Секция «Цифровая экономика и перспективные технологии управления данными»

Риски государственного управления социально-экономическими процессами в условиях цифровизации, их верификация и характеристики

Научный руководитель – Воронина Евгения Васильевна

Чеканов Илья Игоревич
Аспирант
Сургутский государственный университет Ханты-Мансийского АО, Сургут, Россия
E-mail: seintsuslik@mail.ru

Управление социально-экономическими процессами, как и любая деятельность, постоянно сталкивается с различными рисками, способными существенно повлиять на эту деятельность.

Риск стал не только философской, но и исторической, а также напрямую связанной с экономикой категорией, появившись на заре создания первых цивилизаций. Риск, являясь внутренними или внешними предпосылками, в первую очередь был связан у человека с чувством страха перед возможной опасностью. В нынешних условиях мировая экономическая формация создала такие понятия, что слово риск стало обыденностью для рыночных отношений любого уровня, подразумевая под собой в первую очередь финансовую неудачу, потери, невыполненный проект. Таким образом, слово риск стало неотъемлемой частью экономических отношений при капитализме, трансформируясь в экономические и финансовые риски.

Финансовым риском является некая вероятность, при которой возможно появление убытков, недополученные доходы, нарушение прогнозируемых вариантов.

Экономическим риском является возможность появления нежелательных убытков, которые измеряются в денежном выражении.

Абсолютно любое производство какой-либо продукции или услуги заведомо подразумевает существование риска. Чаще всего, риск является крайне нежелательным, так как в первую очередь вредит финансовому состоянию предприятия. Риски можно предугадать, выявить, тем самым или подготовиться к заведомо негативным последствиям, либо вовсе избежать их. Анализ и прогноз рисков, а точнее негативных последствий рискованных действий способен выявить серьёзность проблемы и степень капитальных затрат при том или ином результате.

Но также следует добавить, что риск не является сугубо негативным объектов экономических отношений. Благодаря рискованным действиям, компания может не только заиметь убыток, но и получить сверхприбыль, открыть новый рынок сбыта, создать тренд или моду на производимую продукцию, что всецело ведёт к обогащению самого предприятия. Таким образом получается, что риск имеет три экономических результата [3]:

- Отрицательный – ущерб, убыток, проигрыш;
- Нулевой – отсутствие убытка и прибыли;
- Положительный – выгода, прибыль, выигрыш.

Риск приобретает измеряемые и реальные очертания посредством того ущерба или выгоды при его совершении. Таким образом можно понять, насколько удачный или неудачный исход, что можно измерить при помощи применения теории вероятности и закона больших чисел на основе статистических данных. Таким образом, избежать или оценить риск помогает статистика, которую становится куда проще вести в условиях повышения цифровизации экономики и производства на предприятии, тем самым создавая более удобные условия для анализа, прогноза, оценки ситуации и экономического положения производства. Риск всецело зависит от неопределённости, которая подразумевает под собой

неполноту, неточность информации. Чем меньше неопределённость, тем ниже вероятность отрицательного результата при риске. Так как любая экономическая деятельность будет осуществляться в условиях неопределённости внешней среды, фактор успеха зависит от возможности предугадывания. Экономическая система состоит из ряда факторов, которые оказывают друг на друга непосредственное влияние и их можно систематизировать в виде схемы неопределенностей.

Под неопределённостью понимается отсутствие точного значения тех или иных параметров, их изменений, порождаемых различными причинами. Это неполнота и отсутствие точности информации создаёт проблемы для реализации того или иного решения, порождая возможные затраты при неблагосклонных результатах. Основными источниками неопределённости и риска являются спонтанность и случайность. Таким образом получается, что большинство социально-экономических и технологических процессов подвержены неодинаковым, случайным стечением обстоятельств [1].

В реальном времени происходит ситуация, когда небыли предугаданы риски закрытия иностранных рынков для Российской Федерации, что приводит к не самым благоприятным последствиям для экономического состояния некоторых предприятий и российской экономики в принципе. Данная ситуация является проявлением противоборствующей тенденции, которая также является отдельным источником риска. Для грамотного использования рискованных ситуаций в качестве собственной выгоды или избежание потерь и издержек, существует такое понятие, как риск-менеджмент. Управление риском является процессом, при котором происходит принятие и выполнение управленческих решений с целью максимальной минимизации неблагоприятного влияния на предприятие и организацию в качестве убытков. Таким образом, риск-менеджмент является системой по управлению риском и экономическими отношениями, влияющими и возникающими в процессе управления.

Управление рисками в современных экономических условиях проявляется в следующих позициях [2]:

- Выявление условий и последствий деятельности определённых субъектов в рискованных ситуациях;

- Умение правильно реагировать на возможные отрицательные последствия экономической деятельности;

Разработка и осуществление мер для максимального урегулирования, нейтрализации или компенсации возможные негативные результаты экономических отношений и действий внутри них.

Вне зависимости от размеров компании, количества производимой продукции, видов услуг его хозяйственная деятельность будет строиться на рисках. Риск ведёт к возможному вознаграждению, тем самым порождая смысл существования некоторых предприятий. Удаление рисков невозможно, так как таким образом пропадает фактор вознаграждения, что обесценивает любые попытки инноваций в производственных процессах. Риск-менеджмент нацелен на то, чтобы в первую очередь суметь не контролировать, но управлять рисками, тем самым создавая благоприятные условия для собственного развития.

В связи с общей непредсказуемостью любых процессов растёт и неопределённость. Отсутствие должного внимания со стороны компаний способно принести существенный вред их финансовому состоянию, либо вовсе привести к окончанию какой-либо деятельности. Из такого вреда можно выделить [4]:

- Финансовые убытки;
- Уменьшение стоимости акций и капитала;
- Репутационные издержки;
- Добровольное увольнение сотрудников, менеджеров;

- Банкротство.

Современный этап экономических отношений оригинален тем, что риски перестали рассматриваться обособленно друг от друга. Таким образом, риск-менеджмент является комплексной управленческой программой. Управление риска состоит из двух подсистем, таких как управляемая подсистема и управляющая подсистема. У каждой из систем есть данные элементы:

- Цель, вход основной системы;
- Выход основной системы;
- Канал обратной связи;
- Блок управления.

На управление любым предприятием взваливается обязанность учитывать влияние факторов воздействия внутренней и внешней среды. Внешняя среда, являясь совокупностью элементов, способна сильно повлиять на предприятие, так как оно сильно связано с самой системой. Нынешние экономические условия, покупательская способность населения, тарифы поставщиков, законы, тарифы и положения, общественные взгляды, возможность и развитость технологий – всё из этого входит в понятие внешней среды. Она динамична, неопределённа, но всегда закономерна по сложившимся ключевым факторам и их взаимодействии.

хранения больших объемов информации, их анализа и использования, хранения этой информации, из-за чего общий набор данных растёт экспоненциально. Среди преимуществ необходимо выделить:

- Данный метод использует сбор данных из разных источников, что диверсифицирует информацию и позволяет критически оценивать те или иные тенденции;
- Аналитика проводится в реальном времени, что способствует улучшению уровня управления над любым процессом, позволяя своевременно вносить корректировки;
- Метод подразумевает использование больших объемов данных, что способствует хранению этих самых объемов в структурах организации.

В свою очередь, риски больших данных имеют свою определённую специфику и заключаются в следующем (таблица 1).

Таблица 1. Риски больших данных [10].

Возможные риски

Описание рисков

Риски, связанные с конфиденциальностью

Существует риск потери значимых данных, что способно повлиять на внутренние структуры организации, а также эти данные могут быть использованы недобросовестно.

Данные также могут быть использованы в различных сетях интернет, а также в средствах массовой информации, что также создаст нежелательную огласку. Данные риски возможно минимизировать посредством ввода в использования различных уровней контроля и проверок, в том числе по биометрическим данным или электронной подписи.

Риски, связанные с потерями различных данных

Среди них можно выделить полное или частичное уничтожение с последующей потерей данных из-за ошибочных действий специалистов или вреда со стороны злоумышленников, а также технических неполадок и чрезвычайных ситуаций, в которых возможно физическое повреждение носителей данных. Данные риски возможно минимизировать при помощи создания резервных копий данных.

Риски, связанные с хранением и переполнением информации

Связано с несистематическим заполнением различными данными инфраструктуры хранения, при котором формируется невозможность хранения необходимых данных из-за отсутствия места. Данные риски возможно минимизировать посредством корректного

размещения информационных ресурсов и своевременного удаления уже не актуальных данных.

Риски, связанные с формированием неэффективного процесса по набору данных

Данный риск связан с отсутствием возможности или опыта специалистами, которые осуществляют подбор информации и её фильтрации. Решается посредством повешения квалификации работников, прохождения специальных курсов и формирования структурированной системы по поиску информации и сопутствующих целей. В работе с данными необходимо соблюдение информационной гигиены.

Риски, связанные с снижением эффективности используемого метода больших данных

Это риски, связанные с обесцениванием получаемой информации из-за её количества и отсутствия возможности должным образом информацию фильтровать. Решается при помощи наличия чёткой классификации данных.

Риски, связанные с ошибками больших данных

Это риски, связанные с применением неправильных инструментов для работы с данными.

Риски, связанные с экономической необоснованностью и нецелесообразностью по применению метода больших данных

При объеме большего пласта данных может возникнуть ситуация, в которой специалисты не могут найти то или иное решение на проблему, с которой столкнулась организация.

Риски, связанные с отсутствием готовности организации по адаптированию к переменам

Возможна ситуация, в которой компания или организация не может использовать данный метод из-за определённой политики или структуры, при которой осуществляет свою деятельность.

Риски, связанные с активизацией мошенников

Это риски, которые могут возникнуть при приобретении объемов больших данных или использовании различных платных сервисов для упрощения использования информации.

Таким образом, метод больших данных способствует объединению различных разрозненных источников и объемов в данных в некую единую систему, которая может быть подвержена анализу с целью получения необходимых результатов и получению определённых экономических преимуществ.

Далее необходимо разобрать риски использования промышленного интернета. Под промышленным или индустриальным интернетом подразумевается информационная и коммуникационная инфраструктура, которая объединяет различные промышленные объекты и способствует обмену данных между ними, из-за чего они могут взаимодействовать без использования услуг посредников. Данный метод цифровизации формирует новые бизнес-модели и организационные структуры, когда взаимодействие производителя и покупателя или потребителя услуг осуществляется напрямую без каких-либо переменных между ними. Использование промышленного интернета осуществляется посредством применения специфического программного обеспечения, что может привести к возможным угрозам по кибер-атакам на промышленные объекты и структуры. Необходимо выделить следующие угрозы и риски (Таблица 2.).

Таблица 2. Риски использования промышленного интернета организацией [9].

Возможные риски

Описание рисков

Риски, связанные с действием третьих лиц при помощи различных манипуляций, которые производятся с специализированным программным обеспечением по использованию производственного интернета.

Среди них можно выделить ситуации, в котором третьи лица внедряют в программное обеспечение вредоносные программы, способные повлиять на работоспособность или поспособствовать утечки данных без согласия самого пользователя. Такими ситуациями могут является массовые хакерские атаки на информационные структуры организации с целью формирования ошибки по «отказу в обслуживании», при которой сервисы перестают функционировать. Также следует выделить различные «эксплойты», которые подразумевают под собой программный код, нацеленный на поиск уязвимостей в информационной системе и получения доступа к ней.

Риски, связанные с взломом системы

Это риски, которые подразумевают прямое воздействие на информационные системы, которые реализуются на уровне сети. Туда входят такие процедуры, как подслушивание, когда информация внутри организации передаётся третьей стороне. Также может осуществляться захват сессии, при котором злоумышленник получает доступ к информации. И в конце необходимо сказать о сетевой разведке, в которой злоумышленник получает доступ к подключению различных устройств к сети, открывать порты, использовать различные службы, что способствует получению внутренней информации об организации.

Риски, связанные с возможными ошибками конфигурации и администрировании информационных систем

Риск, при котором то или иное программное обеспечение работает некорректно. Это возможно либо из-за некачественного программного обеспечения, либо из-за нехватки умений и навыков при установке и использовании информационных программ и систем.

Риски, связанные с возможными отключениями коммуникаций, потери электропитания, отключения сервисов

Риск, при котором осуществляется преднамеренный или случайный сбой в работе электрических сетей, при которых использование информационных структур становится невозможным, а также сбой в работе самих устройств, которые были повреждены или отказываются функционировать из-за невыполненных условий эксплуатации.

Риски, связанные с форс-мажорными ситуациями

В основном, судя входят риски, связанные с различными происшествиями природного характера. Это могут быть различные наводнения, затопления, сильные понижения температур, снегопады и землетрясения, которые физически делают невозможным использование и функционирование оборудования из-за физического воздействия на него.

Риски, связанные с отключением и выводом из строя различных устройств для работы с информационными системами

Сюда входят риски, связанные с повреждением оборудования, необоснованной модификацией, которая в последствии сказалась на работоспособности оборудования, а также физическое воровство оборудования.

Риски, связанные с общими уязвимостями программного обеспечения для работы с информационными системами.

Это риски, в которых сама информационная система может пострадать из-за недостаточного уровня безопасности при использовании внутренних сервисов. Среди них могут быть слабые пароли, которые легко взломать, различные ошибки программного обеспечения, которые могут критически повлиять на данные, а также остановка работы сервисов, которые предоставляет провайдер посредством прекращения деятельности или сбоев.

Риски, связанными с изменениями в законодательстве.

Возможные риски, так как законы имеют свойство пополняться и меняться с течением времени, что способно повлиять на использования тех или иных информационных программ, которые, например, были заблокированы на территории страны, или были осуществлены требования по продвижению отечественного программного обеспечения, из-за

которого его применение необходимо.

Таким образом, промышленный интернет является одним из наиболее важных элементов по формированию четвёртой промышленной революции. Данный метод активно вводится на предприятия со стороны государства посредством Ростеха, так как это крайне эффективный инструмент для повышения эффективности управления и коммуникации различных субъектов между собой.

Необходимо также выделить искусственный интеллект и риски, связанные с его использованием. Искусственный интеллект — это технология по созданию различных аппаратно-программных средств, которые могут осуществлять всяческие творческие задачи и создавать посредством генерации новую информацию на базе уже существующей информации. Искусственный интеллект не самостоятелен в плане создания различной информации и базируется уже на созданном человеком контенте, в связи с чем любое создание контента от искусственного интеллекта является моделированием уже существующего контента человеческого, только немного иначе, с другими наборами переменных. Искусственный интеллект, при создании чего либо, использует следующие инструменты:

- Машинное обучение;
- Различные нейронные сети;
- Компьютерное зрение для поиска информации;
- Распознание различных объектов, в том числе образов;
- Распознание лиц и выявления соответствий;
- Распознание звука.

Искусственный интеллект как технология развивается не в одной плоскости, а во множестве разных направлений. Среди них можно выделить такие как [7]:

- Анализ уже существующих данных с последующим принятием решений посредством чистой аналитики;
- Использование машинного зрения и анализа изображений;
- Машинное обучение с применением голосовой аналитики;
- Осуществление переноса технологии искусственного интеллекта в настоящий мир;
- Создание и формирование роботов на базе искусственного интеллекта.

Также необходимо более подробно озвучить риски внедрения искусственного интеллекта в различные сферы деятельности по управлению чем-либо.

Таблица 2. Риски использования искусственного интеллекта.

Возможные риски

Описание рисков

Риски, связанные с потерями контактов с клиентами

Автоматизация может полностью ликвидировать человеческий контакт между производителем и клиентом, что не всегда положительно может сказаться на общем уровне оказания услуг, так как человек в большинстве своём предпочтёт личный, человеческий контакт.

Риски нехватки специалистов с достаточным уровнем квалификации

Появляются ситуации, когда одни профессии уходят в прошлое, так как были вытеснены искусственным интеллектом и создаются новые, которые на данный момент достаточно нишевые и полноценных специалистов для данных вакансий найти сложно, ибо они являются новыми в постоянно изменяющейся ситуации.

Риски неподготовленности информационно-технологической базы

Отсутствие условной инфраструктурной базы на предприятии, у которого не хватает технологических мощностей для использования искусственного интеллекта в полном формате, из-за чего с ним возникают проблемы, либо он вовсе не применяется из-за своей дороговизны в подготовке этой самой базы.

Риски различных ошибок в производственных процессах и при управлении производством

Искусственный интеллект не самостоятелен, в связи с чем процессы и навыки по выполнению тех или иных задач он берёт от специалистов, анализируя их работу. Это создаёт ситуацию, в которой искусственный интеллект может унаследовать различные ошибки от специалиста, с которого он учился, из-за чего будет в первую очередь страдать выполнение тех или иных процессов в организации.

Искусственный интеллект, как технология, способствует существенному сокращению осуществления рутинного труда посредством человека, освобождая его от данной обязанности. Таким образом, искусственный интеллект способен заменять в определённых областях человека, способствуя перемещению его производственного потенциала в другие сферы, где требуется творчество и гибкий ум. Но также существует и достаточно весомый минус. Искусственный интеллект может создать ситуацию, в которой человеческий труд будет обесценен и, как следствие, многие люди будут заменены на своих работах.

Далее нужно поговорить о рисках беспроводных технологий. Посредством них осуществляется передача информация разного масштаба, от большого до малого. Сама передача осуществляется либо посредством радиоволн, либо при помощи инфракрасного излучения до точки приёма информации. На данный момент времени, практически везде применяется беспроводной интернет, обеспечивающий доступ к общению и базам данных для поиска информации, которым пользуются как на производственных или управленческих предприятиях, так и дома в обычной потребительской жизни. Это технологии, которые открывают доступ к интернету из различных общественных мест и позволяют управлять чем-либо, напрямую не находясь при этом в одном рабочем и стационарном месте. В связи с этим, для применения данных технологий существуют различные протоколы по осуществлению безопасности для противодействия несанкционированному подключению к сети и воровству информации. Существует несколько типов беспроводных сетей, среди них выделяют такие как [8]:

- WWAN – это глобальные беспроводные сети, действия которых могут распространяется на огромные расстояния. В основном, это мобильные сети, осуществляющие свою работу посредством пакетной передачи данных, что позволяет как проводить общение с другими устройствами, так и выходить в общую сеть интернет;

- WMAN – это сети, масштаб которых распространяется на город и они начинают хуже работать при выезде за его приделы;

- WLAN – наиболее распространённым примером подобных сетей является сеть WI-FI, которая имеет небольшое распространение, вплоть до пары сотен метров;

- WPAN – сети, в основном используемые персонально для подключения различных устройств в небольшом отдалении друг от друга на расстоянии в паре десятков метров. К ним можно отнести такие сети, как Bluetooth.

Таким образом, одни сети позволяют выходить в интернет и поддерживать общение практически из любой точки мира, где присутствует сетевое покрытие, другие же ограничиваются паре десятков метров, объединяя в одну сеть несколько устройств для более комфортного их использования. В любом случае, данные сети созданы с целью упрощения работы с различным оборудованием, объединяя его в одну систему, в которой можно как мониторить состояние того или иного объекта, так и непосредственно управлять им на расстоянии, что не требует непосредственного прибывания на рабочем месте или нахождения специалиста рядом с самим объектом. Данные сети удобны для подключения к ним за счёт простоты и быстроты данного действия, а также крайне эффективны, так как любой специалист в любой момент времени может как задать необходимую задачу откуда угодно, так и наблюдать за процессом посредством поступающей напрямую информации.

С другой стороны, в этом кроется и основная опасность данных сетей. Их вездесущность и простата в использовании напрямую вредит защищённости данных сетей. Использующие их организации должны всегда быть готовы к несанкционированному подключению к ним, а также попыток выкрасть информацию. В данном случае проводное соединение намного безопаснее, о котором говорилось раннее. Для внедрения в проводную сеть необходимо получить доступ к тому или иному оборудованию, которое соединено в сети, что делается посредством воровства, незаконного проникновения на объект, вредоносной программы и так далее. В случае беспроводной сети, недоброжелателю достаточно лишь получить сигнал сети, к которой он хочет подключиться и тем или иным образом ввести правильный пароль, который может быть либо утёкшим в общие базы, либо получен методом подбора. Многие беспроводные сети вовсе работают без пароля, так как на предприятии могут не задумываться о потенциальной опасности со стороны третьих лиц. В свою очередь, злоумышленники, получив доступ к сети, могут заниматься воровством конфиденциальной информации, распространению вредоносного программного обеспечения и прочего. Необходимо более подробно описать различные виды атак на беспроводные сети. Среди них выделяют [6]:

- Создание «человека по середине», либо ложное лицо;
- DDOS атаки, нацеленные на нарушение работы сети;
- Создание ложной точки доступа;
- Проведение атак на различное сетевое оборудование;

Первый способ атак применяется при подключении к сетям, которые не защищены паролем, либо даже при взломе этой самой защиты банальным методом подбора или использованием определённых для этого программ. Данные атаки подразумевают под собой либо подслушивание, либо манипуляцию. Под подслушиванием подразумевается пассивный способ атаки, при котором злоумышленник наблюдает за целью, получает доступ к посещённым сайтом, видит передаваемую информацию, получает доступ к различным картам и счетам, а также логинам и паролям посредством наблюдения. Манипуляция же является методом активным, в котором злоумышленник не только ворует информацию, но и получает доступ к дистанционному управлению устройствами через беспроводные сети. Может происходить переадресация на различные страницы в интернете с вирусной угрозой на них с последующим заражением устройства.

Под DDOS атаками или атаками по распределённому отказу в обслуживании подразумевается атака, которая нарушает возможность использования беспроводной сети. Атаки могут происходить как на программном уровне, так и на аппаратном уровне. В случае аппаратной угрозы, находится уязвимость программы, через которую и осуществляется сама атака. В случае же аппаратном, со стороны злоумышленников осуществляется атака по перегрузке сети запросами, что не позволяет оборудованию вовремя обрабатывать эти самые запросы и она исчерпывает свои ресурсы, после чего, с целью сохранения системы, либо останавливает свою работу, либо перезагружается. Таким образом, хакеры направляют огромные пласты несвязанной информации с целью перегрузить систему и нарушить её работоспособность, что может полностью парализовать работу системы и нарушить обмен данными. В таком случае, сеть выходит из строя. Конечно, могут осуществляться ещё и атаки, которые используют генерации помех и замедляют или нарушают работоспособность устройств, но это уже сопоставимо с военными устройствами РЭБ и маловероятно их применение с целью нарушения сетей на том или ином предприятии.

Под ложной точкой доступа подразумевается создание ложной точки для подключения, когда в этом месте работает настоящая точка. Иными словами, создаётся клон точки для запутывания людей, с целью их подключения к этой сети и последующим воровством данных или нарушения работоспособности оборудования. Данный способ посредством ми-

микрировали под легальную точку доступа создан для хищения траффика и получения необходимой информации.

Под атакой на сетевое оборудование подразумевается действие, в котором при взломе беспроводной сети злоумышленники получают доступ также и к проводной сети, которая была подключена к беспроводным системам. Таким образом, недоброжелатели могут нарушить не только целостность и работоспособность беспроводной сети, но и также навредить основным системам на производстве, также завладев конфиденциальными данными. Беспроводные сети, за счёт своей незащищённости, могут создавать условия, в которых они же негативно влияют на безопасность более защищённых устройств, которые подключены через провод, что создаёт брешь в безопасности всей информационной системы.

В связи с этим, необходимо грамотно обеспечить безопасность беспроводных сетей, что, несомненно, является нетривиальной задачей. Основная трудность заключается в невозможности закрытия доступа от злоумышленников к сети и невозможность отслеживать из местонахождения из-за отсутствия необходимости прибывания в одном месте. В любом случае, существует перечень рекомендаций, которые могут существенно повлиять на безопасность сетей:

- Необходимо обеспечить физическую безопасность устройств по передаче сигнала беспроводных сетей. Например, необходимо обеспечить нахождение роутера подальше от различного оборудования, которое может создавать электромагнитные волны, в том числе микроволновок, которые своей работой могут мешать передаче данных или вовсе заглушить сигнал роутера. Также необходимо максимально минимизировать ситуацию, в которой работник или сотрудник может как-либо задеть роутер и тем самым поспособствовать его отключению, например, нажав на кнопку отключения или перезапуска, а также случайно выдернув провод питания;

- Необходимо посвятить время для создания максимально защищённого и надёжного логина и пароля для подключения к сети с целью избежания несанкционированного подключения. Всецело запрещается использовать те логины и пароли, которые предлагаются устройством при установке, а также подсказываются различными программами. Пароль должен быть надёжным и исключающим возможность банального подбора без необходимого оборудования, а также желательно время от времени обновлять его, как и логин;

- Ограничить трансляцию ID сети, то есть ограничить частоту или возможность её появления при поиске сетей со сторонних устройств. Таким образом, пользователь сможет найти сеть только при том условии, когда знает необходимый идентификатор этой самой сети, что поспособствует невозможности нахождения сети со стороны недоброжелателей, которые не знают идентификатора;

- Необходимо использовать фильтрацию подключаемых устройств, например, по MAC-адресам. Таким образом, фильтрация не позволит подключаться к сети устройствам, которые не содержат в настройках подключения MAC-адрес, что существенно снизит вероятность подключения различных неизвестных пользователей и упростит поиск и идентификацию пользователей и устройств, которые уже подключены;

- Необходимо устанавливать и настраивать протоколы защиты беспроводных соединений, таких как WPA и WPA2, что поспособствует общему уровню защищённости сетей;

- Поддержание в включенном состоянии различных брандмауэров и файрволлов для защищённости и фильтрации траффика извне от различных сетевых угроз;

- Необходимо использование надёжного антивируса и постоянного его обновления с целью поддержания безопасности сетей;

- Желательно настроить радиус действия сети таким образом, чтобы её применение ограничивалось пространством предприятия и не позволяло подключаться к сети извне,

не находясь тем самым на территории организации. Это затруднит возможность для злоумышленников подключиться к сети без физического нахождения на территории организации или предприятия, что соответственно вынудит идти на определённые риски;

- Запрет на внесения изменений в настройку сети роутера через WI-FI, что подразумевает необходимость прямого подключения по кабелю к устройству для того, чтобы внести изменения. В данном случае, злоумышленнику также придётся непосредственно прибывать на территории организации, когда у посторонних нет физического доступа к устройствам;

- Проведения различных необходимых треннингов для работников и персонала с целью повышения осведомлённости действиям злоумышленников, чтобы те имели понимания по различным методам несанкционированных подключений и могли не вестись на различные ложные точки доступа к сети;

Таким образом, беспроводные сети являются крайне полезными для формирования социального взаимодействия с людьми в различных общественных местах и организациях, но и при этом крайне опасны для внедрения со стороны недоброжелателей, которые способны либо нарушить саму систему обмена информации, либо похитить эту самую информацию с целью незаконного её использования [5].

Посредством второго пункта первой главы были перечислены основные риски государственного управления социально-экономическими процессами, а также риски при введении цифровых технологий для улучшения управления этими самыми процессами. Таким образом, государственное управление постоянно сталкивается с различными опасностями как со стороны внешней среды, так и внутренней, не имея при этом возможности наладить уверенный контроль над каждым из факторов этих рисков, что обусловлено человеческим фактором и остудившем возможности стопроцентного прогнозирования тех или иных последствий принятых или не принятых вовремя решений. Цифровизация в свою очередь существенно упрощает государственное управления, позволяя высвободить определённые мощности и перенаправить их, а также проводить анализ больших объёмов информации с целью повышения более эффективного государственного или производственного управления, но при этом порождает свои, специфические риски, которые в основном могут быть связаны с различными сбоями систем и нарушения безопасности этих самых систем извне с целью дестабилизации ситуации. Таким образом, государственное управление рисками в данное время существенно прогрессирует и не стоит на месте, но также сталкивается с различными опасностями, так как открываются новые пути и способы влияния на государства извне, посредством других, уже политических сторон, других государств или объединений этих самых государств, что способно пошатнуть безопасность как социальную, так и экономическую. Делается это с целью нанесения определённого политического урона государству посредством создания информационной и финансовой опасности для населения, что способно подтолкнуть его к недоверию к собственному государству и правительству посредством создания различных фэйков, пропаганды, общество ощущения незащищённости. Именно для этого и необходимо говорить, и анализировать как риски государственного управления социально-экономическими процессами с точки зрения уже устоявшейся теории, так и о изменении этой самой теории посредством вводимых инноваций, то есть вездесущей цифровизации, которая существенно влияет на каждый аспект жизни обычного гражданина, затрагивая работу различных структур и организаций, всецело влияя на экономику различных стран. Посредством осознания определённых рисков возможно найти способы по их идентификации, классификации и способами избегать или управлять ими, тем самым используя их для определённой выгоды или не позволяя наносить вред этой самой выгоде.

Источники и литература

1) 1. Абрамов В. И. Первый год реализации программ цифровой трансформации в регионах России: проблемы и результаты // В. И. Абрамов., В. Д. Андреев // Вопросы государственного и муниципального управления. – 2024. – №2. – С. 110-127.
2) 2. Версан В. Г. Концептуальные основы обеспечения качества управления социально-экономическими процессами // В. Г. Версан // Россия: тенденции и перспективы развития. – 2022. – №17-1. – С. 65-67.
3) 3. Вишнякова О. Н. Внедрение цифровых технологий в управление объектами спортивной инфраструктуры // О. Н. Вишнякова. // Интеллект. Инновации. Инвестиции. – 2024. – №2. – С. 23-30.
4) 4. Гаврилюк Е. С. Основные направления и факторы цифровой трансформации сектора науки и образования // Е. С. Гаврилюк, А. Г. Изотова // Экономика и экологический менеджмент. – 2021. – №1. – С. 22-30.
5) 5. Голлай А. В. Цифровая трансформация социально-экономических систем как конечный результат процесса цифровизации // А. В. Голлай, И. Н. Голлай, О. В. Логиновский // Вестник ЮУрГУ. Серия: Компьютерные технологии, управление, радиоэлектроника. – 2023. №2. – С. 65-81.
6) 6. Кабанов Ю. А. Цифровая трансформация государства и социально-экономическое неравенство в кросс-национальной перспективе // Ю. А. Кабанов., А. Г. Санина., Е. М. Стырин // ЖИСП. – 2024. – №2. – С. 195-208.
7) 7. Косинский П. Д. Организационно — экономический механизм управления Северо-Кузбасской агломерацией // П. Д. Косинский., В. В. Меркурьев., Е. В. Мягков // РЭиУ. – 2024. – №1 (77). – С. 1-17.
8) 8. Логиновский О.В. Проблемы цифровой трансформации субъектов Российской Федерации // О. В. Логиновский, Е. А. Лясковская, Р. Р. Габдулин // Вестник ЮУрГУ. Серия: Компьютерные технологии, управление, радиоэлектроника. – 2023. №3. – С. 76-91.
9) 9. Парфенов Д. А. Развитие механизма обеспечения экономической безопасности в РФ в условиях цифровизации // Д. А. Парфенов // Вестник Московского университета. Серия 21. Управление (государство и общество). – 2020. – №4. – С. 106-121.
10) 10. Попов Е. В. Проблемы экономической безопасности цифрового общества в условиях глобализации / Е. В. Попов, А. А. Семечков // Экономика региона. Т. 14, вып. 4. – 2018. – С. 1088–1099.