DOI 10.22394/1726-1139-2023-7-28-41

Цифровизация и киберриски

Халин В. Г., Чернова Г. В.*

Санкт-Петербургский государственный университет, Санкт-Петербург, Российская Федерация; *v.halin@spbu.ru

РЕФЕРАТ

Цифровизация, рассматриваемая в широком смысле как современная важнейшая тенденция общественного развития, в общем случае сопровождается не только положительными последствиями для экономики и общества, но и вызовами, угрозами, а также отрицательными последствиями реализации этих угроз. Цифровизация, рассматриваемая в узком смысле как трансформация информации любого вида в ее цифровую форму и предполагающая использование цифровой информации, также может описываться вызовами, угрозами, отрицательными последствиями и рисками. Среди последних существенную роль играют риски нарушения безопасности цифровой информации — киберриски. Так как они могут оказывать негативное влияние на цифровизацию, рассматриваемую как в широком, так и в узком смысле, возникает проблема выделения киберрисков и управления ими в целях снижения возможных потерь и ущерба, обусловленных реализацией этих киберрисков. В статье определены взаимосвязи понятий цифровизация, вызов, угроза, отрицательное последствие и риск; выявлена роль и обоснована высокая значимость кибервызова как требования по обеспечению безопасности цифровой информации; определены факторы влияния на киберриски; предложен вариант построения программы управления киберрисками, реализация которой будет способствовать снижению возможных отрицательных последствий цифровизации, обусловленных нарушением безопасности цифровой информации.

Ключевые слова: цифровизация в широком смысле, цифровизация в узком смысле, вызов, угроза, отрицательное последствие, риск, информационная безопасность, кибервызов, киберугроза, киберриск, управление киберрисками

Для цитирования: *Халин В. Г., Чернова Г. В.* Цифровизация и киберриски // Управленческое консультирование. 2023. № 7. С. 28–41.

Digitalization and Cyber Risks

Vladimir G. Khalin, Galina V. Chernova*

Saint Petersburg State University, Saint Petersburg, Russian Federation; *v.halin@spbu.ru

ABSTRACT

Digitalization, considered in a broad sense as the most important modern trend of social development, is generally accompanied not only by positive consequences for the economy and society, but also by challenges, threats, as well as negative consequences of the implementation of these threats. Digitalization, considered in a narrow sense as the transformation of information of any kind into its digital form and involving the use of digital information, can also be described by challenges, threats, negative consequences and risks. Among the latter, a significant role is played by the risks of violating the security of digital information — cyber risks. Since they can have a negative impact on digitalization, considered both in a broad and narrow sense, there is a problem of allocating cyber risks and managing them in order to reduce possible losses and damage caused by the implementation of these cyber risks. The article defines the interrelationships of the concepts of digitalization, challenge, threat, negative consequence and risk; identifies the role and justifies the high importance of a cyber call as a requirement to ensure the security of digital information; determines the factors of influence on cyber risks; suggests a variant of building a cyber risk management program, the implementation of which will contribute to reducing the possible negative consequences of digitalization caused by a violation of the security of digital information.

Keywords: digitalization in the broad sense, digitalization in the narrow sense, challenge, threat, negative consequence, risk, information security, cyber challenge, cyber threat, cyber risk, cyber risk management.

For citing: Khalin V. G., Chernova G. V. Digitalization and Cyber Risks // Administrative consulting. 2023. N 7. P. 28–41.

Введение

Как показывает анализ, в настоящее время термин «цифровизация» используется в двух смыслах — узком и широком. Под цифровизацией в узком смысле обычно понимают процесс трансформации любой информации в цифровую форму ее представления. Данное определение делает акцент именно на переводе информации из одной формы ее представления в другую и тех возможностях, которые дает ее цифровое представление.

Однако более точным, по мнению авторов, является понимание цифровизации в узком смысле. Цифровизация в узком смысле есть процесс преобразования и использования информации, включающий только определенные или все из следующих этапов: трансформация информации, представленной в любой форме, в цифровую (в цифру); использование цифровой информации; трансформация цифровой информации в любую другую форму.

Повышенный интерес к цифровой форме представления информации объясняется следующими ее преимуществами. Она предполагает возможности применения разных физических принципов представления, запоминания и передачи информации, в том числе с использованием различных материальных носителей; шифрование и дешифрование; копирование и распространение с сохранением точности; увеличение плотности записи и скорости передачи; сохранение при ее потреблении и т. д. Особые свойства цифровой информации привели к очень большим возможностям повышения эффективности всех сторон экономической и общественной жизни, что в конечном счете спровоцировало вполне обоснованный взрыв интереса к цифровой информации и ее использованию.

Авторское определение понятия цифровизации, понимаемой в узком смысле, отличается тем, что оно охватывает все этапы — появление цифровой информации как результата трансформации информации, первоначально представленной в любой другой форме; использование информации в ее цифровой форме; перевод цифровой информации в другую форму ее представления.

Целью данной статьи является изучение проблем, связанных с возможными негативными воздействиями цифровизации на развитие экономики и общества, а также на деятельность отдельного экономического субъекта. Статья содержит, в частности, уточнение содержания и взаимосвязей таких понятий, как вызов и угроза цифровизации, рассматриваемой как в широком, так и в узком смыслах, а также описание возможных отрицательных последствий и рисков, обусловленных этими вызовами и угрозами. Отдельно выделен анализ и описание киберрисков как рисков нарушения безопасности цифровой информации, и предложен вариант управления ими на основе соответствующих программ.

В данной статье выдвигается следующая гипотеза: возможность отрицательных последствий цифровизации может быть в конечном итоге описана через риски, поэтому задача повышения эффективности воздействия цифровизации на развитие экономики и общества предполагает обязательность выявления таких рисков и управления ими в целях снижения или нивелирования возможных отрицательных последствий. Одним из наиболее значимых рисков, связанных с трансформацией инфор-

мации в цифровую форму и с использованием цифровой информации, является киберриск — риск, обусловленный невыполнением требований по обеспечению безопасности цифровой информации. Поэтому управление киберрисками, направленное на снижение потерь, связанных с их реализацией, будет способствовать повышению эффективного воздействия цифровизации на деятельность любого экономического субъекта.

Соотношение понятий «цифровизация как тренд общественного развития» и «цифровизация как процесс трансформации информации в цифровую форму и использования цифровой информации»

Так как информация все больше и больше становится важнейшим ресурсом для всех сторон общественной и экономической сторон жизни, то степень охвата ею важнейших сторон жизни характеризует процесс перерастания цифровизации, рассматриваемой в узком смысле, в цифровизацию, рассматриваемую в широком смысле. В настоящее время уже можно говорить о тех сторонах общественной и экономической жизни, степень проникновения в которые конкретного и эффективного преобразования любой информации в цифровую, имеющую особенности и большие преимущества, позволяет описывать цифровизацию как современный тренд всего общественного развития.

К числу сторон общественной и экономической жизни, которые, по признанию мирового сообщества, должны быть охвачены процессами цифровизации, для того чтобы она (цифровизация) рассматривалась как важнейшая тенденция общественного развития, можно отнести, например, те, которые были предложены Европейской комиссией и вошли в расчет Индекса цифровизации экономики и общества DESI (Digital Economy and Society Index)[1], используемого для оценки степени охвата цифровизацией стран Евросоюза.

Этот Индекс как итоговый рассчитывается по методике Евросоюза на основе значений следующих пяти вербальных параметров, характеризующих определенную сторону общественной жизни и определяемых на основе 31 конкретного показателя[2]: Connectivity — связь, обеспечивающая доступность цифровой информации для ее пользователей; Human Capital / Digital skills — навыки населения по использованию возможностей, предлагаемых цифровым сообществом; Use of Internet by citizens — использование интернета гражданами в обычной жизни; Integration of Digital Technology by businesses — интеграция цифровых технологий в бизнес; Digital Public Services — параметр, описывающий степень проникновения цифровизации, в первую очередь, в социальную сферу.

Для оценки влияния цифровизации на общественную и экономическую жизнь разных стран могут использоваться и другие значимые для развития этих стран направления воздействия цифровизации, оцениваемые, например, посредством применения следующих индексов: Индекс развития информационно-коммуникационных технологий (The ICT Development Index)[3], Индекс развития электронного правительства (The

[1] [Электронный ресурс]. URL: https://ec.europa.eu/digital-single-market/en/desi (дата обращения: 18.03.2023).

[2] См.: *Халин В.Г., Чернова Г.В.* Цифровизация и ее влияние на российскую экономику и общество: преимущества, вызовы, угрозы и риски // Управленческое консультирование. 2018. № 10. С. 46–63. DOI: 10.22394/1726-1139-2018-10-46-63.

[3] [Электронный ресурс]. URL: https://www.itu.int/en/ITU-D/Statistics/Pages/IDI/default.aspx (дата обращения: 18.03.2023).

E-government Development Index)[1], Индекс сетевой готовности NRI (Networked Readiness Index)[2], Глобальный индекс кибербезопасности (The Global Cybersecurity Index)[3], Глобальный индекс конкурентоспособности (The Global Competitiveness Index)[4], Глобальный инновационный индекс (The Global Innovation Index)[5], Индекс социального прогресса (The Social Progress Index)[6].

Влияние цифровизации может оцениваться не только на уровне отдельных стран, но и для их групп, в том числе для целей построения рейтинга стран по уровню этого влияния. Естественно, что задача оценки влияния цифровизации возникает и внутри стран. Примером является использование разработанного Центром финансовых инноваций и безналичной экономики Московской школы управления СКОЛКОВО Индекса «Цифровая Россия», рассчитанного впервые по итогам 2018 г. по 85 субъектам РФ[7].

Вызовы, угрозы, последствия и риски цифровизации

В настоящее время в научной литературе вопросам воздействия цифровизации на развитие общества уделяется достаточное внимание[8]. При этом авторы обращают внимание не только на положительный эффект воздействия цифровизации на общественное развитие, но и на те отрицательные последствия, которые также возможны[9].

---

[1] [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/Статья:Рейтинг_электронного_правительства_ООН_(EGDI) (дата обращения: 18.03.2023).

[2] [Электронный ресурс]. URL: https://networkreadinessindex.org (дата обращения: 18.03.2023).

[3] [Электронный ресурс]. URL: https://www.tadviser.ru/images/8/84/Global_Cybersecurity_Index_2020.pdf (дата обращения: 18.03.2023).

[4] [Электронный ресурс]. URL: https://gtmarket.ru/ratings/global-competitiveness-index (дата обращения: 18.03.2023).

[5] [Электронный ресурс]. URL: https://www.globalinnovationindex.org/Home (дата обращения: 18.03.2023).

[6] [Электронный ресурс]. URL: https://www.socialprogress.org/ (дата обращения: 18.03.2023).

[7] [Электронный ресурс]. URL: https://www.skolkovo.ru/researches/indeks-cifrovaya-rossiya/ и https://sk.skolkovo.ru/storage/file_storage/00436d13-c75c-46cf-9e78-89375a6b4918/SKOLKOVO_Digital_Russia_Application01_2019-04_ru.pdf (дата обращения: 18.03.2023).

[8] См., например: *Хамитжанов Д. В.* Проблемы цифровизации экономики в современных условиях [Электронный ресурс]. URL: https://moluch.ru/archive/381/84217/; *Бродач М. М.* Цифровизация и внедрение умных технологий в России [Электронный ресурс]. URL: http://zvt.abok.ru/upload/pdf_articles/777.pdf; *Головчин М. А.* Влияние интернет-активности на жизнь в эпоху цифровизации общества и экономики: на данных регионального исследования [Электронный ресурс]. URL: http://apel.ieml.ru/storage/archive_articles/9920.pdf; *Белоусов Ю. В.* Методология определения цифровой экономики [Электронный ресурс]. URL: https://elibrary.ru/item.asp?id=41853553; *Гончаренко Л. П.* Цифровизация национальной экономики [Электронный ресурс]. URL: https://vestnik.guu.ru/jour/article/view/1644; *Гатилова И. Н.* Тенденции и перспективы развития цифровой экономики России на современном этапе [Электронный ресурс]. URL:https://www.elibrary.ru/item.asp?id=42572423 (дата обращения: 18.03.2023).

[9] См., например: *Халин В. Г., Чернова Г. В.* Цифровизация и ее влияние на российскую экономику и общество: преимущества, вызовы, угрозы и риски [Электронный ресурс]. URL: https://www.acjournal.ru/jour/article/view/943; *Гретченко А. И., Горохова И. В., Марцелова Т. А.* Цифровая экономика: вызовы и перспективы для развития Российской Федерации [Электронный ресурс]. URL: https://mining--cryptocurrency-ru.turbopages.org/mining-cryptocurrency.ru/s/cifrovaya-ehkonomika; *Козаев И. С.* К теории цифровой экономики: выгоды и риски [Электронный ресурс]. URL: https://elibrary.ru/item.asp?id=37657920; [Электронный ресурс]. URL: https://www.elibrary.ru/item.asp?id=42676077; [Электронный ресурс]. URL: https://docs.yandex.ru/docs/view?tm=1679551406&tld=ru&lang=ru&name=doclad_spch.pdf&text=Вызовы%20и%20угрозы%20цифровизации&url=https%3A%2F%2Fd-russia.ru/ (дата обращения: 18.03.2023).

Вызовы и угрозы цифровизации, рассматриваемой как тренд общественного развития (цифровизация, рассматриваемая в широком смысле)

Динамичность и сила разностороннего воздействия цифровизации на все стороны жизни обусловливает актуальность и необходимость более тщательного изучения проблем возможного как положительного, так и негативного воздействия цифровизации на развитие общества. Цифровизация, рассматриваемая в широком смысле как мощный тренд современного развития экономики и общества, помимо того, что является фактором положительного воздействия на многие стороны жизни, в то же время, выставляет обществу определенные вызовы — те требования, которые должны быть выполнены для того чтобы цифровизация действительно стала трендом эффективного развития экономики и повышения качества жизни.

В тех случаях, когда эти требования (вызовы) не выполняются, общество сталкивается с угрозами, которые для него могут сопровождаться различными отрицательными последствиями. Примером вызова цифровизации и отвечающей ему угрозы является вызов (требование) цифровизации о необходимости борьбы с мошенничеством, обусловленным возможностями цифровизации. Этому вызову, если эффективная борьба с мошенничеством все же отсутствует или недостаточна, отвечает, например, угроза цифрового мошенничества, которая, к сожалению, может привести к самым разным отрицательным последствиям и, в том числе, к потере финансовых средств как хозяйствующих субъектов, так и граждан. И только опережающее развитие цифровых технологий по предотвращению разных проявлений цифрового мошенничества может снизить его возможные отрицательные последствия.

Любой вызов цифровизации формулируют те требования, соблюдение которых обеспечит положительный вектор воздействия цифровизации на определенные стороны жизни. Так, например, выполнение требований цифровизации по созданию соответствующей цифровизации нормативной базы и по подготовке квалифицированных в области цифровизации кадров будет способствовать положительному воздействию цифровизации на развитие экономики и общества. В то же время, невыполнение этих требований означает возникновение угроз для экономики и общества, которые могут сопровождаться теми или иными отрицательными последствиями. Каждое из возможных отрицательных последствий может быть описано через риск — возможность появления отрицательного последствия цифровизации, связанную с возможной реализацией угрозы, обусловленной невыполнением соответствующего вызова цифровизации, рассматриваемой в широком смысле. Риск может быть описан параметрами «размер возможного отрицательного результата» и «вероятность наступления отрицательного результата»[1].

Так, обусловленное цифровизацией такое положительное воздействие на развитие общества, как расширение спектра и индивидуализация цифровых услуг, объявляет обществу вызов о необходимости контроля в области цифровых сервисов. Этот вызов несет в себе и угрозу — недостаточный контроль или его снижение в области цифровых сервисов могут сопровождаться такими отрицательными последствиями, как искажение информации, ее уничтожение и т. д. Эти возможные отрицательные последствия, обусловленные угрозой снижения контроля, могут быть описаны совокупностью соответствующих рисков — риск искажения информации, риск уничтожения информации и т. д.

Представление возможных отрицательных последствий реализации той или иной угрозы, обусловленной определенным вызовом цифровизации, в виде рисков с па-

[1] См.: *Халин В. Г., Чернова Г. В.* Цифровизация и ее влияние на российскую экономику и общество: преимущества, вызовы, угрозы и риски.

раметрами «размер возможного ущерба» и «вероятность его наступления», использование в отношении этих рисков определенных методов управления ими позволяют сформировать целостную программу управления такими рисками, направленную на нивелирование или снижение отрицательных последствий, связанных с определенными угрозами цифровизации.

Ниже представлена схема взаимосвязи понятий, отражающих возможные отрицательные последствия цифровизации, которые (последствия) обусловлены невыполнением требований (вызовов), позволяющих рассматривать цифровизацию как тренд эффективного развития экономики и общества:

> **Цифровизация** (как тенденция общественного развития) => **вызов цифровизации** (как одно из требований, которые необходимо выполнить для того, чтобы цифровизация действительно стала трендом эффективного развития экономики и повышения качества жизни) => **угроза** (как возможность появления отрицательных последствий, обусловленных невыполнением требований соответствующего вызова) => **отрицательное последствие** (как возможный вариант реализации угрозы, обусловленной невыполнением требований вызова) => **риск** (как описание возможного отрицательного последствия, связанного с реализацией угрозы, обусловленной невыполнением требований вызова).

Вызовы и угрозы цифровизации, рассматриваемой как процесс преобразования и использования цифровой информации (цифровизация, рассматриваемая в узком смысле)

Вопросы использования любой информации, в том числе вопросы ее трансформации в цифровую форму, и проблемы использования цифровой информации становятся особенно важными ввиду того, что сама информация становится все более значимым ресурсом. Именно поэтому, в целях выявления возможных отрицательных последствий, связанных с использованием информации, необходимо также выявление всех вызовов, угроз и возможных отрицательных последствий.

Проблема выявления вызовов, угроз и возможных отрицательных последствий особенно актуальна для информации, вовлеченной в процессы ее трансформации в цифровую форму, и самой цифровой информации. Это объясняется, прежде всего, масштабами этих процессов и появлением новых факторов, влияющих именно на процесс трансформации информации и на саму цифровую информацию. К числу таких факторов, например, могут быть отнесены возможности влияния на информацию используемых материальных преобразователей информации, а также доступность цифровой информации.

Для того чтобы любая информация качественно удовлетворяла потребности в ее использовании, она должна быть своевременной, достоверной (с определенной вероятностью), достаточной, надежной (с определенной степенью риска), в правовом отношении корректной, адресной и актуальной. Дополнительно цифровая информация должна обладать следующими свойствами: ее организация обеспечивает комплектность системы информации, перспективу многократного использования, высокую скорость ее сбора, обработки и передачи, а также возможность кодирования.

Для того чтобы названные свойства информации любого вида, и в том числе цифровой информации, выполнялись, обязательным является соблюдение соответствующих требований — информационных вызовов (рис.).

В числе основных вызовов, связанных с любой информацией, — обязательность разработки и соблюдения положений нормативно-правовой базы, регулирующей взаимоотношения всех субъектов, связанных с информацией. Первая редакция Федерального закона «Об информации, информационных технологиях и о защите

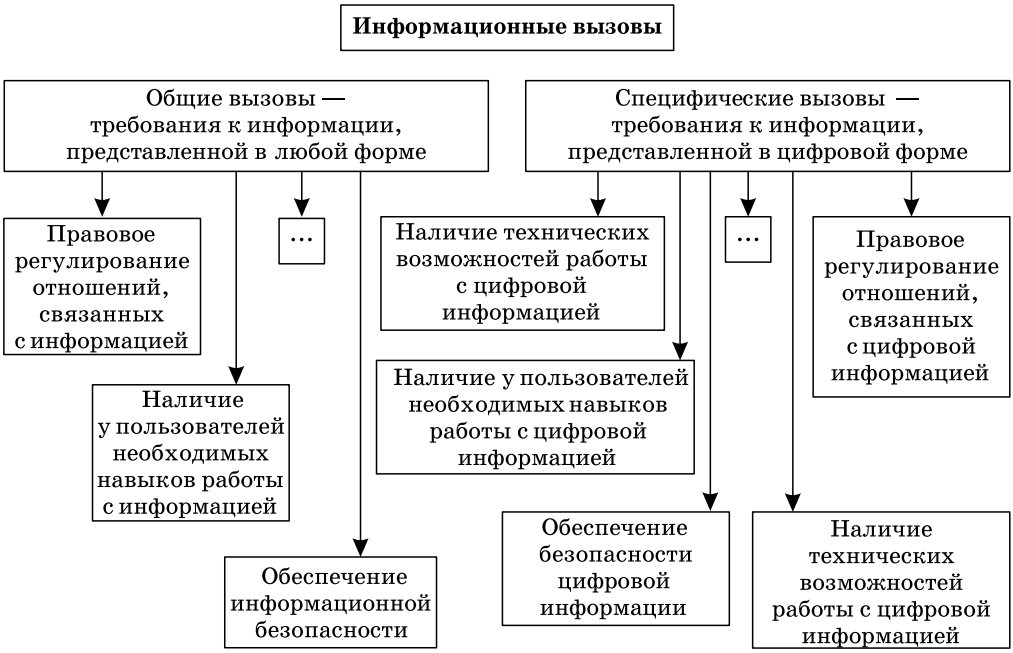

Рис. Схема возможных вызовов любой цифровой информации
Fig. Scheme of possible calls of any and digital information

информации» (№ 149-ФЗ), была принята 27.07.2006. Последующие поправки к этому базовому закону, оформленные в виде целой серии дополнительных Федеральных законов[1], относятся не только к улучшению первоначальной редакции закона, связанной с использованием любой информации, но и к вопросам, связанным с созданием и использованием цифровой информации.

Необходимо отметить, что для цифровой информации, помимо общих информационных вызовов, могут быть определены специфические. Так, среди возможных вызовов, выдвигаемых трансформацией информации в цифровую форму и применением цифровой информации, можно выделить, например, требования об обязательности создания нормативной и законодательной базы, регулирующей вопросы взаимодействия различных экономических субъектов и отдельных граждан по поводу применения цифровой информации, требования о подготовленности специалистов и граждан к использованию цифровой информации, требования о создании материальной базы, обеспечивающей доступ к цифровой информации и т. д. (рисунок). Однако, по мнению специалистов, среди возможных вызовов, выдвигаемых трансформацией любой информации в цифровую форму и применением самой цифровой информации, особое место занимает вызов цифровизации, рассматриваемой в узком смысле, выделенный в научной и практической литературе как «кибервызов», который предполагает обязательность обеспечения безопасности цифровой информации[2].

[1] [Электронный ресурс]. URL: https://normativ.kontur.ru/document?moduleId=1&documentId=442123; [Электронный ресурс]. URL: https://www.iso/org/ru/standards.html (дата обращения: 18.03.2023).

[2] См., например: *Полякова Т. А.* Информационная безопасность через призму национального проекта «цифровая экономика»: правовые проблемы и векторы решений [Электронный ресурс]. URL: https://elibrary.ru/item.asp?id=38203006 (дата обращения: 18.03.2023).

Информационная безопасность представляет собою практику предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации[1]. В общем случае обеспечение информационной безопасности можно рассматривать на трех уровнях — всего общества, национальном и на уровне различных субъектов экономики[2].

Важность кибербезопасности любого уровня признается обществом в том числе через разработку и определение значений глобального индекса кибербезопасности The Global Cybersecurity Index, который разрабатывается Международным союзом электросвязи и характеризует уровень кибербезопасности в стране[3]. Для его расчета используются данные о развитии правовых, технических и организационных мер в области кибербезопасности, наличии государственных образовательных и научных институтов, партнерств, механизмов сотрудничества и систем обмена информацией, способствующих наращиванию потенциала в сфере информационной безопасности.

Для уровня отдельного экономического субъекта вызов безопасности цифровой информации (кибервызов) обозначает группу тех требований[4], которые должны быть соблюдены для того чтобы информации не был нанесен ущерб, и чтобы она оставалась достоверной и доступной в той мере, как это предусмотрено ее обладателями. Соблюдение этих требований обеспечивается действиями, направленными на предотвращение несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации[5]. Невыполнение выделенной группы требований несет в себе киберугрозу, которая может сопровождаться самыми разными отрицательными последствиями нарушения информационной безопасности.

Киберугроза, обусловленная цифровизацией как способом перевода информации в цифровую форму и методами работы с цифровой информацией, представляет собою совокупность факторов и условий, создающих опасность нарушения безопасности цифровой информации не только в компьютерах, глобальной сети Интернет, но и во всех других объектах и средах, использующих цифровые технологии. Как неопределенная возможность нарушения безопасности цифровой информации, киберугроза может быть представлена различными отрицательными последствиями, к числу которых могут быть отнесены несанкционированный доступ к цифровой информации, ее кража, уничтожение и т. д.

Ввиду неопределенности реализации самой киберугрозы, каждое из возможных отрицательных последствий может быть описано через киберриск — неопределенную возможность нарушения безопасности цифровой информации, связанную с реализацией киберугрозы, обусловленной невыполнением требований кибервызова об обеспечении ее безопасности. Киберриск представляет собою описание возможного отрицательного последствия нарушения безопасности цифровой информации (отрицательного последствия цифровизации, рассматриваемой в узком смысле), свя-

---

[1] Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/Информационная_безопасность:~:text=Информационная%20безопасность%20—%20практика%20предотвращения,применяется%20вне%20зависимости%20от%20формы:) (дата обращения: 18.03.2023).

[2] В статье проблемы информационной безопасности рассматриваются на уровне отдельного экономического субъекта.

[3] Global Cybersecurity Index 2020 [Электронный ресурс]. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx (дата обращения: 18.03.2023).

[4] Другие вызовы, связанные с трансформацией информации в цифровую форму и с использованием цифровой информации, например связанные с созданием соответствующего нормативного сопровождения, будут включать другие требования.

[5] [Электронный ресурс]. URL: https://www.researchgate.net/publication/220102979_Information_security_culture_From_analysis_to_change (дата обращения: 18.03.2023).

занного с реализацией киберугрозы, обусловленной невыполнением требований кибервызова. Он может быть представлен параметрами «размер возможного отрицательного последствия» и «вероятность наступления отрицательного последствия»[1].

Ниже схематично представлена взаимосвязь понятий и терминов, используемых для отражения возможного отрицательного воздействия цифровизации, рассматриваемой в узком смысле, обусловленного нарушением безопасности именно цифровой информации:

> **Цифровизация** (как процесс трансформации информации в цифровую форму и использования цифровой информации) => **кибервызов** (как группа требований, которые необходимо выполнить для того чтобы цифровизация обеспечивала безопасность цифровой информации) => **киберугроза** (как возможность появления отрицательных последствий, обусловленных невыполнением требований кибервызова об обеспечении безопасности цифровой информации) => **отрицательное последствие** (как возможный вариант реализации киберугрозы, обусловленной невыполнением требований кибервызова об обеспечении безопасности цифровой информации) => **киберриск** (как параметр описания возможного отрицательного последствия, связанного с реализацией киберугрозы, обусловленной невыполнением требований кибервызова об обеспечении безопасности цифровой информации).

Цифровизация в широком смысле предусматривает обязательное использование цифровой информации. Поэтому кибервызов о безопасности цифровой информации (для цифровизации, рассматриваемой в узком смысле) можно рассматривать и как вызов цифровизации, рассматриваемой в широком смысле. Последнее, а также место и роль информации как важнейшего современного ресурса обусловливают высокую значимость кибервызова — вызова об обеспечении безопасности цифровой информации.

Среди различных факторов и условий появления киберугрозы, т. е. факторов, создающих опасность нарушения безопасности цифровой информации, необходимо выделить те, которые сами являются порождением цифровизации и поэтому требуют особого контроля. К их числу можно отнести вирусы, черви, троянские программы, программы-шпионы, фишинг, руткиты, шифровальщики, программы-майнеры, ботнеты, hoax, спам, deep fake (подделка голоса и/или лица), программы для организации DoS и DDoS-атак, хакерские утилиты, конструкторы вирусов и т. д. Для любого компьютера наличие программ-шпионов, являющихся порождением цифровизации, также является фактором киберугрозы, т. е. фактором, создающим опасность нарушения безопасности цифровой информации.

Киберриски деятельности отдельного экономического субъекта

Киберриски — риски нарушения безопасности цифровой информации — могут появиться на любом уровне использования цифровой информации, в том числе на уровне отдельного экономического субъекта. Они связаны с определенными отрицательными последствиями возможной реализации киберугрозы, которая, в свою очередь, обусловлена невыполнением требований кибервызова об обеспечении безопасности цифровой информации.

Примерами киберрисков являются риски: несанкционированного доступа; кражи данных; изменения/подмены данных; утраты/уничтожения данных; временной потери доступа к данным и/или объекту (блокировки); вывода из строя объекта; нарушения корректного функционирования объекта (преднамеренное/не преднамерен-

[1] *Халин В. Г., Чернова Г. В.* Цифровизация и ее влияние на российскую экономику и общество: преимущества, вызовы, угрозы и риски.

ное) и т. д. Примерами киберрисков, обусловленных влиянием самой цифровизации, могут быть риски, обусловленные внесением или проникновением в компьютеры, серверы, сети и т. д., используемые человеком, отдельной организацией, отраслью или государством, различных вирусов, шпионских программ и т. д., которые сами являются продуктом цифровизации; хакерскими атаками и т. д.

На появление киберрисков в рамках отдельного экономического субъекта влияние оказывают две группы факторов — факторы, обусловленные непосредственным воздействием цифровизации как совокупности процессов трансформации информации в цифру и работы с цифровой информацией, и факторы, обусловленные спецификой деятельности отдельного предприятия. В свою очередь, факторы киберугроз, обусловленные спецификой всей деятельности отдельной организации, условно также могут быть разделены на две группы:

- внешние факторы, влияющие на деятельность отдельной организации, например, фактор использования цифровой информации, к которой имеют доступ и другие экономические субъекты, например, недобросовестно использующие ее;
- внутренние факторы, например, связанные с реализацией определенных направлений деятельности отдельной организации.

Возможности проявления на уровне отдельного экономического субъекта киберрисков, с одной стороны, а также рисков, обусловленных спецификой реализации деятельности экономического субъекта, с другой стороны, актуализируют вопрос соотношения этих групп рисков и значимости их влияния на результаты деятельности субъекта. Ниже представлены выводы, полученные авторами, на основе анализа результатов опроса, проведенного среди предприятий производственного комплекса, совместно с «Microsoft» — мировым лидером в области информационных технологий, поставляющим широкий диапазон устройств и сервисов, программного обеспечения и ИТ-услуг, и «Marsh & McLennan Companies» — американской сервисной компанией, оказывающей профессиональные услуги в области управления рисками, страхования и перестрахования[1].

Опрос прежде всего был направлен на выяснение понимания, значимости и места киберрисков среди других рисков производственных организаций. Изучение результатов этого опроса, а также современного освещения этих проблем в научной и практической литературе показало следующее: киберриск как самостоятельный признало более 70% предприятий, участвующих в опросе, при этом осознание значимости этого риска резко возросло за 2017–2019 гг.; примерно 80% опрошенных киберриск ввели в число первых, самых значимых для предприятий рисков, а 22% опрошенных поставили его на первое место; уверенность организаций в обеспечении киберустойчивости и в возможности управлять киберрисками все время снижается.

К числу причин нарушения безопасности цифровой информации, обусловленных спецификой деятельности организации, можно отнести следующие:

- недостаточно серьезное отношение к самой проблеме киберрисков, прежде всего со стороны руководства компаний;
- недостаточная прозрачность деятельности организаций на всех технологических этапах по обработке данных;
- усиленное внимание к другим возможным рискам, а не к киберриску, обусловленным спецификой деятельности компании, например, к риску неопределенности экономической ситуации, разрыва цепочки поставок и т. д.;
- недостаточное внимание к киберриску, который для определенного экономического субъекта может быть самым значимым среди других;

[1] [Электронный ресурс]. URL: 2019 Global Cyber Risk Perception Survey https://www.marshmclennan.com/content/dam/mmc-web/insights/publications/2020/february/marsh-microsoft-2019-global-cyber-risk-perception-survey-manufacturing-report.pdf (дата обращения: 18.03.2023).

- непонимание того, что киберриски могут быть связаны не только с отдельным направлением деятельности организации, также они могут определяться зависимостью бизнес-процессов, протекающих внутри организации;
- непонимание ситуации возникновения и влияния киберрисков на общие результаты деятельности организации в зависимости от фактора «закрытости организации». Если компания работает самостоятельно и технологически не зависит от других, то это ее киберриск. Включение же организации в цепочку технологически взаимосвязанных других экономических субъектов означает вовлечение в свою деятельность киберрисков других экономических субъектов, вовлеченных в общую технологическую цепь;
- недопонимание необходимости проведения не только технических и профилактических мероприятий по снижению киберрисков, но и экономических мероприятий, в частности, использования киберстрахования, а также мер по привлечению внешних ресурсов для управления киберрисками;
- недопонимание важности инвестиций в технологии кибербезопасности и обучение персонала, и инноваций, направленных на предотвращение реализации киберрисков, их профилактику и снижение ущерба при их реализации;
- отсутствие или несовершенство методов и методик оценки киберрисков, в первую очередь, методов количественной оценки киберрисков;
- неготовность к использованию новых цифровых технологий (облачные вычисления, цифровые продукты, подключенные устройства, интернет вещей и т. д.), а также технологий материального производства, наделенных цифровыми преимуществами;
- недооценка фактора встраивания новых технологий в бизнес-инфраструктуру, каким-то образом связанных с цифровой информацией;
- недооценка важности обучения персонала и, в первую очередь, менеджеров высшего звена, работе с цифровой информацией и пониманию проблем реализации киберрисков;
- дискретный, а не непрерывный контроль за киберрисками;
- излишнее доверие организаций к поставщикам новых технологий, оборудования, продуктов и т. д. в отношении возможных сопутствующих киберрисков;
- неспособность управления киберрисками и т. д.

Управление киберрисками

Как показывает проведенный анализ, в компаниях, уже пытающихся управлять киберрисками, уверенность в положительном эффекте такого управления отсутствует. Зачастую, выбирая новую технологию или инновацию, предприниматели не особо обращают внимание на то, как эти новшества связаны с киберрисками. В большинстве случаев киберриски рассматриваются как технологическая проблема, а не как важнейший фактор формирования конечных результатов бизнеса. Хотя в понимании руководства небольших компаний и организаций киберриски все еще отодвигаются на второй план по сравнению с технологическими рисками, тем не менее, в крупных компаниях возрастает осознание опасности киберрисков. Большие надежды по борьбе с киберрисками предприниматели связывают с обязательностью выполнения требований государственного регулирования отношений по цифровизации, в том числе с необходимостью соблюдения отраслевых стандартов, а также с применением такой формы финансовой защиты от киберрисков, как киберстрахование.

Снижению размера возможных отрицательных последствий, описываемых киберрисками, должно способствовать целенаправленное управление ими, принимающее во внимание целый ряд факторов. Ввиду специфики деятельности различных

экономических субъектов при управлении киберрисками возникает проблема учета влияния этой специфики на сам перечень киберрисков и на методы управления ими.

Не весь перечень возможных киберрисков может присутствовать в организациях, занимающихся одинаковыми видами деятельности, но имеющих отличающиеся приоритетные направления осуществления этой деятельности, или вообще занимающиеся разными видами деятельности. Так, даже для двух организаций промышленного производства одинаковой продукции, приоритетные направления деятельности могут отличаться между собой. Одна из них в настоящее время занимается встраиванием в процессы производства новых цифровых технологий, и поэтому для нее актуальными становятся киберриски, связанные с решением этой задачи. А для другой организации, также занимающейся выпуском аналогичной продукции, актуальными становятся киберриски освоения новой маркетинговой стратегии.

Выделение двух групп факторов киберугрозы — обусловленных спецификой сфер внедрения цифровизации, в том числе спецификой деятельности отдельного экономического субъекта, и самой цифровизацией как процессом создания и использования цифровой информации, обусловливает два уровня управления киберрисками: опосредованное управление киберрисками — через такое управление определенными областями и сферами цифровизации, которое способствует снижению киберрисков; непосредственное управление киберрисками, как рисками, угрожающими безопасности цифровой информации.

Вариантами реализации опосредованного управления киберрисками могут быть:

- государственное и отраслевое регулирование деятельности компаний по управлению киберрисками. Примером эффективного регулирования процессами управления киберрисками являются стандарты, разработанные в National Institute of Standards and Technology (NIST) — американском национальном институте стандартизации [1; 2; 3], и в International Organization for Standardization (ISO) — международной организации, занимающейся выпуском стандартов[1];
- пересмотр инвестиционной стратегии любой фирмы в сторону учета значимости киберрисков;
- применение количественных методов измерения киберрисков — вероятности их реализации и размеров возможного ущерба;
- разработка программ управления киберрисками, направленных на снижение вероятности реализации киберрисков и на снижение размера возможного ущерба;
- обучение персонала правильному управлению киберрисками на базе изучения содержания разработанных программ управления киберрисками;
- учет при определении количественной оценки возможного ущерба от реализации киберрисков не только технологического ущерба, но и экономических потерь, связанных с ними;
- применение киберстрахования и т. д.

Условием эффективного управления киберрисками на уровне отдельного экономического субъекта прежде всего является осознание значимости киберрисков, и не только как технологических рисков, но, в первую очередь, как важнейших экономических рисков для самого бизнеса. Управление киберрисками на уровне отдельного экономического субъекта предполагает:

- изучение бизнес-процессов деятельности этого экономического субъекта и их связей как источников возникновения киберрисков и основы взаимосвязей групп рисков, связанных с отдельными бизнес-процессами;

[1] [Электронный ресурс]. URL: https://www.securityvision.ru/blog/upravlenie-riskami-informatsionnoy-bezopasnosti-chast-7-standart-iso-iec-27005-2018-prodolzhenie-sta/ (дата обращения: 18.03.2023).

- выбор методов оценки киберрисков, в первую очередь количественных, а также методов управления всеми выявленными киберрисками (по всем бизнес-процессам) с выделением необходимых для этого ресурсов, исполнителей и сроков выполнения;
- разработку инструментов по восстановлению нормальной работы экономического субъекта после реализации киберрисков, с определением размера возможного ущерба и поиском необходимых ресурсов, с указанием исполнителей и сроков.

В рамках профилактики управление киберрисками должно охватывать вопросы выбора мер защиты от киберрисков — будет ли экономический субъект оставлять эти риски на собственной ответственности, избегать их, передавать риски. При этом, естественно, принятие решения будет предполагать оценку соотношения затрат, связанных с внедрением мер защиты от киберриска, с одной стороны, и возможных потерь, сопровождающих реализацию киберрисков, с другой стороны. Важными также являются вопросы выделения редких, но разрушительных киберрисков, ранжирования киберрисков, определения временного интервала действия того или иного принятого решения по киберрискам и т. д.

Дополнительно управление киберрисками должно учитывать влияние таких факторов, как модернизация имеющихся и появление новых бизнес-процессов компании; освоение новых и модернизация старых технологий; наличие технологически связанных цепочек разных экономических субъектов. Отдельного внимания в проблеме управления киберрисками заслуживают вопросы инвестиций в технологии кибербезопасности; измерения эффективности разных вариантов инвестиций по снижению киберрисков в целях выбора наилучшего из них; сопоставления эффективности инвестиций по снижению киберрисков с эффективностью инвестиций по снижению других видов рисков; отбора конкретных технологий кибербезопасности, направленных на снижение возможностей реализации киберугрозы, т. е. направленных против несанкционированного доступа к информации, ее кражи, уничтожения данных и т. д.

Выводы

Помимо положительного воздействия на развитие общества цифровизация может оказывать на него и отрицательное влияние. Именно поэтому актуальным является изучение вопросов, связанных с ее возможным негативным влиянием на развитие экономики и общества. К числу полученных методологических результатов можно отнести уточнение содержания терминов, применяемых для отражения возможного отрицательного воздействия цифровизации, рассматриваемой в широком смысле:

- под вызовом цифровизации понимается то требование, которое необходимо выполнить для того, чтобы цифровизация действительно стала трендом эффективного развития экономики и повышения качества жизни;
- под угрозой цифровизации понимается возможность появления отрицательных последствий, обусловленных невыполнением требований соответствующего вызова;
- под отрицательным последствием цифровизации понимается вариант реализации угрозы, обусловленной невыполнением требований вызова;
- под риском цифровизации понимается параметр описания возможного отрицательного последствия, связанного с реализацией угрозы, обусловленной невыполнением требований какого-либо вызова цифровизации.

Все вызовы, угрозы, последствия и риски цифровизации условно можно разделить на две группы — те, которые обусловлены влиянием цифровизации, рас-

сматриваемой как тренд общественного развития, на ту или иную сферу деятельности человека, в том числе на деятельность отдельного экономического субъекта, и те, которые связаны с рассмотрением цифровизации в узком смысле — как процесса трансформации информации любой формы ее представления в цифровую и использования цифровой информации.

Аналогичный подход к уточнению и связям понятий цифровизации, используемой в узком смысле, в статье представлен в отношении кибервызова — важнейшего требования к обеспечению безопасности цифровой информации. В частности, выделена следующая цепочка связей между названным кибервызовом и отвечающими ему киберрисками:

> Цифровизация => кибервызов => киберугроза => отрицательное последствие киберугрозы => киберриск.

Цифровизация, рассматриваемая в узком и широком смыслах, связана с цифровой формой представления информации, поэтому киберриски, реализация которых может привести к нарушению безопасности цифровой информации, являются очень значимыми с позиций их влияния на результаты деятельности любого экономического субъекта. Это определяет необходимость выявления причин нарушения информационной безопасности, в том числе причин нарушения безопасности цифровой информации, определения факторов киберугроз, возможных отрицательных последствий и киберрисков, описывающих их.

В целях снижения возможных отрицательных последствий цифровизации, обусловленных нарушением безопасности цифровой информации, необходимо такое управление киберрисками, которое будет способствовать снижению возможного отрицательного воздействия цифровизации, т. е. будет отвечать усилению ее положительного эффекта, что и подтверждает выдвинутую в статье гипотезу.

Литература/ References

1. *NIST* Interagency or Internal Report 7298 : Glossary of Key Information Security Terms / Richard L. Kissel, ed., Computer Security Division, Information Technology Laboratory. Rev. 2. Gaithersburg, MD, USA : National Institute of Standards and Technology, 2013. 222 p.
2. *NIST* Special Publication 800-14 : Generally Accepted Principles and Practices for Securing Information Technology Systems. Gaithersburg, MD, USA : National Institute of Standards and Technology, 1996. 61 p.
3. *NIST* Special Publication 800-160 : Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2016. Vol. 1. 260 p.

Об авторах:

Халин Владимир Георгиевич, профессор кафедры информационных систем в экономике Санкт-Петербургского государственного университета (Санкт-Петербург, Российская Федерация), доктор экономических наук, профессор; v.halin@spbu.ru

Чернова Галина Васильевна, профессор кафедры управления рисками и страхования Санкт-Петербургского государственного университета (Санкт-Петербург, Российская Федерация), доктор экономических наук, профессор; g.chernova@spbu.ru

About the authors:

Vladimir G. Khalin, Professor of the Chair of Information Systems in Economics of Saint-Petersburg State University (Saint Petersburg, Russian Federation), Doctor of Science (Economic), Professor; v.halin@spbu.ru

Galina V. Chernova, Professor of the Chair of Risk management and Insurance of Saint-Petersburg State University (Saint Petersburg, Russian Federation), Doctor of Science (Economic), Professor; g.chernova@spbu.ru