

Риски цифровизации и управление ими

Халин В. Г. *, Чернова Г. В., Калайда С. А.

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

РЕФЕРАТ

Цифровизация как важнейшая тенденция современного развития экономики и общества может сопровождаться не только положительными, но и отрицательными последствиями. Для того чтобы она оказывала только положительное воздействие, необходимо выполнить те требования, которые она выставляет обществу в виде содержания вызовов. В том случае, когда эти требования не выполняются, возникает угроза появления отрицательных последствий воздействия цифровизации, которые предлагается описывать через риск. Проблему усиления положительного и уменьшения отрицательного влияния цифровизации на деятельность определенного субъекта и/или на содержание какого-либо объекта воздействия цифровизации в статье предлагается решать на основе создания и внедрения Комплексной программы управления рисками цифровизации. Она включает Программу № 1 управления рисками, обусловленными влиянием цифровизации на определенное направление жизнедеятельности общества; Программу № 2 управления рисками, обусловленными применением основных продуктов цифровизации; Программу № 3 управления киберрисками или Программу № 4 управления информационными рисками, частью которой является Программа № 3. Каждая из этих программ содержит 2 части: ч. 1 содержит управленческие решения, разрабатываемые самостоятельно, ч. 2 — содержит управленческие решения по реализации требований нормативных правовых актов, а также национальных и межгосударственных стандартов, реализующих управление рисками нарушения информационной безопасности на государственном, межгосударственном или на отраслевом уровне.

Ключевые слова: цифровизация, понимаемая в узком смысле; цифровизация, понимаемая в широком смысле; направление воздействия цифровизации; параметры описания направления воздействия цифровизации; основные продукты цифровизации; информационные риски; киберриски; Программы управления рисками цифровизации; регулирование рисков цифровизации

Для цитирования: Халин В. Г., Чернова Г. В., Калайда С. А. Риски цифровизации и управление ими // Управленческое консультирование. 2024. № 3. С. 67–85.

Digitalization Risks and Their Management

Vladimir G. Khalin*, Galina V. Chernova, Svetlana A. Kalayda

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

ABSTRACT

Digitalization, as the most important trend in the modern development of the economy and society, can be accompanied by not only positive but also negative consequences. In order for it to have only a positive impact, it is necessary to fulfill the requirements that it presents to society in the form of the content of the challenges. In the case when these requirements are not met, there is a threat of negative consequences of the impact of digitalization, which are proposed to be described through risk. The article proposes to solve the problem of enhancing the positive and reducing the negative impact of digitalization on the activities of a certain subject and/or on the content of any object impacted by digitalization on the basis of the creation and implementation of a Comprehensive Digitalization Risk Management Program. It includes Program N 1 for managing risks caused by the impact of digitalization on a certain area of society; Program N 2 for managing risks caused by the use of main digi-

talization products; Cyber Risk Management Program N 3 or Information Risk Management Program N 4, of which Program N 3 is a part. Each of these programs contains 2 parts: part 1 contains management decisions developed independently, part 2 contains management decisions to implement the requirements of regulatory legal acts, as well as national and interstate standards that implement risk management of information security violations at the state, interstate or industry levels level.

Keywords: digitalization, understood in a narrow sense; digitalization, understood in a broad sense; direction of impact of digitalization; parameters for describing the direction of impact of digitalization; main products of digitalization; information risks; cyber risks; Digitalization risk management programs; regulation of digitalization risks

For citing: Khalin V. G., Chernova G. V., Kalayda S. A. Digitalization Risks and Their Management // Administrative consulting. 2024. N 3. P. 67–85.

Введение

Развитие любой национальной экономики находится под влиянием самых разных факторов и тенденций, имеющих различное воздействие на нее.

К числу важнейших современных тенденций общественного развития, которые могут оказывать положительное влияние на развитие национальной экономики¹, относятся цифровизация и экономическая конвергенция, а в числе тенденций и факторов, которые могут оказывать отрицательное воздействие на развитие национальной экономики, можно назвать экономические санкции против РФ; новые высокие катастрофические, в том числе природные, техногенные и т. п. риски и т. д.

Целью данной статьи является выявление рисков возможных отрицательных последствий влияния цифровизации на деятельность субъекта и/или на содержание объекта определенного уровня управления рассматриваемой сферы жизнедеятельности общества и построение комплексной программы управления ими.

Цифровизация как тенденция общественного развития

В настоящее время термин «цифровизация» используется как в узком, так и в широком смысле.

Цифровизация, понимаемая в узком смысле. В узком смысле цифровизация рассматривается как процесс преобразования и использования информации, включающий только определенные или все из следующих этапов:

- трансформация информации, первоначально представленной в любой форме, в цифровую форму (в цифру);
- использование цифровой информации;
- трансформация цифровой информации в любую другую форму.

Относительно трансформации любой информации в цифровую форму необходимо отметить следующее.

Цифровизация такого банковского продукта как договор срочного банковского вклада означает перевод информации, содержащейся в этом договоре, в цифровую форму, т. е. означает создание соответствующего *цифрового продукта*, в данном примере банковского, — «Договор срочного банковского вклада».

¹ Так как в общем случае помимо определенных положительных последствий эти факторы и тенденции могут сопровождаться и конкретными отрицательными последствиями, в статье они (факторы и тенденции) оцениваются как положительные, если итоговая оценка их возможных последствий является положительной.

Этот продукт может использоваться при работе с клиентами через интернет, т. е. при работе в режиме онлайн. В данном случае технология работы банка и клиента с этим цифровым продуктом может быть оцифрована, т. е. переведена в цифровую форму, представляющую собою *информационную технологию* работы с цифровым банковским продуктом — этим договором.

Для работы не с одним, а с разными цифровыми банковскими продуктами и с различными клиентами банк может формировать специальную *цифровую платформу* (далее «платформу»), включающую соответствующие цифровые продукты, а также информационные технологии, используемые для работы не только с отдельными цифровыми банковскими продуктами, но и с их совокупностью, а также связанные с организацией работы самой платформы.

Если отдельный банк расширяет свою деятельность за счет ее оцифровки или несколько банков объединяют свои усилия по работе с цифровыми банковскими и сопровождающими их продуктами, они в этом случае могут создавать *сети*, объединяющие уже известные и создаваемые новые платформы, цифровые продукты и информационные технологии. При этом попутно могут создаваться новые цифровые продукты и информационные технологии.

Обратите внимание!

Цифровизация, понимаемая в узком смысле, есть процесс, включающий только определенные или все из следующих этапов: трансформация информации, первоначально представленной в любой форме, в цифровую форму; использование цифровой информации; трансформация цифровой информации в любую другую форму.

Основные продукты цифровизации. Названные этапы реализации цифровизации, понимаемой в узком смысле (трансформация любой информации в цифровую форму, использование цифровой информации, перевод цифровой информации в другую форму), являются основой создания самих продуктов цифровизации, через которые и проявляется влияние цифровизации как тенденции, оказывающей влияние на развитие общества.

А так как не все виды продуктов цифровизации появляются сразу, то в развитии цифровизации, определяемом применяемыми основными продуктами цифровизации, когда она (цифровизация) рассматривается как тенденция общественного развития, можно выделить определенные этапы.

Прежде всего цифровизация коснулась отдельных цифровых продуктов и информационных технологий. Поэтому основным продуктом цифровизации первого этапа ее развития являются «отдельные цифровые продукты и информационные технологии»¹.

На втором этапе развития цифровизации к более масштабному применению различных цифровых продуктов и информационных технологий присоединяется новый цифровой продукт — «платформа», объединяющая определенные цифровые продукты и информационные технологии на базе их совместного применения. По этой причине основным продуктом цифровизации второго этапа ее развития как тенденции общественного развития являются «цифровые продукты, информационные технологии и платформы». Заметим, что в состав цифровых продуктов и информационных технологий этого этапа входят не только те, которые формировали основной продукт первого этапа развития цифровизации, но и появляющиеся дополнительные новые.

Дальнейшее развитие процессов цифровизации приводит к тому, что создаваемые платформы начинают объединяться между собой и образуют сети. Поэтому

¹ Понятие «основной продукт цифровизации», отвечающий определенному этапу развития цифровизации, носит обобщающий характер — оно включает перечень тех продуктов цифровизации, которые на данном этапе имеют наибольшее распространение.

основным продуктом цифровизации третьего этапа ее развития становятся «цифровые продукты, информационные технологии, платформы и сети, объединяющие их». При этом состав цифровых продуктов, информационных технологий и платформ может быть шире, чем для второго этапа развития цифровизации.

Обратите внимание!

Основными продуктами цифровизации как тенденции общественного развития являются:

- ◆ на первом этапе ее развития — отдельные цифровые продукты и информационные технологии;
- ◆ на втором этапе — цифровые продукты, информационные технологии и платформы;
- ◆ на третьем этапе — цифровые продукты, информационные технологии, платформы и сети, объединяющие их.

Хотя на каждом конкретном этапе могут быть продукты цифровизации, относящиеся к другим этапам, каждому этапу в соответствии ставится ее основной продукт, применяемый на этом этапе. И только появление новых продуктов цифровизации, которые все больше находят применение, будет означать возможность проявления следующего этапа цифровизации.

В настоящее время, например, все больше внимания уделяется месту и возможности искусственного интеллекта, как обучающего механизма, используемого в работе с цифровой информацией. При этом появление нового этапа развития цифровизации и формирование, в связи с этим, нового основного продукта цифровизации будет определяться тем, какое влияние этот этап и характерный для него основной продукт будут оказывать на развитие экономики и общества.

Цифровизация, понимаемая в широком смысле. Это понятие связано с рассмотрением ее как тенденции общественного развития.

Цифровизация, понимаемая в широком смысле, это тенденция общественного развития, которая может проявляться по разным направлениям функционирования и развития общества, каждое из которых определяется сферой жизнедеятельности общества, субъектом и/или объектом цифровизации и уровнем управления, на котором это воздействие на субъект и/или объект проявляется.

Так, цифровизация как тенденция общественного развития может проявляться, например, в сфере образования (сфера жизнедеятельности общества) для такого субъекта ее влияния, как высшая школа (система высшего образования), причем на уровне всего общества — первый уровень управления образованием, или, например, на уровне отдельного вуза — второй уровень управления образованием. Цифровизация оказывает влияние на функционирование высшей школы, рассматриваемой на уровне всего государства, например, через такие ее продукты, как цифровой продукт, информационные технологии и образовательные платформы, охватывающие всю национальную систему высшего образования. В то же время на уровне вуза цифровизация может оказывать влияние, например, только через цифровой продукт и информационные технологии, применяемые в его учебном процессе. Также цифровизация может оказывать влияние на систему высшего образования, например, через такой объект ее воздействия, как организационная структура всей системы, который (объект) относится к первому уровню управления высшей школой.

Влияние цифровизации как тенденции общественного развития может проявляться в экономике, культуре, политике, искусстве и т. д., причем на самых разных уровнях функционирования тех или иных субъектов и/или объектов этой сферы. Поэтому управление процессами цифровизации как тенденции общественного развития предполагает обязательный анализ ее влияния на рассматриваемое направление жизнедеятельности общества, описываемое следующими тремя параметрами: «сфера влияния цифровизации», «субъект и/или объект воздействия

цифровизации в этой сфере влияния» и «уровень проявления влияния цифровизации на функционирование субъекта и/или объекта в этой сфере».

Обратите внимание!

1. Цифровизация как тенденция общественного развития проявляется по самым разным направлениям жизнедеятельности общества.
2. Любое конкретное направление воздействия цифровизации как тенденции общественного развития описывается следующими параметрами:
 - сфера жизнедеятельности общества,
 - субъект и/или объект рассматриваемой сферы жизнедеятельности общества, на который цифровизация воздействует,
 - уровень управления, на котором воздействие цифровизации проявляется.

Влияние цифровизации на общественное развитие через определенное направление жизнедеятельности общества

Осваивая процессы цифровизации любой сферы жизнедеятельности и уровня проявления влияния цифровизации на функционирование того или иного субъекта и/или на содержание определенного объекта этой сферы, общество, прежде всего, ориентируется на ее положительное воздействие, т. е. на те преимущества, которые она дает ему. Однако в общем случае цифровизация может сопровождаться не только положительными последствиями для экономики и общества, но и вызовами, угрозами, а также отрицательными последствиями реализации этих угроз¹ [1, 2].

Являясь действенным фактором общественного развития, цифровизация предъявляет обществу определенные *вызовы* — те требования, которые должны быть выполнены для того, чтобы она (цифровизация) действительно стала трендом эффективного общественного развития.

Так, цифровизация, субъектом воздействия которой являются банки — субъекты финансовой сферы, рассматриваемые на уровне всего финансового рынка, для обеспечения только положительного ее воздействия на банковскую деятельность может выставлять обществу следующий вызов — работающие в банках сотрудники, не имеющие навыков работы с цифровой информацией, должны либо получить соответствующие знания, либо им должна быть предоставлена возможность получить другую специальность. Естественно, что это требует от общества дополнительных затрат, но в случае невыполнения этих требований говорить о том, что цифровизация только положительно повлияла на банковскую деятельность, нельзя.

В тех случаях, когда требования вызовов не выполняются, общество сталкивается с *угрозами*, которые могут быть реализованы и поэтому несут в себе для общества возможность появления различных отрицательных последствий влияния цифровизации.

Другим примером вызова цифровизации и отвечающей ему угрозы является вызов (требование) цифровизации о необходимости борьбы с мошенничеством на уровне организации, применяющей, например, определенные цифровые продукты и информационные технологии работы с ними. При этом, если эффективная борьба с мошенничеством отсутствует — требование вызова не выполняется или принима-

¹ 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> (дата обращения: 09.03.2024); *Хамитжанов Д. В.* Проблемы цифровизации экономики в современных условиях [Электронный ресурс]. URL: <https://moluch.ru/archive/381/84217/> (дата обращения: 09.03.2024); *Бродач М. М.* Цифровизация и внедрение умных технологий в России [Электронный ресурс]. URL: http://zvt.abok.ru/upload/pdf_articles/777.pdf (дата обращения: 09.03.2024); *Гончаренко Л. П.* Цифровизация национальной экономики [Электронный ресурс]. URL: <https://vestnik.guu.ru/jour/article/view/1644> (дата обращения: 09.03.2024).

емые меры недостаточны, возникает угроза появления отрицательного последствия влияния цифровизации. В данном случае возникает возможность проявления цифрового мошенничества, которое, в свою очередь, может привести к самым разным отрицательным последствиям и, в том числе, к потере финансовых средств организации.

Содержание вызовов и угроз цифровизации зависит от специфики рассматриваемого направления воздействия цифровизации на развитие общества, которое (направление), в свою очередь, описывается субъектом и/или объектом воздействия цифровизации определенного уровня управления конкретной сферы жизнедеятельности общества.

Обратите внимание!

Выполнение требований, сформулированных в вызовах цифровизации, отвечает положительному воздействию цифровизации на развитие общества, в то время как их невыполнение несет в себе угрозу цифровизации — возможность появления ее отрицательных последствий.

Каждое из возможных отрицательных последствий может быть описано как *риск* — неопределенная возможность появления отрицательного последствия цифровизации, связанная с возможной реализацией угрозы, обусловленной невыполнением требований соответствующего вызова цифровизации. При этом риск описывается значениями следующих двух параметров — «размер возможного отрицательного результата» и «вероятность наступления отрицательного результата»¹.

Схематично взаимосвязь понятий и терминов, используемых для отражения возможного отрицательного воздействия цифровизации на деятельность субъекта и/или объекта определенного уровня управления конкретной сферы общественной жизни, может быть представлена следующим образом (рис. 1).

Представление возможных отрицательных последствий реализации той или иной угрозы, обусловленной определенным вызовом цифровизации, в виде рисков позволяет сформировать программу управления ими, направленную на нивелирование или уменьшение отрицательных последствий, связанных с соответствующими угрозами цифровизации.

Обратите внимание!

Управлять возможными отрицательными последствиями цифровизации можно на основе программ управления рисками, описывающими возможность появления этих отрицательных последствий.

При составлении программы управления риск ставится в соответствие всем требованиям рассматриваемого вызова цифровизации — решение о выполнении которых либо принимается субъектом воздействия цифровизации самостоятельно, либо становится обязательным, так как подпадает под нормативно-правовое регулирование.

Схематичное представление взаимосвязи терминов и понятий, связанных с влиянием цифровизации на деятельность отдельного субъекта и/или на содержание объекта определенного уровня управления в конкретной сфере общественной жизни, позволяет выделить самостоятельную программу управления соответствующими рисками. Это Программа управления рисками № 1, обусловленными влиянием цифровизации на определенное направление жизнедеятельности общества.

Так как риски, которые должны быть включены в эту программу, определяются спецификой рассматриваемого направления воздействия цифровизации на обще-

¹ Халин В. Г., Чернова Г. В. Цифровизация и ее влияние на российскую экономику и общество...

Цифровизация [как тенденция общественного развития, проявляющаяся на определенном направлении жизнедеятельности общества] => **вызов цифровизации** [как группа требований, которые необходимо выполнить для того, чтобы цифровизация действительно оказала положительное влияние на функционирование и развитие конкретного субъекта и/или на содержание объекта определенного уровня управления рассматриваемой сферы жизнедеятельности общества] => **угроза** [как возможность появления отрицательных последствий, обусловленных невыполнением требований соответствующего вызова] => **отрицательное последствие** [как вариант реализации угрозы, обусловленной невыполнением требований вызова] => **риск** [как описание возможного отрицательного последствия, связанного с реализацией угрозы, обусловленной невыполнением требований вызова].

Рис. 1. Схема взаимосвязи понятий, отражающих возможные отрицательные последствия влияния цифровизации, которые (последствия) обусловлены невыполнением требований вызова, связанного с воздействием цифровизации на функционирование конкретного субъекта и/или на содержание объекта определенного уровня управления рассматриваемой сферы жизнедеятельности общества

Fig. 1. A scheme of the relationship of concepts reflecting the possible negative consequences of the impact of digitalization, which (consequences) are caused by failure to comply with the requirements of the challenge associated with the impact of digitalization on the functioning of a specific subject and/or on the content of an object of a certain level of management of the considered sphere of life of society

ственную жизнь, они условно могут быть разделены на 3 группы: риски, связанные со спецификой воздействия цифровизации на рассматриваемую сферу жизнедеятельности общества; риски, связанные с конкретным субъектом и/или объектом воздействия цифровизации; риски, связанные с исследуемым уровнем управления этой сферы (рис. 2).

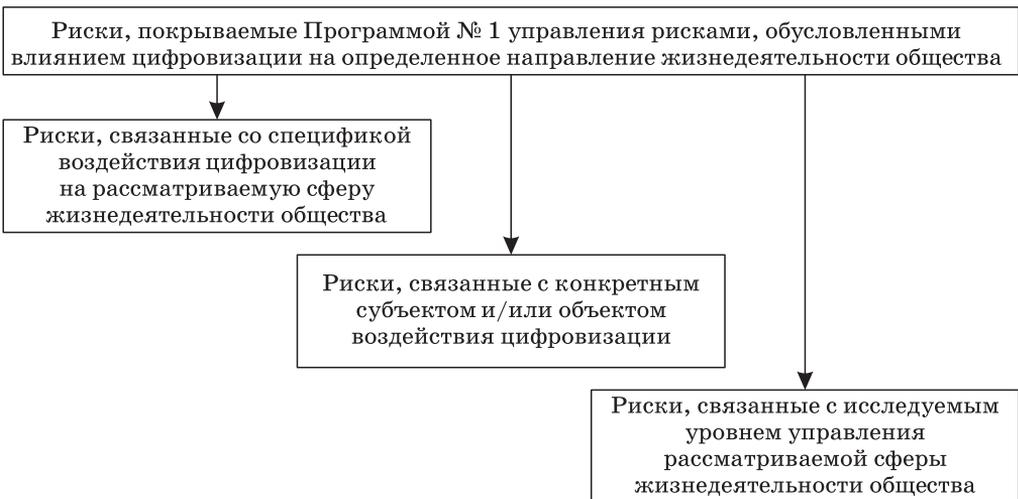


Рис. 2. Риски, управление которыми осуществляется на основе Программы № 1
 Fig. 2. Risks managed on the basis of the Program N 1

Содержанием Программы № 1 является перечень управленческих решений по управлению рисками, связанными со спецификой воздействия цифровизации на рассматриваемое направление жизнедеятельности общества (рис. 3).

Программа № 1 становится структурным элементом Комплексной программы управления рисками цифровизации, рассматриваемой как тенденция общественного развития (рис. 4).

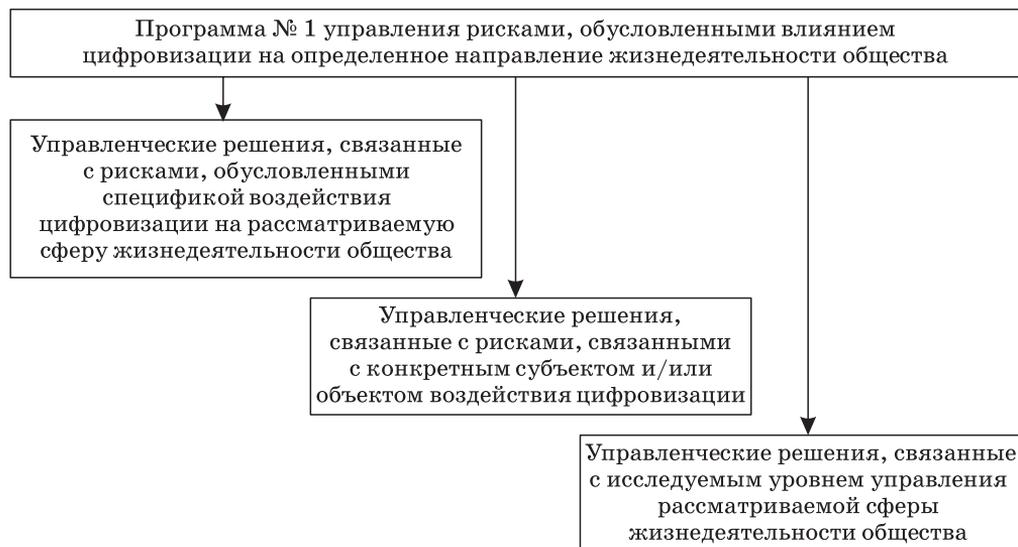


Рис. 3. Структура Программы № 1 управления рисками, обусловленными влиянием цифровизации на определенное направление жизнедеятельности общества

Fig. 3. Structure of the Program N 1 for managing risks caused by the impact of digitalization on a certain area of society's life

Влияние цифровизации на общественное развитие через основные продукты цифровизации

Как уже отмечалось выше, цифровизация оказывает влияние на развитие общества через ее продукты.

Поэтому взаимосвязь соответствующих понятий и терминов, используемых для отражения возможного отрицательного воздействия цифровизации, обусловленного использованием основных продуктов цифровизации, схематично может быть представлена следующим образом (рис. 5).

Схематичное представление взаимосвязи терминов и понятий, связанных с использованием основных продуктов цифровизации, позволяет выделить самостоятельную программу управления соответствующими рисками — Программу управления рисками № 2, обусловленными применением основных продуктов цифровизации (рис. 6). Содержанием Программы № 2 является перечень управленческих решений по управлению рисками, связанными со спецификой используемых основных продуктов цифровизации. Программа № 2 становится структурным элементом Комплексной программы управления рисками цифровизации, рассматриваемой как тенденция общественного развития (см. рис. 4.).

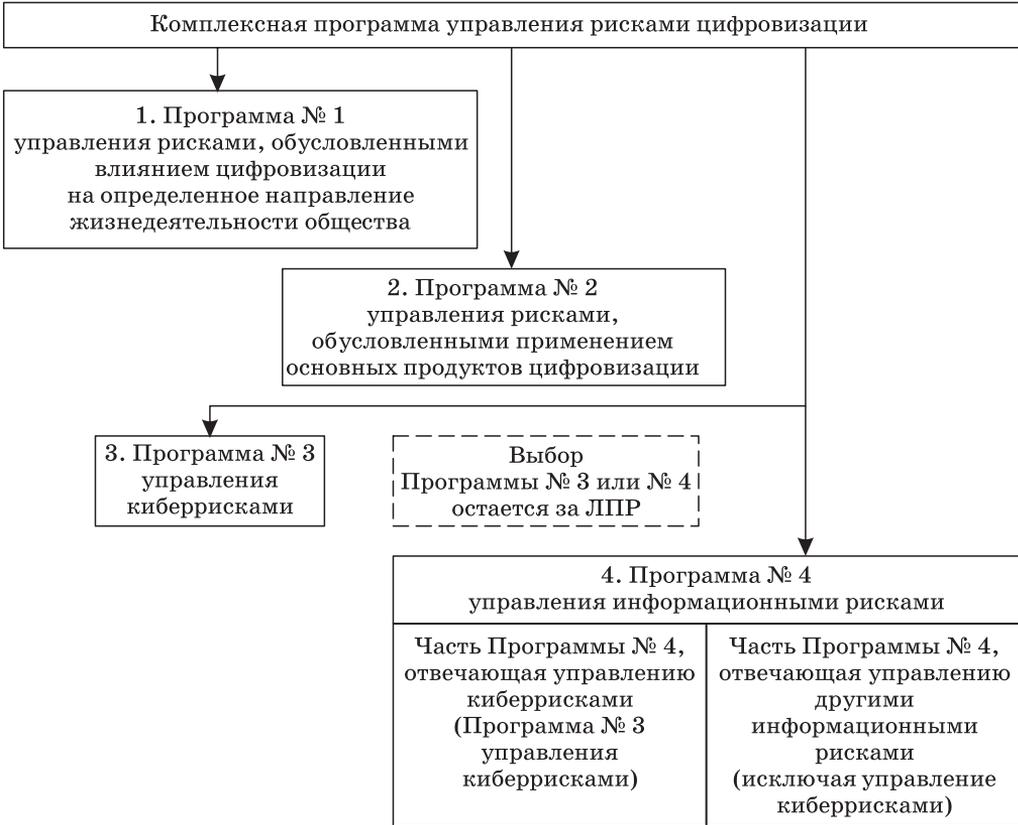


Рис. 4. Структура Комплексной программы управления рисками цифровизации
Fig. 4. Structure of the Comprehensive Digitalization Risk Management Program

Цифровизация [как тенденция общественного развития, проявляющаяся на определенном направлении жизнедеятельности общества и использующая определенный основной продукт цифровизации] => **вызов цифровизации** [как группа требований, которые необходимо выполнить для того, чтобы при использовании определенного основного продукта цифровизации действительно оказала положительное влияние на функционирование и развитие конкретного субъекта и/или на содержание какого-либо объекта воздействия цифровизации определенного уровня управления рассматриваемой сферы жизнедеятельности общества] => **угроза** [как возможность появления отрицательных последствий, обусловленных невыполнением требований соответствующего вызова] => **отрицательное последствие** [как вариант реализации угрозы, обусловленной невыполнением требований вызова] => **риск** [как описание возможного отрицательного последствия, связанного с реализацией угрозы, обусловленной невыполнением требований вызова]

Рис. 5. Схема взаимосвязи понятий, отражающих возможные отрицательные последствия цифровизации, которые (последствия) обусловлены невыполнением требований вызова, связанного с использованием определенного основного продукта цифровизации
Fig. 5. Scheme of the relationship of concepts reflecting the possible negative consequences of digitalization, which (consequences) are caused by failure to meet the requirements of the challenge associated with the use of a certain main product of digitalization



Рис. 6. Структура Программы № 2 управления рисками, обусловленными применением основных продуктов цифровизации

Fig. 6. Structure of the Program N 2 for managing risks caused by the use of main digitalization products

Примером содержания такой программы являются управленческие решения, связанные с использованием платформ. Известно, что любая платформа объединяет усилия различных пользователей по использованию цифровой информации. Это означает возможность появления и реализации такого риска как сбой в работе платформы, обусловленный влиянием каких-либо факторов, внешних или внутренних. Именно поэтому необходимо выделение рисков, специфических для различных продуктов цифровизации — в данном случае рисков, являющихся специфическими именно для платформ.

Информационные риски

Важнейшим ресурсом современного развития общества является информация. Поэтому в целях обеспечения положительного воздействия цифровизации на развитие общества необходимо выделить риски цифровой информации, а также риски любой информации, так или иначе связанной с цифровизацией.

Информация и информационные вызовы. В общем случае информация, связанная с цифровизацией, может быть разделена на три вида:

- информация, связанная с воздействием цифровизации как тенденции общественного развития на то или иное направление жизнедеятельности общества, т. е. информация, используемая для описания субъекта и/или объекта воздействия цифровизации определенного уровня управления рассматриваемой сферы жизнедеятельности общества;
- информация, связанная с использованием основных продуктов цифровизации;
- информация, связанная с понятием цифровизации в узком смысле, т. е. связанная хотя бы с одним из следующих процессов:



Рис. 7. Схема возможных вызовов любой и цифровой информации
 Fig. 7. Scheme of possible calls to any and digital information

- ◆ перевод любой информации в цифровую форму,
- ◆ использование цифровой информации,
- ◆ перевод цифровой информации в другую форму ее представления.

Известно, что любая информация оценивается как качественная, если она является своевременной, достоверной, достаточной, надежной, корректной, адресной, актуальной. Ее правильная организация обеспечивает комплектность системы информации, дает перспективу многократного использования, высокую скорость ее сбора, обработки и передачи, а также возможность кодирования.

Для соблюдения перечисленных свойств информации любого вида и, в том числе цифровой информации, обязательным является соблюдение соответствующих требований — информационных вызовов (рис. 7¹).

Киберриски — риски цифровой информации. Отличительной чертой цифровизации как тенденции общественного развития является то, что ее рассмотрение в узком смысле является обязательной составляющей цифровизации, рассматриваемой в широком смысле. Несмотря на многообразие направлений влияния цифровизации на общественную жизнь, общий перечень всех возможных требований к цифровой информации, обусловленной процессами перевода любой информации в цифровую форму, использованием цифровой информации, переводом цифровой информации в любую другую форму, является единым. При этом отличие списка реальных требований для того или иного субъекта и/или объекта воздействия цифровизации от общего перечня возможных рисков, связанных с цифровой информацией, обусловлено различием в содержании и протекании функционирования

¹ Источник рисунка: Халин В. Г., Чернова Г. В. Цифровизация и киберриски // Управленческое консультирование. 2023. № 7. С. 28–41.

или развития этого субъекта либо объекта определенного уровня управления конкретной сферы общественной жизни.

Взаимосвязь понятий и терминов, используемых для отражения возможного отрицательного воздействия цифровизации, рассматриваемой в узком смысле, т. е. воздействия, обусловленного переводом любой информации в цифровую форму, использованием цифровой информации и переводом ее в другую форму, схематично может быть представлена в следующем виде (рис. 8).

Примером вызова цифровизации, понимаемой в узком смысле, и отвечающей ему угрозы, является ее вызов о создании условий по недопуску несанкционированного использования цифровой информации. В случае невыполнения требований этого вызова возникает угроза появления отрицательных последствий цифровизации, например, в виде цифрового мошенничества, которое может обернуться для соответствующего субъекта воздействия цифровизации потерей его финансовых ресурсов.

Представленная взаимосвязь терминов и понятий, связанных с цифровой информацией (см. рис. 8), определяет целесообразность создания самостоятельной программы управления киберрисками, учитывающей названные особенности их появления и возможной реализации, — Программы управления киберрисками № 3 (рис. 9). Содержанием Программы № 3 является перечень управленческих решений по управлению рисками, связанными с проведением операций, отвечающих цифровизации, понимаемой в узком смысле — с проведением операций перевода любой информации в цифровую форму, с использованием цифровой информации, переводом цифровой информации в любую другую форму ее представления. Программа № 3 становится структурным элементом Комплексной программы управления рисками цифровизации, рассматриваемой как тенденция общественного развития (см. рис. 4).

Цифровая информация, используемая на уровне субъекта и/или объекта воздействия цифровизации конкретного уровня управления определенной сферы жизнедеятельности общества, является частью информации, используемой на уровне этого субъекта и/или объекта воздействия цифровизации, но не являющейся цифровой. Соотношение между объемами и значимостью общей (нецифровой) и цифровой частью информации может быть самым разным.

Цифровизация [понимаемая в узком смысле, т. е. понимаемая по крайней мере как один из процессов трансформации любой информации в цифровую форму, использования цифровой информации, перевода цифровой информации в любую другую форму ее представления] => **кибервызов** [как группа требований, которые необходимо выполнить при работе с цифровой информацией для того, чтобы цифровизация, понимаемая в широком смысле, обеспечила положительное воздействие на определенное направление жизнедеятельности общества] => **киберугроза** [как возможность появления отрицательных последствий, обусловленных невыполнением требований кибервызова при работе с цифровой информацией] => **отрицательное последствие** [как возможный вариант реализации киберугрозы, обусловленной невыполнением требований кибервызова при работе с цифровой информацией] => **киберриск** [как параметр описания возможного отрицательного последствия, связанного с реализацией киберугрозы, обусловленной невыполнением требований кибервызова при работе с цифровой информацией]

Рис. 8. Схема взаимосвязи понятий, отражающих возможные отрицательные последствия невыполнения требований при работе с цифровой информацией

Fig. 8. Scheme of the relationship of concepts reflecting the possible negative consequences of failure to comply with requirements when working with digital information

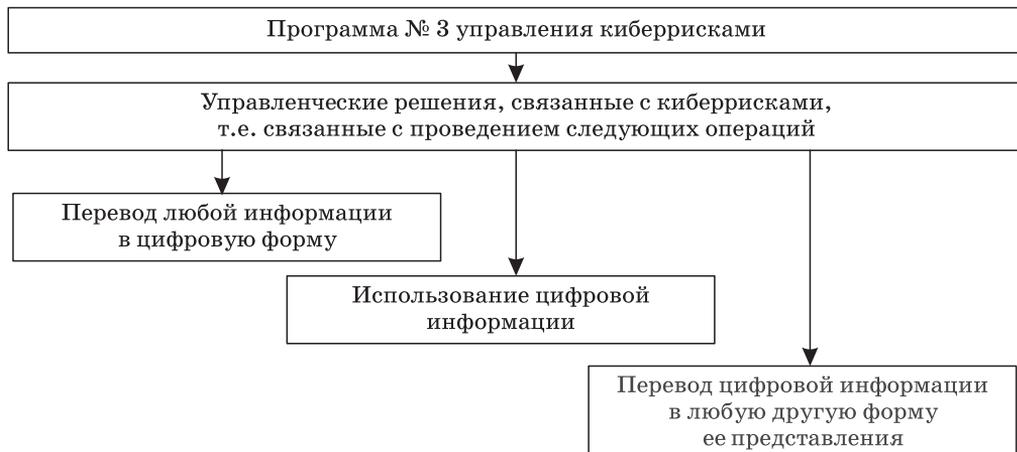


Рис. 9. Структура Программы № 3 управления киберрисками
 Fig. 9. Structure of Cyber Risk Management Program N 3

Именно поэтому наряду с программами управления рисками цифровизации, обусловленными понятием ее в узком смысле (учитываются риски по переводу любой информации в цифру, по использованию цифровой информации и по переводу цифровой информации в любую другую форму), субъект и/или объект воздействия цифровизации, зачастую, формирует общую программу управления информационными рисками¹ — Программу управления информационными рисками № 4, в которую Программа управления цифровыми рисками № 3 входит как обязательный элемент (см. рис. 4).

Далее. Все киберриски условно могут быть разделены на следующие две группы:

- те, появление которых носит случайный характер:
 - ◆ случайная потеря данных,
 - ◆ временная случайная невозможность доступа к данным и/или объекту,
 - ◆ случайный выход из строя объекта и т. д.

Группа этих киберрисков описывает киберугрозу, реализация которой носит случайный характер, например, киберугроза как возможность появления отрицательных последствий цифровизации, связанных со случайной потерей данных. В этом случае вероятность появления отрицательных последствий определяется случайностью потери этих данных;

- те, появление и реализация которых обусловлены преднамеренными причинами. Это:
 - ◆ риски целенаправленного (преднамеренного) действия по
 - нарушению корректного функционирования объекта,
 - краже данных;
 - изменению/подмене данных;
 - утрате/уничтожению данных;
 - внесению или проникновению в компьютеры, серверы, сети и т. д., используемые человеком, отдельной организацией, отраслью или государством,

¹ Информационная безопасность [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/Информационная_безопасность:~:text=Ин-формационная%20безопасность%20-%20практика%20предотвраще-ния,применяется%20вне%20зависимости%20от%20формы:) (дата обращения: 09.03.2024).

различных вирусов, шпионских программ и т. д., которые зачастую сами являются продуктом цифровизации;

- ◆ риски хакерских атак и т. д.

Группа этих киберрисков описывает киберугрозу, реализация которой носит преднамеренный характер, например, киберугроза как возможность появления отрицательных последствий цифровизации, связанных с преднамеренной кражей/уничтожением данных. Естественно, что при этом вероятность появления отрицательных последствий становится более высокой, чем при случайной потере данных.

Факторы формирования и реализации целенаправленных, преднамеренных киберугроз условно могут быть разделены на:

- внешние, влияющие на деятельность отдельной организации, например, фактор использования цифровой информации другими экономическими субъектами, использующие ее недобросовестно;
- внутренние, например, связанные с некорректным поведением своих сотрудников компании.

Обратите внимание!

1. Все киберриски могут быть разделены на две группы — появление которых носит случайный характер (первая группа киберрисков) и появление которых связано с целенаправленными, преднамеренными действиями третьих лиц, направленными на невыполнение требований соответствующих кибервызовов (вторая группа киберрисков).
2. При преднамеренном создании условий для невыполнения требований кибервызова значение вероятности как параметра киберриска, описывающего киберугрозу, будет выше, чем при случайном невыполнении этих требований.

Программы управления процессами цифровизации на уровне отдельного субъекта и/или объекта цифровизации

Как было показано выше, управление процессами цифровизации, рассматриваемой как тенденция общественного развития, оказывающая воздействие на деятельность субъекта и/или на содержание объекта определенного уровня управления конкретной сферы жизнедеятельности общества, может быть реализовано на основе совокупности Программ управления рисками № 1, 2, 3 (№ 1, 2, 4), формирующих Комплексную программу управления рисками (см. рис. 4):

- Программа № 1 управления рисками, обусловленными влиянием цифровизации как тенденции общественного развития на определенное направление жизнедеятельности общества;
- Программа № 2 управления рисками, обусловленными применением основных продуктов цифровизации;
- Программу № 3 управления киберрисками, или Программу управления информационными рисками № 4, часть которой представляет управление киберрисками. Включение в Программу управления рисками цифровизации № 4 помимо управленческих решений, связанных с цифровой информацией (содержание Программы № 3), остается за лицом, принимающим решение (ЛПР). Решение, как правило, формируется с учетом того, что другие информационные риски — не связанные с цифровой информацией, могут быть, во-первых, очень существенными и значимыми сами по себе, и, во-вторых, они либо становятся причиной появления рисков цифровой информации (киберрисков), либо существенно связаны с ними как причина их появления.

Естественно, что все эти Программы управления, направленного на снижение возможных отрицательных последствий цифровизации, формируются субъектом воздействия цифровизации определенного уровня управления конкретной сферы

общественной жизни самостоятельно, например, страховой компанией как субъектом страхового рынка уровня отдельного страховщика. При этом субъект самостоятельно несет свою ответственность как за составление таких программ, их реализацию, так и за результаты внедрения.

Однако необходимо отметить следующее. С учетом все возрастающей значимости процессов цифровизации, а также увеличивающейся потребности в снижении или нивелировании рисков цифровизации, общество берет на себя такую функцию как регулирование процессов цифровизации, понимаемой как в узком, так и в широком смысле.

Регулирование процессов цифровизации

Целью регулирования является разработка правовых норм, определяющих деятельность по работе с информацией (в том числе с цифровой), соблюдение которых становится обязательным для всех тех, для кого эти нормы предназначены. Соблюдение требований нормативных правовых актов, национальных и межгосударственных стандартов¹ заведомо будет означать снижение рисков, обусловленных цифровизацией, рассматриваемой как в широком, так и в узком смысле.

С учетом отмеченного, в каждой из Программ управления рисками № 1, 2, 3 (№ 1, 2, 4) условно можно выделить два блока:

- блок 1 — управленческие решения, за разработку и внедрение которых субъект воздействия цифровизации отвечает самостоятельно, — они охватывают риски цифровизации, нерегулируемые обществом;
- блок 2 — управленческие решения, за разработку и внедрение которых субъект воздействия цифровизации несет ответственность в рамках тех полномочий, которые предусмотрены правовыми нормами по регулируемым рискам. Управленческие решения этого блока охватывают риски цифровизации, регулируемые обществом.

Следует понимать, что регулирование совсем необязательно покрывает все аспекты воздействия цифровизации на деятельность субъекта и/или на содержание объекта воздействия цифровизации определенного уровня управления рассматриваемой сферы жизнедеятельности общества.

Например, в Программе № 1 управления рисками цифровизации, обусловленными влиянием цифровизации как тенденции общественного развития на определенное направление жизнедеятельности общества, под регулирование может попадать деятельность только тех субъектов и/или объектов воздействия цифровизации, которые имеют очень высокую значимость для всего Российского государства, например, деятельность государственных информационных систем².

В Программе № 2 управления рисками, обусловленными применением основных продуктов цифровизации, под нормативное правовое регулирование подпадают риски лишь тех основных продуктов цифровизации, которые, с позиций общества, являются чрезвычайно высокими или таковыми становятся. Примером являются риски нарушения безопасности информационных технологий³. Регулирование ими предполагает соблюдение требований национальных и международных стандартов

¹ [Электронный ресурс]. URL: <https://cppmsp52.ru/assets/mgr/files/doc/2023/08/prilozhenie-6.pdf> (дата обращения: 09.03.2024); [Электронный ресурс]. URL: <https://www.gost.ru/portal/gost/home/standarts/catalognational> (дата обращения: 09.03.2024); [Электронный ресурс]. URL: <https://www.gost.ru/portal/gost/home/standarts/aistandarts> (дата обращения: 09.03.2024).

² [Электронный ресурс]. URL: <https://cppmsp52.ru/assets/mgr/files/doc/2023/08/prilozhenie-6.pdf> (дата обращения: 09.03.2024).

³ [Электронный ресурс]. URL: <https://cppmsp52.ru/assets/mgr/files/doc/2023/08/prilozhenie-6.pdf> (дата обращения: 09.03.2024).

ГОСТ Р ИСО/МЭК 15408-1-2012¹.

Другим примером регулирования рисков, связанных с основными продуктами цифровизации, является обязательность соблюдения требований национальных стандартов по направлению «искусственный интеллект ГОСТ Р 24669-2022»².

В Программе № 3 управления киберрисками регулирование, предусмотренное законодательством, прежде всего присутствует в отношении киберриска нарушения безопасности цифровой информации.

Выбор именно этого киберриска как объекта регулирования обусловлен следующим. С одной стороны, любой киберриск может быть описан значениями двух параметров — вероятность его реализации и размер возможного ущерба. При этом реализация этого киберриска в общем случае должна иметь случайный характер, что должно находить отражение в значении вероятности реализации этого риска. С другой стороны, появление и реализация киберриска нарушения безопасности цифровой информации зачастую связаны с целенаправленными, противоправными действиями в форме компьютерных атак, что очень резко повышает значение вероятности реализации этого риска. Именно поэтому управление данным риском является чрезвычайно важным не только для отдельного субъекта и/или объекта воздействия цифровизации, но и для всего общества в целом³. Этой причиной и вызвано регулирование риска нарушения безопасности цифровой информации, реализуемого на базе компьютерных атак⁴. Оно осуществляется на базе нормативных правовых актов в области создания государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (указы Президента Российской Федерации, приказы ФСБ России, документы по субсидированию на создание центров ГосСОПКА, постановления Правительства Российской Федерации, приказы Минцифры России). Регулирование направлено на борьбу с кибератаками, т. е. направлено на предотвращение или уменьшение ущерба, обусловленного преднамеренными, противоправными действиями третьих лиц.

Так как киберриски могут рассматриваться вместе с другими связанными с ними информационными рисками, управление ими (киберрисками) может быть частью управления всеми информационными рисками, которые подпадают под регулирование в Программе управления информационными рисками № 4.

Помимо регулирования рисков нарушения безопасности цифровой информации (они могут быть учтены в Программах № 3 и/или № 4), в Программе № 4 под регулирование обязательно подпадают другие риски нарушения информационной безопасности.

Это риски⁵:

- различных субъектов и/или объектов экономики —

¹ [Электронный ресурс]. URL: <https://www.gost.ru/portal/gost/home/standarts/catalognational> (дата обращения: 09.03.2024).

² [Электронный ресурс]. URL: <https://www.gost.ru/portal/gost/home/standarts/aistandarts> (дата обращения: 09.03.2024).

³ См., например: Кибератаки и кибертеррор [Электронный ресурс]. URL: <https://www.forbes.ru/tekhnologii/477173-posti-50-rossijskih-vedomstv-podverglis-kiberatakam> (дата обращения: 09.03.2024); Кибератаки и кибертеррор [Электронный ресурс]. URL: <https://www.forbes.ru/tekhnologii/477173-posti-50-rossijskih-vedomstv-podverglis-kiberatakam> (дата обращения: 21.04.2023); Киберпреступления [Электронный ресурс]. URL: <https://www.calltouch.ru/blog/kiberbezopasnost-v-2022-godu-novye-metody-prestupnikov/> (дата обращения: 06.04.2023).

⁴ [Электронный ресурс]. URL: <https://cppmsp52.ru/assets/mgr/files/doc/2023/08/prilozhenie-6.pdf> (дата обращения: 09.03.2024).

⁵ [Электронный ресурс]. URL: <https://cppmsp52.ru/assets/mgr/files/doc/2023/08/prilozhenie-6.pdf> (дата обращения: 09.03.2024).

- ◆ государственных информационных систем (федеральные законы Российской Федерации, указы Президента Российской Федерации, постановления Правительства Российской Федерации, приказы и иные документы федеральных органов исполнительной власти Российской Федерации),
- ◆ автоматизированных систем управления технологическим процессом (федеральные законы Российской Федерации, постановления Правительства Российской Федерации, приказы ФСТЭК России),

а также

- персональных данных (федеральные законы Российской Федерации, указы Президента Российской Федерации, постановления Правительства Российской Федерации, приказы и иные документы федеральных органов исполнительной власти Российской Федерации),
- биометрических персональных данных (федеральные законы Российской Федерации, постановления Правительства Российской Федерации, приказы Минцифры России).

Программа № 4 также может содержать управленческие решения и меры, связанные с определенным видом деятельности или с каким-либо его аспектом, которые, за счет управления риском нарушения информационной безопасности, должны обеспечивать необходимый уровень информационной безопасности, в том числе безопасности цифровой информации. Такое регулирование в настоящее время существует в отношении рисков¹:

- в области криптографии (постановления Правительства Российской Федерации, приказы ФСБ России),
- использования электронной подписи (федеральные законы Российской Федерации, постановления Правительства Российской Федерации, приказы ФСБ России, приказы Минцифры России),
- сертификации средств защиты информации (постановления Правительства Российской Федерации, приказы ФСТЭК² России, иные документы по сертификации),
- лицензирования деятельности по технической защите конфиденциальной информации (федеральные законы Российской Федерации, постановления Правительства Российской Федерации, приказы ФСТЭК России),
- в области образования специалистов по информационной безопасности и иных специалистов (приказы Минобрнауки России, приказы Минтруда России),
- банковской деятельности (положения Банка России, указания Банка России, стандарты Банка России, рекомендации по стандартизации, методические рекомендации).

Обратите внимание!

1. Регулирование процессов цифровизации охватывает:
 - те или иные аспекты таких характеристик направления воздействия цифровизации, как рассматриваемая сфера жизнедеятельности общества, субъект и/или объект воздействия цифровизации; уровень управления субъектом и/или объектом рассматриваемой сферы;
 - особенности различных применяемых продуктов цифровизации;
 - содержание операций по цифровизации, понимаемой в узком смысле, т. е. содержание операций перевода любой информации в цифровую форму, использования цифровой информации, перевода цифровой информации в любую другую форму.
2. Регулирование киберрисков нарушения безопасности цифровой информации зачастую является частью регулирования вопросов обеспечения всей информационной безопасности.

¹ [Электронный ресурс]. URL: <https://cppmsp52.ru/assets/mgr/files/doc/2023/08/prilozhenie-6.pdf> (дата обращения: 09.03.2024).

² Федеральная служба по техническому и экспортному контролю.

Особенностью содержания всех действующих в настоящее время нормативных правовых норм, стандартов и сертификатов, связанных с цифровизацией, является то, что они формулируют разные требования к информации различных субъектов и/или объектов экономики и видов их деятельности в зависимости от значимости и важности этой информации. Выполнение этих требований по смыслу означает проведение превентивных мероприятий, направленных на снижение рисков нарушения информационной безопасности, в том числе на снижение рисков нарушения безопасности цифровой информации.

Выводы

Термин «цифровизация» в настоящее время используется в узком и в широком смысле. В узком смысле цифровизация представляет собой процессы перевода любой информации в цифровую форму, использования цифровой информации, перевода цифровой информации в любую другую форму ее представления. В широком смысле цифровизация представляет собой тенденцию общественного развития, проявляющуюся через определенное направление жизнедеятельности общества, описываемое конкретной сферой общественной жизни, субъектом и/или объектом воздействия цифровизации, уровнем управления, на котором воздействие цифровизации проявляется.

Цифровизация будет оказывать положительное воздействие на рассматриваемое направление общественного развития лишь в том случае, если будут выполняться ее требования, выставляемые обществу как вызов. В случае, когда эти требования не выполняются, возникает угроза появления отрицательных последствий влияния цифровизации, которая может быть представлена риском. Последний описывается вероятностью реализации угрозы — вероятностью появления отрицательного последствия и размером возможного ущерба.

Решение задачи появления, уменьшения или нивелирования отрицательных последствий цифровизации возможно на основе построения и реализации Комплексной программы управления цифровизацией, включающей Программу № 1 управления рисками, характерными для рассматриваемого направления воздействия цифровизации на общественную жизнь; Программу № 2 управления рисками, характерными для используемых при этом продуктов цифровизации; Программу № 3 управления цифровыми рисками (киберрисками). В ряде случаев вместо Программы № 3 или в дополнение к ней в Комплексную программу управления цифровизацией может входить Программа управления информационными рисками № 4.

Высокая значимость проблемы снижения киберрисков нарушения безопасности цифровой информации и других рисков нарушения информационной безопасности приводит к целесообразности регулирования вопросов, связанных с решением этой проблемы и, как следствие, приводит к обязательному выполнению требований нормативных правовых актов, национальных и межгосударственных стандартов в области информационной безопасности.

Обязательное выполнение требований нормативных правовых актов, национальных и межгосударственных стандартов в области информационной безопасности приводит к тому, что в структуре Программ № 1–4, формирующих Комплексную программу управления процессами цифровизации, обязательно присутствует 2 блока: первый включает управленческие решения и меры, разрабатываемые субъектом воздействия цифровизации самостоятельно, второй — управленческие решения и меры, предусмотренные государственным регулированием.

Литература

1. Халин В. Г., Чернова Г. В. Цифровизация и киберриски // Управленческое консультирование. 2023. № 7. С. 28–41.
2. Цифровая трансформация экономики: тенденции, поведение акторов, модели процессов : монография / Д. Н. Верзилин, А. А. Волкова, С. А. Калайда [и др.] / под ред. В. В. Трофимова, С. И. Шаныгина. СПб. : Изд-во СПбГЭУ, 2023. 283 с.

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

Калайда Светлана Александровна, доцент кафедры управления рисками и страхования Санкт-Петербургского государственного университета (Санкт-Петербург, Российская Федерация), доктор экономических наук, доцент; s.kalayda@spbu.ru

References

1. Khalin V. G., Chernova G. V. Digitalization and cyber risks // Administrative consulting [Upravlencheskoe konsul'tirovanie]. 2023. N 7. P. 28–41.
2. Digital transformation of the economy: trends, behavior of actors, process models. Monograph / D. N. Verzhilin, A. A. Volkova, S. A. Kalajda [et al.] / ed. V. V. Trofimov, S. I. Shanygin. Saint Petersburg : Publishing house of Saint Petersburg State Economic University, 2023. 283 p.

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

Svetlana A. Kalayda, Associated Professor of the Chair of Risk management and Insurance of Saint-Petersburg State University (Saint-Petersburg, Russian Federation), Doctor of Science (Economic), Associated professor; s.kalayda@spbu.ru