## МАТЕМАТИЧЕСКИЕ И ИНСТРУМЕНТАЛЬНЫЕ МЕТОДЫ ЭКОНОМИКИ

УДК 330.341
DOI: 10.26456/2219-1453/2022.4.106–123

# РИСКИ И УГРОЗЫ ЦИФРОВИЗАЦИИ ЭКОНОМИКИ ДЛЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ БЕЛАРУСЬ

**В.Б. Криштаносов**

УО «Белорусский государственный технологический университет», г. Минск, Республика Беларусь

Целью статьи является обнаружение основных подходов к оценке рисков, связанных с внедрением современных цифровых технологий (Интернет Вещей (IoT), анализ больших данных (BDA), искусственный интеллект (AI), Блокчейн, облачные технологии) и бизнес-операционные (производственные) системы на уровне ключевых национальных отраслей. Научная новизна представлена разработанной методологией расчета показателя интегрального отраслевого цифрового риска; выделением основных факторов, определяющих уровень и глубину распространения рисков и угроз цифровизации для экономики страны; наиболее уязвимых производственных систем с точки зрения киберугроз, риски взлома которых потенциально могут нанести максимальный урон деятельности предприятий.

***Ключевые слова:*** *цифровизация, риски и угрозы, модели оценки рисков цифровизации.*

## СОСТОЯНИЕ ПРОБЛЕМЫ

Цифровизация несет риски и угрозы для национальной безопасности Республики Беларусь, влияя в различной степени на ключевые отрасли экономики страны. Идентификация и классификация рисков цифровизации, их вероятности и объема негативного воздействия на разные уровни экономики являются необходимым условием для разработки системного подхода к нивелированию цифровых угроз и обеспечения стабильного функционирования экономической системы страны. Малый открытый характер экономики Республики Беларусь предопределяет ее вовлеченность в международные экономические отношения, подверженность соответствующим тенденциям и технологическим инновациям. Вместе с тем особенности структуры и функционирования хозяйственного комплекса и роль государства в экономики страны формируют национальную специфику комплекса цифровых рисков и угроз.

Представляется, что к основным факторам, определяющим уровень и глубину распространения рисков и угроз цифровизации для экономики страны, в настоящее время возможно отнести следующие:

А. Финансово-экономические:

1. Наличие жестких ограничений в сфере располагаемых финансовых ресурсов для внедрения новых технологий в сфере

цифровизации, включая современные технологии киберзащиты. Сложность, высокая стоимость и необходимость систематических обновлений технологических решений выступают в качестве барьера для их адаптации на низовом уровне.

2. Нарастающее санкционное давление на внутреннем и внешних рынках как для традиционных национальных отраслей, так и в инновационных сферах предоставления услуг и высокотехнологического производства, меняет структуру международной торговли, сокращает приток финансовых ресурсов на отраслевом уровне.

Б. Технологические:

1. Низкий уровень использования ИТ технологий и соответствующих компетенций на уровне предприятий. По данным Министерства статистики Беларуси, объем промышленного производства сегмента высокотехнологичного производства в 2020 г. составил лишь 3,3 % (среднетехнологического – 50,3 %). Соответственно предприятия на данном технологическом уровне не готовы к новым цифровым вызовам и по мере внедрения современных ИТ технологий без соответствующего внимания и компетенций в отношении кибербезопасности будут сталкиваться с нарастающими киберрисками.

2. Неразвитая инновационная инфраструктура, которая представлена, главным образом, Парком высоких технологий и индустриальным парком «Великий камень». Внутренние инвестиционные (венчурные) ресурсы для инновационного производства носят ограниченный характер, их стоимость на внутреннем кредитном рынке чрезвычайно высока.

3. Отсутствие актуальных шаблонов (и соответствующих стандартов) комплексного эффективного внедрения цифровых технологий при модернизации предприятий традиционных отраслей экономики страны.

4. Недостаточная защищенность внутренней ИКТ инфраструктуры перед угрозой киберпреступности, что подтверждено низким рейтингом страны в Глобальном индексе кибербезопасности ITU [1]. Отставание от ЕС, России в формировании современной институциональной экосистемы киберзащиты генерируют дополнительные риски обеспечения конфиденциальности и безопасности коммерческой информации, персональных данных, устойчивости критической инфраструктуры к внешним и внутренним угрозам.

В. Управленческие:

1. Недостаточная поддержка и понимание необходимости внедрения цифровых технологий на уровне руководства предприятий и организаций. Отсутствие оценочных показателей цифровизации предприятий и отраслей в рамках государственной промышленной, инвестиционной и кадровой политик оказывает демотивирующее влияние на принятие соответствующих управленческих решений, как в разрезе внедрения инновационных цифровых технологий, так и обеспечения кибербезопасности.

2. Возрастающее значение взаимодействия на уровне государственно-частного партнерства с учетом отсутствия достаточных компетенций для эффективного внедрения цифровых технологий в сферы госуправления как на уровне ограниченного кадрового состава ИТ специалистов и аналитиков, так и отсутствия системности и концептуальности в подходах к формированию актуальных задач для реализации цифровых проектов.

3. Сложность межведомственного и межотраслевого взаимодействия при реализации комплексных национальных проектов цифровизации экономики.

Г. Социально-образовательные. Отсутствие системного подхода к подготовке, обучению населения использованию ИТ технологий как на уровне государства, так и предприятий традиционных отраслей. Цифровая грамотность населения, а именно базовые навыки программирования, Big Data Analytics способствуют внедрению цифровых технологий. В Республике Беларусь, по данным ОЭСР [2], не более 25 % населения Беларуси обладает, по крайней мере, «стандартными» навыками[1], что составляет только половину показателя, характерного для развитых экономик мира.

Д. Политические. В контексте текущей политико-экономической ситуации в стране возрастает вероятность осуществления хакерских атак или DDoS-атак во имя «социальной справедливости» и\или «возмездия» в отношении отдельных организаций, государственных институтов, а также инсайдерские угрозы, создаваемые недовольными сотрудниками, включают использование доступа к внутренней системе и учетным данным или «социальную инженерию» для получения конфиденциальной информации либо нарушения стабильного функционирования ИТ систем организаций.

## МЕТОДЫ И РЕЗУЛЬТАТЫ

Для управления рисками кибербезопасности требуется четкое понимание специфики функционирования, как отраслей, так и отдельных предприятий, поскольку риски, приоритеты и системы каждой организации имеют свои особенности. При этом если лидирующий в сфере изучения цифровых инноваций международный исследовательский центр McKinsey для расчета потенциала угроз использует матричную сетку рисков, Boston Consulting Group предлагает расчетную функцию, включающую частоту и влияние успешных кибератак относительно ожидаемых киберпотерь касательно конкретного предприятия. Модель McKinsey имеет абстрактный характер и охватывает весь спектр возможных угроз (как природного, так и техногенного характера) для стабильного функционирования предприятий без учета структуры экономики и

[1] Стандартные навыки предполагают осуществление следующих четырех компьютерных видов деятельности: использование базовой арифметической формулы в электронной таблице; подключение и установка новых устройств; создание электронных презентаций с помощью программного обеспечения для презентаций; и поиск, загрузка, установка и настройка программного обеспечения.

национальных особенностей. Модель Boston Consulting Group ориентируется, в первую очередь, на расчет потерь, вызванных кибератаками, и фокусируется на микроуровне отдельных организаций.

Министерством связи и информатизации Республики Беларусь, ОАО «Гипросвязь» разработана методика оценки уровня цифровизации предприятий и отраслей [3], согласно которой в рамках бизнес-аудита рассчитывается: «…обобщенный показатель как функции от множества взвешенных частных показателей цифровизации каждого бизнес-процесса.

$$Ц = \frac{\sum_{1}^{n} \alpha_i Ц_i}{\sum_{1}^{n} \alpha_i} \left| \begin{array}{l} K_i \geq K_{тр} \\ A_i \geq A_{тр} \\ И_i \geq И_{тр} \end{array} \right.$$

где *Ц – показатель уровня цифровизации предприятия (организации); Цi – показатель уровня цифровизации i-го бизнес-процесса; αi – вес i-го бизнес-процесса в деятельности предприятия (организации); Ki , Ai , Иi – уровни компьютеризации, автоматизации и информатизации i-го бизнес-процесса; Kтр, Aтр, Итр – требуемые уровни компьютеризации, автоматизации и информатизации».*

С точки зрения потенциальных рисков и угроз, связанных с внедрением цифровых технологий, данная формула требует корректировки ввиду того, что среднее квадратичное значение частных показателей цифровизации не отражает уровень потенциального ущерба в случае нарушения устойчивости функционирования системы и его вероятность. В этой связи представляется целесообразным использование следующей классификации уровней цифровизации предприятий / отраслей в разрезе не только «цифрового прогресса», но и соответствующего комплекса цифровых рисков и угроз: 0 – цифровизация отсутствует, соответственно ИКТ риски функционирования предприятия/отрасли практически отсутствуют; 1 – уровень «автоматизация» затрагивает ключевые производственные процессы, предполагает агрегирование Big Data в режиме реального времени, алгоритмизацию отдельных операций и низкий уровень взаимодействия внутренней цифровой среды с внешним контуром. Цифровые риски имеют ограниченный характер возникновения, связаны с ошибками программного продукта, настройками/обновлениями, а также относительно простой механизм выявления и корректировки. Умышленное «заражение»/ нарушение стабильного функционирования цифровой среды предприятия возможно только изнутри системы и является маловероятным; 2 – уровень «кибернетизация» предполагает комплексное внедрение элементов автоматизации в производственные и бизнес-процессы, включая агрегирование цифровых данных (использование систем управления мастер-данными) для оптимизации производственных процессов, формирование цифровых активов предприятия. Риски аналогичны уровню «автоматизация» с поправкой на возможный более масштабный ущерб в случае нарушения стабильного функционирования цифровых систем, и целостности цифровых данных. Потери цифровых данных означают потери цифровых активов организаций; 3 – уровень «базовая интеллектуализация» предполагает выстраивание двустороннего обмена данных цифровой инфраструктуры предприятия с использованием технологий BDA и IoT.

Цифровые данные агрегируются машинами, которые самостоятельно принимают оперативные производственные и управленческие решения. Уровень проникновения цифровых технологий высокий. Внешний контур цифрового взаимодействия представлен Cloud технологиями. Уровень рисков увеличивается за счет автоматизации принятия решения (риски сбоев и ошибки алгоритмов могут привести к поломке технологического оборудования и серьезным финансовым потерям на уровне предприятия) и появления внешнего контура (возникают риски потери цифровых данных: персональных и коммерческой информации); 4 – уровень «цифровизация» предполагает концептуализацию соответствующей сферы в рамках «новой экономики 2.0»[1], создание экосистемы предприятия, включающей оцифрованные производственные и бизнес-процессы, автоматизацию значительного объема управленческих решений. Для данного уровня характерно комплексное применение современных ИКТ технологий на всех этапах производства, продажи, логистики и управления, и соответственно максимальная концентрация цифровых рисков на всех указанных этапах.

Экстраполяция данной методики оценки уровня цифровизации предприятий/отраслей с учетом возможных цифровых рисков в отношении текущей структуры экономики Республики Беларусь позволяет сформировать следующую матрицу (см. Приложение 1).

«Эмпирические оценки рисков и угроз по основным системам управления и интеллектуализации показывают, что наиболее уязвимыми системами с точки зрения киберугроз, риски взлома которых потенциально могут нанести максимальный урон деятельности предприятий, являются: PDM, SCADA, CAM, MES, BPM, системы AI, IoT и роботизированные устройства конвейера. Кроме того, анализ цифровых рисков по методологии CIA позволяет в разрезе современных отраслей экономики Республики Беларусь, в динамике внедрения цифровых концепций и технологий, провести оценку потенциальных рисков и угроз цифровизации» [4].

В качестве критерия уровня цифровизации, представляется целесообразным принять расчетный показатель цифровизации на основе данных межотраслевого баланса (см. Приложение 2). Как показывает анализ данных приложения 2, максимальный показатель цифровизации (четвертый уровень) ожидаемо характеризует сектор ИКТ (величина 6,44), третий уровень – оптовую и розничную торговлю (3,03), второй уровень – финансовую и страховую деятельность (1,71) и государственное управление (1,27). Первый уровень характерен для всех оставшихся секторов экономики за исключением сельского хозяйства (0,04) и нефтехимии (0,09).

[1] «Новая экономика 2.0» – авторская концепция, характеризующая среднесрочный этап формирования цифровой экономики, для которого характерны формирование новой экономической среды на основе платформизации и алгоритмизации, экономическими механизмами и институтами, комплексными цифровыми концепциями производства и управления

Обращает внимание отсутствие корреляции в оценке цифровизации и технологичности в отношении таких отраслей как: производство вычислительной, электронной и оптической аппаратуры и фармацевтика (высокий уровень технологичности и первый уровень цифровизации), машиностроение (среднетехнологический высокий уровень и первый уровень цифровизации); нефтехимия (среднетехнологический высокий уровень и начальный уровень цифровизации). Отсутствие данной тождественности может свидетельствовать об относительном отставании данных белорусских отраслей от общемировых трендов в разрезе внедрения цифровых технологий на уровне секторов и различий в методологии оценки уровней «технологичности» и «цифровизации». Преодоление данного отставания требует масштабной системной модернизации на уровне отраслей и предприятий с целью повышения технологичности производства, снижения затрат и соответствующего роста конкурентоспособности продукции.

Наибольшую динамику роста объем расходов на ПО относительно среднего показателя (241,09 %) показывают здравоохранение (348,1 %), образование (296,73 %) и оптовая и розничная торговля (296,61%). Более низкими темпами относительно среднего показателя растут сектора «производство вычислительной, электронной и оптической аппаратуры» (142,86 %), «финансовая и страховая деятельность» (150,74 %), энергетика (152,14 %).

Отмечается поступательное за период 2016–2019 гг. замедление темпов роста расходов на программное обеспечение по ключевым отраслям с 156,27 % в 2017 г. до 117,62 % в 2019 году. Вместе с тем, за указанный период средний показатель расходов на ПО в ключевых отраслях экономики страны поступательно рос – с 0,43 % в 2016 г. до 0,75 % в 2019 г. Разнонаправленность данных трендов может свидетельствовать о положительном влиянии цифровизации на относительное снижение затрат отраслей экономики страны.

Агрегирование данных о потенциальных рисках и угрозах цифровизации на уровне конкретных белорусских отраслей с учетом возможных каскадных эффектов позволило сформировать следующую матрицу и рассчитать средневзвешенный уровень потенциальных угроз (см. Приложение 3).

Для комплексной оценки цифровых рисков на отраслевом уровне представляется целесообразным учитывать ряд факторов, определяемых следующими показателями:

1) уровень значимости отрасли для национальной экономики: доля отрасли в общем объеме экспорта (%), доля в среднесписочной численности работников (%);

2) текущий уровень цифровизации (в диапазоне уровней от 1 до 3) и технологичности отрасли (от низкого до высокого):

3) степень потенциала глубины цифровых рисков и угроз и каскадного распространения ущерба в случае кибератаки конкретной отрасли: уровень «каскадности» угроз и рисков (по шкале от 1 до 3), наличие в отрасли критической инфраструктуры и соответствующих рисков, средневзвешенный уровень потенциальных цифровых угроз (табл. 4, 5, см. Приложение). С учетом

данных факторов, представляется возможным отобразить интегральный уровень риска отрасли следующим образом:

$$У_и = О_ц \times К_т \times С_р \times Кас_э \times К_к + (Д_э + Д_р) / 100,$$

где *$У_и$ – интегральный отраслевой уровень риска, $О_ц$ – оценочный текущий уровень цифровизации, $К_т$ – коэффициент уровня технологичности, $Кас_э$ – коэффициент потенциала каскадного эффекта, $Д_э$ – доля в экспорте, $Д_р$ – доля в среднесписочной численности работников, $К_к$– коэффициент наличия в отрасли объектов критической инфраструктуры, $С_р$ – средневзвешенный уровень потенциальных цифровых угроз.*

С учетом данной модели возможно провести расчет уровня потенциальных угроз для ключевых областей экономики Республики Беларусь (см. Приложение 4).

Вместе с тем, по мере внедрения цифровых технологий, создания новых высокотехнологических производств и, возможно, новых отраслей, структура экономики Беларуси будет трансформироваться, приближаясь к концепции «новой экономики 2.0» – к 4 стадии в рамках предложенной классификации уровней цифровизации. Соответственно вырастает количество потенциальных угроз, которые будут носить комплексный характер и не только будут связаны с кибератаками. Следует отдельно выделить экономические и социальные риски и угрозы, которые будут генерироваться внедрением высокотехнологических цифровых концептов, а также потенциал каскадного эффекта распространения рисков (см. Приложение 5).

С учетом оценки данных Приложения 2, включая средневзвешенный уровень потенциальных цифровых угроз, вероятности их каскадного распространения, оценочных показателей экономического и социального влияния внедрения цифровых концептов, представляется возможным отобразить величину интегрального отраслевого цифрового риска следующим образом:

$$У_и = О_ц \times С_р \times Кас_э + (О_э + О_с) / 100,$$

где *$У_и$ – интегральный отраслевой уровень риска, $О_ц$ – оценочный текущий уровень цифровизации равный 4, $Кас_э$ – коэффициент потенциала каскадного эффекта, $О_э$ – оценочный показатель экономического влияния, $О_с$ – оценочный показатель социального влияния, $С_р$ – средневзвешенный уровень потенциальных цифровых угроз.*

С учетом данной модели представляется возможным произвести расчет уровня потенциальных угроз для ключевых областей экономики Республики Беларусь (см. Приложение 6)

## НАУЧНАЯ НОВИЗНА

Как свидетельствуют результаты оценки, при текущих экономических условиях, в разрезе поступательного внедрения цифровых технологий, в зоне наибольшего риска и растущих угроз (≥3,4) оказываются такие сектора как: ИКТ, финансовая и страховая деятельность, государственное управление, оптовая и розничная торговля, производство электрооборудования, машиностроение и фармацевтика.

Риски, связанные с концепциями «новой экономики 2.0», имеют схожий характер угроз (из-за близости 3 и 4 уровней цифровизации), однако больший каскадный эффект и макроэкономические, социальные последствия для страны. Наиболее уязвимыми из них являются: «Smart City», «Industry 4.0», «Smart Grid», «E-Government», «FinTech».

Потери, связанные с рисками цифровизации, включают такие составляющие как: прямые убытки (финансовые убытки, материальный ущерб, смерть и телесные повреждения); репутационный ущерб (в особенности в случае потери личных цифровых данных клиентов); юридическую ответственность и нормативные штрафы; а также (опционально) негативное влияние на цены акций атакованного предприятия.

Вместе с тем, важно отметить, что в белорусских реалиях не представляется целесообразным дифференцированное выделение макроэкономических рисков: рыночного и системного. *Рыночный риск* (потеря рыночной стоимости компании) в условиях доминирования в промышленном секторе экономики государственных предприятий и определяющей роли государства в регулировании ключевых отраслей может быть исключен из рассмотрения как маловероятностный. Как показывает практика, государство, одновременно выступая в качестве собственника и регулятора, не допускает банкротства системообразующих (флагманских) предприятий, предоставляя им финансовые ресурсы на льготных условиях. *Системный риск* (вероятность возникновения на уровне компании такого события, которое может спровоцировать нестабильность или обрушить всю отрасль или экономику) учитывается, в первую очередь, в разрезе выделения критически важной инфраструктуры и вероятности возникновения каскадных эффектов.

## ЗАКЛЮЧЕНИЕ

Таким образом, для оценки рисков и угроз цифровизации экономики в контексте национальной экономической безопасности Республики Беларусь представляется целесообразным учитывать комплексные факторы, включая финансово-экономические, технологические, управленческие, социально-образовательные и политические.

Предложена модель расчета рисков цифровизации как для традиционных отраслей белорусской экономики, так и в рамках цифровых концепций «новой экономики 2.0». Авторская модель носит более комплексный, прикладной характер, применимый как на уровне предприятий, так и отраслей, учитывает особенности сложившейся в стране экономической системы относительно моделей, используемых, например McKinsey и Boston Consulting Group. Элементом предложенной расчетной модели является показатель уровня цифровизации отрасли, выведенный на основе данных межотраслевого баланса. Отмечено отсутствие корреляции в оценке цифровизации и технологичности в отношении ряда отраслей, что может свидетельствовать об относительном отставании данных белорусских отраслей от общемировых трендов в разрезе внедрения цифровых технологий на уровне секторов и различий в методологии оценки уровней «технологичности» и «цифровизации».

## Список литературы


1. Global Cybersecurity Index 2020 // International Telecommunication Union (ITU). – Geneva: ITU, 2021. – 172 p. – URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (date of access: 13.11.2021).
2. Beyond COVID-19 Advancing Digital Business Transformation in the Eastern Partner Countries / Organisation for Economic Co-operation and Development. – 2021. – 116 p. – URL: https://www.oecd.org/eurasia/Covid19_%20Advancing%20digital%20business%20transformation%20in%20the%20EaP%20countries.pdf (date of access: 15.11.2021).
3. Оценка уровня цифрового развития организаций, отраслей и функциональный отраслей: Министерство связи и информатизации Республики Беларусь, ОАО «Гипросвязь». – 2019. – Режим доступа: https://www.mpt.gov.by/sites/default/files/spravochno_1_kratkoe_opisanie_metodiki_ocenki_urovnya_cifrovizacii.pdf (дата обращения: 25.09.2019).
4. Криштаносов В. Б. Угрозы и риски цифровой экономики на секторальном уровне // Труды БГТУ. 2022. № 1. С. 28–52.



*Об авторе:*

КРИШТАНОСОВ Виталий Брониславович – кандидат экономических наук, докторант, кафедра менеджмента, технологий бизнеса и устойчивого развития, УО «Белорусский государственный технологический университет», e-mail: krishtanosov@mail.ru, ORCID: 0000-0002-1146-368X, Spin-код: 3207-4374


## RISKS AND THREATS OF THE ECONOMIC DIGITALIZATION FOR THE NATIONAL SECURITY OF THE REPUBLIC OF BELARUS


**V.B. Krishtanosov**

UO “Belarusian State Technological University”, Minsk, Republic of Belarus



The author identifies the main approaches to the risk assessment associated with the introduction of modern digital technologies, including general technological components (IOT, BDA, AI, Blockchain, Cloud) and business operating (production) systems at the level of certain sectors and the branches. There were highlighted the main factors that determine the level and depth of the spread of risks and threats of digitalization for the country's economy, as well as the most vulnerable production systems in terms of cyber threats, the risks of hacking which can potentially cause maximum damage to the activities of enterprises, are identified. There was a methodology for assessing digital risks at the industry level and within the digital concepts of the “new economy 2.0” proposed. There have been industries and sectors of the country's economy most vulnerable to digital risks identified. It has been methodology for calculating the indicator of the integral industry digital risk developed.



***Keywords:*** *digitalization, risks and threats, digitalization risk assessment models.*



*About the author:*

KRISHTANOSOV Vitalij Bronislavovich – Candidate of Economic Sciences, Doctoral Student, Department of Management, Business Technologies and Sustainable Development, Belarusian State Technological University, e-mail: krishtanosov@mail.ru, ORCID: 0000-0002-1146-368X, Spin-код: 3207-4374

Приложение 1

Составные цифровые (концептуальные) элементы цифрового развития предприятий/отраслей (разработано автором) [4]

| № | Значение показателя уровня цифровизации | Промышленность наличие цифровых систем | Финансовый сектор | Энергетика | Сельское хозяйство | Строительство | Транспорт и логистика | Торговля | Здравоохранение | Образование | Государственное управление |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | 0 | - | - | - | - | - | - | - | - | - | - |
| 1 | [0..1] | автоматический цифровой сбор данных в режиме реального времени | | | | | | | | | |
| 2 | [1..2] | APS, MRP/MRPII CAD, CAE, CAPP, SSM, CRM, PLC, PLM, CALS, SCADA, CAM, KM, TQM, BPM, MDM | SSM, CRM, KM, MDM, Rob/CRob | SSM, CRM, SCADA, CAM, KM, BPM, MDM | PLC, CALS, AITS, MDM | APS, MRP/MRPII, KM, BPM, MDM | APS, SSM, CRM, KM, BPM, MDM | APS, SSM, CRM, PLC, CALS, KM, MDM | KM, MDM | KM | SSM, CRM, KM, MDM |
| 3 | [2..3] | BDA, PDM, MES, Blockchain, 3D, ERP, AI, IoT, Cloud, Rob/CRob, BIM | BDA, Blockchain, ERP, AI, RPA, Cloud | BDA, Blockchain, ERP, IoT, Cloud, BIM | IoT | IoT, Rob, BIM, Rob/CRob | BDA, ERP, IoT, Cloud, Rob/CRob | BDA, ERP, Cloud | BDA, AI, IoT, Cloud | BDA, Cloud | BDA, Blockchain, AI, IoT, Cloud |
| 4 | [3..4] – приближение к цифровым концепциям | I4.0 | FinTech | Smart Grid | A4.0 | Smart Construction | Smart Supply Chain | E-Commerce | Telemedicine | EduTech | E-Government |

«3D-принтеры – Аддитивные технологии и системы; AITS – система идентификации, регистрации, прослеживаемости животных и продукции животного происхождения; APS (Advanced Planning & Scheduling) – система усовершенствованного планирования; BDA (Big Data Analytics) – аналитика больших данных, а также средства моделирования и анализа производственных и бизнес-процессов; BIM (Building Information Modeling) – системы информационного моделирования в области промышленного и гражданского строительства; Blockchain – децентрализованная система хранения информации; BPM (Business Perfomance Managment) – процессное управление организацией; CAD, CAE (ComputerAided Design; Computer-Aided Engineering) – системы цифрового проектирования и моделирования; CAPP (Computer-Aided Process Planning) – системы планирования производства; Cloud – облачные технологии; ERP (Enterprise Resource Planning) –информационная система модулей планирования и управления ресурсами предприятия; IoT – Интернет вещей KM (Knowledge Management) – управление знаниями и навыками на различных уровнях управления; MDM (Master Data Management) – система управления мастер-данными; MES (Manufacturing Execution System) – производственные исполнительные интеллектуальные информационные системы; MRP/MRPII (Material Requirements Planning, manufacturing resource planning) – системы планирования потребности в материалах/ планирования производственных ресурсов, PDM (Product Data Management) – системы управления инженерными данными; PLC /PLM/ CALS (Product Life Cycle, Product Lifecycle Management, Continuous Acquisition and Lifecycle Support) – системы управления жизненным циклом промышленного продукта;; SCADA, CAM (Supervisory Control And Data Acquisition, Computer-Aided Manufacturing) – системы автоматизации цеховых процессов; SSM, CRM – системы продажи и управления сервисом; SCM (Supply Chain Management) – системы управления цепочками поставок; TQM (Total Quality Managment) – модули всеобщего управления качеством; Rob/CRob – Робототехнические (роботизированные) системы и автоматы/колороботы; AI – искусственный интеллект и машинное обучение производственных процессов» [4]

Приложение 2

Расчетный показатель цифровизации на основе данных межотраслевого баланса за период 2016-2019 гг. (разработано автором)

| Сектор экономики | Расчетный показатель цифровизации | | | | Средний показатель цифровиза-ции | Уровень цифровиза-ции[1] | Рост объема затрат на ПО за 2016-2019, % | Изменение объема затрат на ПО к предыдущему периоду, % | | | Справочно уровень технологичности (для промышлен)[2] |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | 2016 | 2017 | 2018 | 2019 | | | | 2017 | 2018 | 2019 | |
| *Промышленность*, в т.ч. | | | | | | | | | | | |
| горнодобывающая | 0,74 | 1,00 | 0,88 | 0,90 | 0,88 | 1 | 163,62 | 152,45 | 101,06 | 106,21 | н |
| *Обрабатывающая,* в т.ч. | | | | | | | | | | | |
| машиностроение | 0,11 | 0,13 | 0,12 | 0,14 | 0,13 | 1 | 216,53 | 146,71 | 122,22 | 120,75 | с |
| легкая промышленность | 0,23 | 0,27 | 0,34 | 0,36 | 0,30 | 1 | 199,96 | 138,06 | 138,39 | 104,65 | н |
| пищевая | 0,25 | 0,34 | 0,38 | 0,44 | 0,35 | 1 | 227,95 | 151,32 | 123,90 | 121,58 | н |
| деревообработка | 0,17 | 0,20 | 0,20 | 0,21 | 0,20 | 1 | 226,12 | 149,99 | 126,31 | 119,36 | н |
| нефтехимия | 0,07 | 0,09 | 0,10 | 0,11 | 0,09 | н | 209,41 | 155,74 | 127,00 | 105,87 | с |
| фармацевтика | 0,28 | 0,41 | 0,42 | 0,46 | 0,39 | 1 | 219,98 | 166,64 | 112,13 | 117,73 | в |
| металлургия | 0,09 | 0,13 | 0,12 | 0,13 | 0,12 | 1 | 215,94 | 164,96 | 110,74 | 118,20 | н |
| производство электрооборудования | 0,87 | 1,16 | 1,27 | 1,52 | 1,21 | 2 | 233,94 | 147,84 | 122,95 | 128,71 | с |
| производство вычислительной, электронной и оптической аппаратуры | 0,20 | 0,19 | 0,18 | 0,19 | 0,19 | 1 | 142,86 | 122,76 | 105,07 | 110,76 | в |
| Сельское хозяйство | 0,03 | 0,04 | 0,05 | 0,05 | 0,04 | н | 229,29 | 164,78 | 124,68 | 111,61 | Н* |
| Энергетика | 0,08 | 0,11 | 0,11 | 0,11 | 0,10 | 1 | 152,14 | 134,38 | 105,54 | 107,28 | С* |
| Строительство | 0,28 | 0,35 | 0,36 | 0,38 | 0,34 | 1 | 204,72 | 135,83 | 123,67 | 121,87 | Н* |
| Водоснабжение | 0,15 | 0,24 | 0,22 | 0,22 | 0,21 | 1 | 232,83 | 180,14 | 108,66 | 118,94 | С* |
| *Сектор услуг* | | | | | | | | | | | |
| Финансовая и страховая деятельность | 1,69 | 1,78 | 1,72 | 1,65 | 1,71 | 2 | 150,74 | 125,87 | 113,60 | 105,42 | В* |
| Сектор ИКТ | 5,18 | 6,44 | 6,29 | 7,87 | 6,44 | 4 | 245,20 | 145,35 | 113,20 | 149,03 | В* |
| Транспорт и логистика | 0,63 | 0,99 | 0,96 | 1,01 | 0,90 | 1 | 224,94 | 176,40 | 109,58 | 116,37 | С* |
| Оптовая и розничная торговля | 1,97 | 2,83 | 3,45 | 3,88 | 3,03 | 3 | 296,61 | 174,90 | 140,32 | 120,86 | В* |
| Госуправление и оборона, обязательное социальное обеспечение | 0,90 | 1,55 | 1,34 | 1,30 | 1,27 | 2 | 249,80 | 200,43 | 99,38 | 125,41 | В* |
| Образование | 0,24 | 0,38 | 0,52 | 0,58 | 0,43 | 1 | 296,73 | 166,50 | 148,33 | 120,15 | С* |
| Здравоохранение | 0,18 | 0,29 | 0,42 | 0,46 | 0,34 | 1 | 348,10 | 180,59 | 161,74 | 119,18 | С* |
| *Средний показатель, %* | **0,43** | **0,59** | **0,64** | **0,75** | | | **241,09** | **156,27** | **120,88** | **117,62** | |

[1] Для начального уровня (н)<0,1; первого уровня (1) показатель ≥0,1, для второго (2) уровня ≥1; для третьего (3) уровня ≥3; для четвертого уровня (4) показатель ≥6;

[2] Группировка по уровню технологичности сформирована по видам экономической деятельности, относящимся к обрабатывающей промышленности, в соответствии с рекомендациями Евростата и ОЭСР на основе NACE, Rev. 2.0., где в – высокотехнологический уровень, с – среднетехнологический высокий уровень, н – среднетехнологический низкий уровень или низкий уровень; В*, С*, Н* эмпирический подход к оценке технологичности

Приложение 3

Ключевые отрасли и сектора белорусской экономики в разрезе актуальных и потенциальных рисков и угроз, связанных с цифровизацией (разработано автором)

| Сектор экономики | Риски и угрозы цифровизации[1] | | | Средне-взвешенный уровень потенциальных цифровых угроз[2] | Потенциал каскадного распростра-нения[3] |
|---|---|---|---|---|---|
| | Низко- | средне- | высоко-рискованные | | |
| Промышленность, в т.ч. | | | | | |
| Горнодобывающая | - | АЦП, КЦД, ККиС, УАСУ, ЭУПО | ВП, ПВSCADA, АКИ, АПР, ПУОИ, ФА(0), АРТ | 3,1 | +++ |
| Обрабатыв., в т.ч. | | | | | |
| машиностроение | - | АЦП, КЦД, ККиС, УАСУ, ЭУПО | АКИ, ВП, ПВSCADA, АПР, ПУОИ, ФА(0). АРТ | 3,1 | +++ |
| легкая промышленность | - | ККиС, ФА(2), КЦД, ЭУПО | ВП, ПВSCADA, АПР, ПУОИ. АРТ | 2,3 | ++ |
| пищевая | - | АЦП, КЦД, ККиС, ЭУПО | АКИ, ВП, ПВSCADA, АПР, ФА(0), ПУОИ, АРТ | 2,9 | +++ |
| деревообработка | - | КЦД, ФА(2), ККиС, ЭУПО | ВП, ПВSCADA, АПР, ПУОИ, АРТ | 2,3 | ++ |
| нефтехимия | - | КЦД, ККиС, АЦП, УАСУ, ЭУПО | ВП, ПВSCADA, ПУОИ, АПР, АКИ, ФА(0), АРТ | 3,1 | +++ |
| фармацевтика | - | КЦД, УАСУ, АЦП, ККиС, ЭУПО | АКИ, ВП, ПВSCADA, АПР, ПУОИ, ФА(0), АРТ | 3,1 | ++ |
| металлургия | - | УАСУ, АЦП, КЦД, ККиС, ЭУПО | АКИ, ВП, ПВSCADA, АПР ФА(0), ПУОИ, АРТ | 3,1 | +++ |
| производство электрооборудова-ния | - | УАСУ, АЦП, КЦД, ФА(2), ККиС, ЭУПО | ВП, ПВSCADA, АПР, ПУОИ, АРТ | 2,7 | +++ |
| производство вычислительной, электронной и оптической аппаратуры | - | УАСУ, АЦП, КЦД, ФА(2), ККиС, ЭУПО | ВП, ПВSCADA, АПР, ПУОИ, АРТ | 2,7 | +++ |
| Сельское хозяйство | - | УАСУ, ЭУПО | | 0,4 | + |
| Энергетика | - | DDOS, УАСУ, ЭУПО | АКИ, ВП, ПВSCADA, ПУОИ, ФА(0), АРТ | 2,4 | +++ |
| Строительство | - | УАСУ, ЭУПО | ВП, АПР | 1,0 | + |
| Водоснабжение | - | УАСУ, ЭУПО | АКИ, ВП, ПВSCADA, ФА(0), АРТ | 1,9 | ++ |
| Сектор услуг | | | | | |
| Финансовая и страховая деятельность | МО, ФА(1) | КЦД, ИПИД, АРИИ, ФА, ККиС, DDoS, АИСС, ЭУПО | АКИ, ВП, ПУОИ, ФА(0), АРТ | 5,1 | +++ |
| Сектор ИКТ | MOSIM | КЦД, УАСУ, ИПИД, DDoS, АРИИ, ККиС, АИСС, ЭУПО | АКИ, ВП, ПУОИ, ФА(0), АРТ | 4,1 | +++ |
| Транспорт и логистика | - | УАСУ, DDoS, ККиС, ЭУПО | АКИ, ВП, ПУОИ, ФА(0), АПР | 2,3 | +++ |
| Оптовая и розничная торговля | - | КЦД, DDoS, ФА(2), ККиС, АИСС, ЭУПО | ВП, ПУОИ | 1,8 | ++ |
| Госуправление и оборона, обязательное социальное обеспечение | - | АЧ, АЧД, КЦД, УАСУ, ИПИД, ПИА, АРИИ, | АКИ, ВП, ПУОИ, ФА(0), АРТ | 3,7 | +++ |

| Сектор экономики | Риски и угрозы цифровизации[1] | | | Средне-взвешенный уровень потенциальных цифровых угроз[2] | Потенциал каскадного распростра-нения[3] |
|---|---|---|---|---|---|
| | Низко- | средне- | высоко- | | |
| | рискованные | | | | |
| | | DDoS, АИСИ, УАИ, ЭУПО | | | |
| Образование | - | КЦД, DDoS, ФА(2), ЭУПО | ВП | 1,1 | + |
| Здравоохранение | - | КЦД, УАСУ, АРИИ, DDoS, ЭУПО | АКИ, ВП, ПУОИ, АИЭЗ, ФА, АРТ | 2,8 | ++ |

[1] «АЗС – атака захвата сеанса, при которой злоумышленник влияет на сеанс связи между узлами / транспортными средствами; АИЭЗ – атака на инфраструктуру электронного здравоохранения; АИСИ – атаки с использованием методов социальной инженерии; АКИ – атака на критическую инфраструктуру; АП – атаки через посредника (Man in the Middle) предполагает размещение злоумышленника между двумя взаимодействующими законными узлами / транспортными средствами и подслушивает их связь и вводит ложную информацию или изменяет сообщение между ними; АПР – атаки на промышленных роботов; АРИИ – атака раскрытия идентификационной информации направлена на нарушение требований аутентификации и конфиденциальности; АЦП – атака цепочки поставок; АЧ – атака червоточины, при которой два вредоносных узла участвуют в сети для создания частного туннеля, называемого червоточиной, где первый вредоносный узел на одном конце передает данные второму вредоносному узлу на другом конце, что приводит к нарушению безопасности для пакетов; АЧД – атака черная дыра, при которой злоумышленник обманывает протокол маршрутизации, представляя себя как узел с кратчайшим путем к узлу назначения, таким образом, вместо того, чтобы полагаться на процесс обнаружения маршрута, все узлы начинают доверять поддельному маршруту, и в конечном итоге пакеты данных перехватываются вредоносным узлом; ВП – вредоносные программы, такие как черви, вирусы, трояны, вымогатели, бэкдоры, шпионское ПО и т.д. использовались мошенниками для организации атак на компьютерные системы с целью нарушения конфиденциальности, целостности передаваемых данных и доступности услуг, предлагаемых базовой инфраструктурой; ВБК\ВКК – взломы биржевых и криптовалютных кошельков; ДТ – двойная трата предполагает возможность пользователю выполнять несколько транзакций с одной и той же криптовалютой; ИПИД – использование поддельных (краденых) идентификационных данных; ККиС – коммерческий кибершпионаж и саботаж для получения коммерческих секретов, получения конкурентного преимущества; Кр – криптоджекинг предполагает несанкционированное использование чужих компьютеров для майнинга криптовалюты; КЦД – кража цифровых (личных) данных, в т.ч с использованием целевых кибератак; М – использование сервисов (миксеров), предназначенных для скрытия взаимосвязи между адресами в последовательных транзакциях, скрытия владельцев криптоактивов и их происхождения; МА – маскарадная атака предполагает маскировку злоумышленником своей личности, чтобы действовать в качестве легитимного узла с намерением генерировать ложные сообщения в сети или модифицировать полученное сообщение; МАР – атака маршрутизации предполагает перехват сообщений в сети Blockchain; МО – мошеннические операции; MOSIM – мошенничество с обходом или мошенничество с SIM; ПАТ – прослушивание и анализ трафика; ПBSCADA – программы взлома систем управления производством; ПИА – поддельная информационная атака, которая направлена на передачу ложной информации по сети; ПУОИ – потеря управления при использовании облачной инфраструктуры; УАИ – узловая атака имитации направлена на нарушение аутентификации в сети; УАСУ – удаленные атаки на системы управления трафиком с поддержкой Интернета вещей; ФА(0) – фишинговая атака – цель объект критической инфраструктуры; ФА(1) – фишинговая атака – цель юридическое лицо; ФА(2) – фишинговая атака – цель клиент юридического лица; ЭУПО – эксплуатация уязвимостей ПО; АРТ – целевые кибератаки; DDoS атаки, генерирующие избыточный трафик, что препятствует доступу пользователей к ресурсу или услуге; Eclipse – предполагает изоляцию конкретного узла одноранговой сети с целью получения контроля всех исходящих соединений узла; GPS атака – направлена на взлом управления положением транспортных средств с помощью имитаторов GPS, которые выдают более сильные сигналы, чем исходная спутниковая система GPS; Sybil – атака узла IoT при которой используется несколько идентификаторов для компрометации основной части сети» [4].

[2] Суммируется количество выявленных рисков в зависимости от уровня потенциальных угроз (сумма угроз «Н»- низкого уровня умножается на коэффициент 0,1; «С» – умножается на коэффициент 0,2; «В» – умножается на коэффициент 0,3.

[3.] Шкала, «+» отражает минимальный уровень «каскадности», «++» – средний уровень; «+++» – максимальный возможный уровень каскадного эффекта.

Приложение 4

Сводная таблица основных показателей оценки рисков цифровизации (разработано автором)

| Сектор экономики | Оценочный уровень цифровизации отрасли, $О_ц$ [1] | Коэффициент уровня технологичности, $К_т$ [2] | Доля в экспорте (2020, %), $Д_э$ [3] | Доля в среднесписочной численности работников (2019, %), $Д_р$ | Коэффициент наличия в отрасли критической инфраструктуры и соответствующих рисков, $К_к$ [4] | Средневзвешенный уровень потенциаль-ных цифровых угроз, $С_р$ | Каскадный эффект, $Кас_э$ [5] | Интегральный показатель, $У_и$ |
|---|---|---|---|---|---|---|---|---|
| **Общие показатели** | | | | | | | | |
| **Промышленность**, в т.ч. | | | | | | | | |
| Горнодобывающая | 1 | 0,8 | 1,5 | 0,3 | 1,2 | 3,1 | 1,0 | 3,0 |
| Обрабатывающая, в т.ч. | | | | | | | | |
| машиностроение | 1 | 0,9 | 10,5 | 3,2 | 1,2 | 3,1 | 1,0 | 3,5 |
| легкая промышленность | 1 | 0,8 | 2,8 | 2,5 | 1,0 | 2,3 | 0,9 | 1,7 |
| пищевая | 1 | 0,8 | 14,0 | 3,5 | 1,2 | 2,9 | 1,0 | 3,0 |
| деревообработка | 1 | 0,8 | 4,7 | 2,2 | 1,0 | 2,3 | 0,9 | 1,7 |
| нефтехимия | н | 0,9 | 24,6 | 1,5 | 1,2 | 3,1 | 1,0 | 0,3 |
| фармацевтика | 1 | 1,0 | 0,9 | 0,3 | 1,2 | 3,1 | 0,9 | 3,4 |
| металлургия | 1 | 0,8 | 5,7 | 1,6 | 1,2 | 3,1 | 1,0 | 3,0 |
| производство электрооборудования | 2 | 0,9 | 2,8 | 0,8 | 1,0 | 2,7 | 1,0 | 4,9 |
| производство вычислительной, электронной и оптической аппаратуры | 1 | 0,9 | 1,9 | 0,5 | 1,0 | 2,7 | 1,0 | 2,5 |
| Сельское хозяйство | н | 0,8 | 1,5 | 8,7 | 1,0 | 0,4 | 0,8 | 0,1 |
| Энергетика | 1 | 0,9 | 0,1 | 2,2 | 1,2 | 2,4 | 1,0 | 2,6 |
| Строительство | 1 | 0,8 | 1,5 | 6,4 | 1,0 | 1,0 | 0,8 | 0,7 |
| Водоснабжение | 1 | 0,9 | 0,3 | 1,0 | 1,2 | 1,9 | 0,9 | 1,9 |
| **Сфера услуг, в т.ч.** | | | | | | | | |
| Финансовая и страховая деятельность | 2 | 1,0 | 0,2 | 1,5 | 1,2 | 5,1 | 1,0 | 12,3 |
| Сектор ИКТ | 4 | 1,0 | 7,2 | 2,9 | 1,2 | 4,1 | 1,0 | 19,8 |
| Транспорт и логистика | 1 | 0,9 | 9,9 | 6,8 | 1,2 | 2,3 | 1,0 | 2,7 |

| Сектор экономики | Оценочный уровень цифровизации отрасли, $О_ц$ [1] | Коэффициент уровня технологичности, $К_т$ [2] | Доля в экспорте (2020, %), $Д_э$ [3] | Доля в среднесписочной численности работников (2019, %), $Д_р$ | Коэффициент наличия в отрасли критической инфраструктуры и соответствующих рисков, $К_к$ [4] | Средневзвешенный уровень потенциаль-ных цифровых угроз, $С_р$ | Каскадный эффект, $Кас_э$ [5] | Интегральный показатель, $У_и$ |
|---|---|---|---|---|---|---|---|---|
| Оптовая и розничная торговля | 3 | 1,0 | н\д (0) | 14,5 | 1,0 | 1,8 | 0,9 | 5,0 |
| Государственное управление и оборона, обязательное соц. обеспечение | 2 | 1,0 | 0,03 | 4,2 | 1,2 | 3.7 | 1,0 | 8.9 |
| Образование | 1 | 0,9 | 0,2 | 10,4 | 1,0 | 1,1 | 0,8 | 0,9 |
| Здравоохранение | 1 | 0,9 | 0,1 | 7,6 | 1,2 | 2,8 | 0,9 | 2,8 |

[1], где 1, 2 , 3 – соответствующие уровни цифровизации отраслей (эмпирический анализ).
[2], где низкий уровень технологичности имеет коэффициент –0,8, средний – 0,9, высокий – 1.
[3] данные приложения 149.
[4] , где наличие в отраслевой структуре предприятий критической инфраструктуры отмечается коэффициентом 1,2. Отсутствие критической инфраструктуры – 1.
[5], где низкий потенциал каскадности имеет коэффициент – 0,8, средний – 0,9, высокий – 1

## Приложение 5

## Перспективные сектора и сфера экономики, управления и социальной системы, в рамках концепции новой экономики 2.0 (разработано автором)

| Сектора и сфера экономики, управления и социальной системы | Риски и угрозы цифровизации[1] | | | Потенциал их каскадного распространения | Степень потенциального влияния на экономическую ситуацию[2] | Степень потенциального влияния на социальную ситуацию[3] |
|---|---|---|---|---|---|---|
| | низкориско-ванные | среднерискованные | высокорискованные | | | |
| | 1 | 2 | 3 | 4 | 5 | 6 |
| «E-Government» | - | АРИИ, ИПИД КЦД, ЭУПО, АИСС | ВП, ПУОИ, АКИ, ФА(0), АРТ | +++ | Угрозы устойчивости системы управления на макроуровне (В) | - |
| «Smart City», «Intellectual Transport Systems» | ПАТ, Sybil, GPS | КЦД, DDoS, УАСУ, АЧД, АЧ, ПИА, УАИ, МА, АРИИ, ЭУПО, АИСС, ФА(2) | ВП, АП, АЗС, АРТ | +++ | - | Физическая угроза здоровью и жизни населения при кибератаках на Intellectual Transport Systems (Ч) |
| «PropTech» | - | АИСИ, АРИИ, ИПИД, КЦД, ЭУПО, | ВП, ПУОИ, АРТ | ++ | Кража информации об объектах критической инфраструктуры (В)<br>Кража коммерчески чувствительной информации об объектах недвижимости (С) | - |
| «Industry 4.0» | - | АЧД, ПИА, УАИ, DDoS, КЦД, ККиС, АЧ, ЭУПО | АП, ВП, АПР, ПВSCADA, ПУОИ, АРТ | +++ | Рост рисков в отношении промышленных активов, финансовых показателей, бизнес-репутации (В) | Физическая угроза здоровью и жизни работников при взломе роботизированных систем (Ч) |

| Сектора и сфера экономики, управления и социальной системы | Риски и угрозы цифровизации[1] | | | Потенциал их каскадного распространения | Степень потенциального влияния на экономическую ситуацию[2] | Степень потенциального влияния на социальную ситуацию[3] |
|---|---|---|---|---|---|---|
| | низкориско-ванные | среднерискованные | высокорискованные | | | |
| | 1 | 2 | 3 | 4 | 5 | 6 |
| | | | | | Кража коммерческой информации о покупателях продукции и поставщиках (С) | |
| «Agriculture 4.0» | - | УАСУ, ЭУПО | ВП | + | Сбой систем может привести к прямым финансовым убыткам и сокращению с/х производства (С) | - |
| «Smart Grid» | МО | КЦД, ПИА, DDoS, АЧД, УАИ, ЭУПО | АП, ВП, АЗС, ПВSCADA, АРТ | +++ | Сбой системы может привести к прямым финансовым потерям энергогенерирующих компаний (В) | - |
| «Smart Supply Chain» | - | ПИА. ККиС, ЭУПО | - | +++ | Сбои систем приведут к финансовым убыткам (С) | - |
| «E-Commerce» | МО, ФА(1) | DDoS, КЦД, ФА (2), ЭУПО, АИСС | ВП, ПУОИ | + | Сбои систем приведут к сокращению объемов торговли, прямым финансовым убыткам (С) | - |
| «Telemedicine» | - | КЦД, DDoS, УАСУ, АРИИ, ЭУПО | АИЭЗ, ВП, ПУОИ, АРТ | +++ | - | Рост угрозы здоровью и жизни граждан при перехвате либо блокировке сигналов удаленной IoT связи (Ч) |
| «CBDC» | МО | ИПИД, ЭУПО | ВП, ВКК | +++ | Ослабление роли коммерческих банковских учреждений с точки зрения финансовой интермедиации (С)<br>Сокращение банковских депозитов и снижение доходов, полученных от предоставления данной финансовой услуги (Н)<br>Увеличение процентной ставки по банковским кредитам, снижение объема кредитования (Н)<br>Рост риска устойчивости финансовой инфраструктуры к кибератакам (С) | - |
| «RTGS» | - | ИПИД, ЭУПО | ВП | +++ | Сбой по причине эндогенных или экзогенных факторов несет прямые финансовые убытки в банковском секторе (В) | - |
| «FinTech» | ВБК\ВКК, Eclipse МО, ДТ, М, ФА(2) | ИПИД, КЦД, ЭУПО, АИСС, ФА(1) | ВП, ПУОИ, АРТ | +++ | Проблема налогообложения данной экономической деятельности (С)<br>Новые риски для стабильности | Социальная напряженность в связи с возможной потерей инвестиций населением в высокорискованные активы FinTech |

| Сектора и сфера экономики, управления и социальной системы | Риски и угрозы цифровизации[1] | | | Потенциал их каскадного распространения | Степень потенциального влияния на экономическую ситуацию[2] | Степень потенциального влияния на социальную ситуацию[3] |
|---|---|---|---|---|---|---|
| | низкориско-ванные | среднерискованные | высокорискованные | | | |
| | 1 | 2 | 3 | 4 | 5 | 6 |
| | | | | | финансовой системы (С)<br>Потенциал сгенерировать системные риски, вызывающие разрушение финансовой системы (В)<br>Риски ликвидности (Н)<br>ПОД/ФТ (В)<br>Угроза алгоритмов AI по разрушения фондовых рынков (Ч)<br>Финансовые пирамиды (В)<br>Прямые финансовые потери от взлома и хищения криптоактивов криптобирж (С)<br>Мошенничество при ICO (С)<br>Кража цифровых данных платежных карт (С)<br>Атаки POS-терминалов и банкоматов (С) | (С) |
| *Опционально*<br>Расширение использования криптовалют | МО, М, Кр, Sybil Eclipse, MAP, ДТ, ВБК\ВКК | - | ВП | +++ | ПОД/ФТ (В)<br>Инвестиционные риски (С)<br>Теневые рынки запрещенных товаров и услуг (В)<br>Легализация краденых активов (С)<br>Инструментарий ухода от банковского контроля. (С)<br>Преодоление санкционных ограничений. (С) | Напряженность в связи с возможной потерей инвестиций населением в высокорискованные криптоактивы (С) |

[1] (см. приложение 3)

[2,3] Ранжирование факторов по методологии CIA, где Н-низкий уровень угроз, С – средний, В – высокий, Ч – чрезвычайный

Приложение 6

Сводная таблица основных показателей оценки рисков цифровизации (разработано автором)

| Сектор экономики | Оценочный уровень цифровизации отрасли, $О_ц$ | Оценочный показатель экономического влияния[1], $О_э$ | Оценочный показатель социального влияния[2], $О_с$ | Средневзвешенный уровень потенциальных цифровых угроз[3], $С_р$ | Каскадный эффект[4], $Кас_э$ | Итоговый показатель, $У_и$ |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| «E-Government» | 4 | 0,9 | | 2,5 | 1,0 | 10,0 |
| «Smart City» | 4 | | 1,0 | 3,9 | 1,0 | 15,6 |
| «Industry 4.0» | 4 | 0,85 | 1,0 | 3,4 | 1,0 | 13,6 |
| «Agriculture 4.0» | 4 | 0,8 | | 0,7 | 0,8 | 2,2 |
| «Smart Grid» | 4 | 0,9 | | 2,8 | 1 | 11,2 |
| «Smart Supply Chain» | 4 | 0,8 | | 0,6 | 1 | 2,4 |
| «E-Commerce» | 4 | 0,8 | | 1,8 | 0,8 | 5,8 |
| «Telemedic-ine» | 4 | | 1,0 | 2,2 | 1,0 | 8,8 |
| «CBDC» | 4 | 0,75 | | 1,1 | 1,0 | 4,4 |
| «RTGS» | 4 | 0,9 | | 0,7 | 1,0 | 2,8 |
| «FinTech» | 4 | 2,3 | 0,8 | 2,5 | 1,0 | 10,0 |
| *Опционально* Расширение использования крипто-валют | 4 | 1,25 | 0,8 | 1,1 | 1,0 | 4,4 |

[1] Дополнительные факторы нецифрового риска (экономические) ранжированы по уровню угроз, где низкий уровень имеет показатель 0,7, средний – 0,8, высокий – 0,9, чрезвычайный -1. Рассчитывается как средняя арифметическая сумма рисков

[2] Дополнительные факторы нецифрового риска (социальные) ранжированы по уровню угроз, где низкий уровень имеет показатель 0,7, средний – 0,8, высокий – 0,9, чрезвычайный -1. Рассчитывается как средняя арифметическая сумма рисков

[3] Суммируется количество выявленных рисков в зависимости от уровня потенциальных угроз (сумма угроз «Н»-низкого уровня умножается на коэффициент 0,1; «С» – умножается на коэффициент 0,2; «В» – умножается на коэффициент 0,3

[4] Низкий потенциал каскадности имеет коэффициент- 0,8, средний – 0,9, высокий – 1