests: Priorities and Security*, 2019, vol. 15, iss. 11, pp. 2029–2041.
<https://doi.org/10.24891/ni.15.11.2029>

References

1. Alosaimi R., Alnuem M. Risk Management Frameworks for Cloud Computing: A Critical Review. *International Journal of Computer Science & Information Technology*, 2016, vol. 8, iss. 4.
URL: <https://doi.org/10.5121/ijcsit.2016.8401>
2. Green I.S. *Cyber Security: An Introduction for Non-Technical Managers*. Routledge, 2015, 264 p.
3. LeClair J., Keeley G. *Cybersecurity in Our Digital Lives*. Hudson Whitman/Excelsior College Press, 2015, 262 p.
4. Dalziel H. *Introduction to US Cybersecurity Careers*. Syngress, 2014, 68 p.
5. Mitnick K. *Iskusstvo obmana* [The Art of Deception]. Moscow, IT Co Publ., 2004, p. 40.

6. Simon W.L., Mitnick K.D. *Iskusstvo vtorzheniya* [The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers]. Moscow, DMK-Press, IT Co Publ., 2005, 138 p.
7. Khrustalev E.Yu., Kostyurin G.A. [Cybersecurity threats: Triggers and prevention recommendations]. *Natsional'nye interesy: priority i bezopasnost' = National Interests: Priorities and Security*, 2019, vol. 15, iss. 6, pp. 1185–1194. (In Russ.)
URL: <https://doi.org/10.24891/ni.15.6.1185>
8. Matyushok V.M., Krasavina V.A. [Global market of brand new information technology and the national interests]. *Natsional'nye interesy: priority i bezopasnost' = National Interests: Priorities and Security*, 2017, vol. 13, iss. 11, pp. 1988–2004. (In Russ.)
URL: <https://doi.org/10.24891/ni.13.11.1988>
9. Revenkov P.V., Berdyugin A.A. [Cybersecurity in the conditions of the Internet of Things and e-banking]. *Natsional'nye interesy: priority i bezopasnost' = National Interests: Priorities and Security*, 2016, vol. 12, iss. 11, pp. 158–169.
URL: <https://cyberleninka.ru/article/v/kiberbezopasnost-v-usloviyah-interneta-veschey-i-elektronnogo-bankinga> (In Russ.)
10. Kudryashova E.V. [Challenges of tax incentives for cybersecurity in small and medium-sized businesses]. *Finansy i kredit = Finance and Credit*, 2019, vol. 25, iss. 3, pp. 609–617. (In Russ.)
URL: <https://doi.org/10.24891/fc.25.3.609>
11. Yur'eva L.V. [Specifics and challenges of the information security system in metallurgical holding groups]. *Natsional'nye interesy: priority i bezopasnost' = National Interests: Priorities and Security*, 2008, vol. 4, iss. 10, pp. 74–80. URL: <https://cyberleninka.ru/article/v/osobennosti-i-problemy-sistemy-informatsionnoy-bezopasnosti-v-metallurgicheskikh-holdingah> (In Russ.)
12. Tumbinskaya M.V. [Organizational support to IT infrastructure management in the information security system of an enterprise]. *Natsional'nye interesy: priority i bezopasnost' = National Interests: Priorities and Security*, 2015, vol. 11, iss. 1, pp. 31–41.
URL: <https://cyberleninka.ru/article/v/organizatsionnoe-obespechenie-protssessa-upravleniya-it-infrastrukturoy-v-sisteme-zaschity-informatsii-na-predpriyatii> (In Russ.)
13. Ovsyanitskaya L.Yu. [Actual issues of information security (for example, industrial enterprises and healthcare institutions in Chelyabinsk)]. *Natsional'nye interesy: priority i bezopasnost' = National Interests: Priorities and Security*, 2013, vol. 9, iss. 21, pp. 54–60.
URL: <https://cyberleninka.ru/article/v/aktualnye-voprosy-zaschity-informatsii-na-primere-promyshlennykh-predpriyatiy-i-uchrezhdeniy-zdravoohraneniya-g-chelyabinska> (In Russ.)
14. Vlasenko M.N. [Organizational aspects and problems of personnel maintenance of managing subjects experts of sphere of information security in modern conditions of market economy of Russia]. *Natsional'nye interesy: priority i bezopasnost' = National Interests: Priorities and Security*, 2011, vol. 7, iss. 24, pp. 64–71. URL: <https://cyberleninka.ru/article/v/organizatsionnye-aspekty-i-problemy-kadrovogo-obespecheniya-hozyaystvuyuschih-subektov-spetsialistami-sfery-informatsionnoy> (In Russ.)
15. Kroshilin S.V. [Micro- and macromedia wars and their influence on the economic security]. *Natsional'nye interesy: priority i bezopasnost' = National Interests: Priorities and Security*, 2011, vol. 7, iss. 7, pp. 46–51. URL: <https://cyberleninka.ru/article/v/informatsionnye-voyny-na-mikro-i-makrourovne-i-ih-vliyanie-na-ekonomicheskuyu-bezopasnost> (In Russ.)

16. Glotina I.M. [Cybercrime as a shadow business]. *Vestnik Chelyabinskogo gosudarstvennogo universiteta* = *Bulletin of Chelyabinsk State University*, 2016, no. 6, pp. 51–57.

URL: <https://cyberleninka.ru/article/v/kiberprestupnost-kak-tenevoy-biznes> (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.