Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)
Институт экономики и менеджмента
Учебный офис Высшей школы бизнеса

ДОПУСТИТЬ К ЗАЩИТЕ В ГЭК
Руководитель ООП
канд. экон. наук, доцент
_____ А.М.Гринкевич
«15» 06 2020 г.

ДИПЛОМНАЯ РАБОТА

ВЛИЯНИЕ ЦИФРОВОЙ ЭКОНОМИКИ НА ОБЕСПЕЧЕНИЕ НАЦИОНАЛЬНОЙ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

по специальности 38.05.01 - Экономическая безопасность

Федоров Евгений Олегович

Руководитель ВКР
канд. экон. наук, доцент
_____ В.Б. Романюк
«15» 06 2020 г.

Автор работы
студент группы № 224851
_____ Е.О. Федоров

Томск 2020

Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)
Институт экономики и менеджмента
Учебный офис высшей школы бизнеса

УТВЕРЖДАЮ
Руководитель ООП
канд. экон. наук, доцент
_____ А.М. Гринкевич
«17» 12 2019 г.

ЗАДАНИЕ

по подготовке дипломной работы
студенту Федорову Евгению Олеговичу группы № 224851
фамилия, имя, отчество

1. Тема ВКР Влияние цифровой экономики на обеспечение национальной экономической безопасности

2. Срок сдачи студентом выпускной квалификационной работы специалиста
в деканат 13.06.2020
в ГЭК 16.06.2020

3. Исходные данные к работе

Цель работы - рассмотреть государственный контроль над Интернет-ресурсами и выявить как возможные опасные последствия этого явления, так и наиболее оптимальные формы осуществления такого контроля путём сравнительно-правового анализа российского и зарубежного опыта в данной области.

Задачи:
- рассмотреть государственные услуги и развитие цифровой экономики в России;
- проанализировать влияние цифровой экономики в банковской сфере;
- рассмотреть цифровую экономику в платформах сети интернет;
- рассмотреть проблемы цифровой экономики с позиции национальной безопасности;
- проанализировать опыт США безопасности цифровой экономики;
- проанализировать опыт Европы безопасности цифровой экономики;
- проанализировать опыт России безопасности цифровой экономики
- рассмотреть совершенствование нормативно законодательной базы в сфере безопасности цифровой экономики;
-рассмотреть осуществление контроля и мониторинг государства с использованием цифровых технологий;
- проанализировать способы измерения доли цифровой экономики.

Объект исследования - влияние цифровой экономики на обеспечение национальной экономической безопасности.

Предмет – особенности правового регулирования цифровой экономики на обеспечение национальной экономической безопасности

Методы - синтез, исторический, наблюдение, SWOT анализ.

4. Краткое содержание работы

1 Сферы деятельности государства с применением цифровой экономики
2 Современные подходы к регулированию деятельности платформ интернета государством
3 Укрепление национальной безопасности на базе цифровой экономики

5. Указать предприятие, организацию по заданию или на примере которого выполняется работа
6. Перечень графического материала
5 таблиц, 2 рисунка
7. Дата выдачи задания 17.12. 2019 г.

Руководитель ВКР
канд. экон. наук, доцент _____ В.Б. Романюк

Задание принял к исполнению _____ 17.12.2019
дата, подпись студента

АННОТАЦИЯ

Структура научной работы включает введение, 3 главы, 10 параграфов, заключение, список использованных источников и литературы. Общий объем работы составил 69 страниц, в него вошли: 2 рисунка, 5 таблиц, 51 источник.

Ключевые слова: цифровая экономика, национальная безопасность, цифровые технологии, государственные услуги, банковская сфера.

Объектом исследования выступает влияние цифровой экономики на обеспечение национальной экономической безопасности.

Предмет состоит в изучении особенности правового регулирования цифровой экономики на обеспечение национальной экономической безопасности.

Методы исследования - исторический, наблюдение, SWOT анализ.

В соответствии с поставленными задачами, в работе были рассмотрены государственные услуги в условиях цифровизации экономики России. Определенны роль цифровой экономики в банковской сфере, рассмотрены модели цифровых банков. Так же рассмотрены проблемы цифровой экономики с позиции национальной безопасности. Проанализирован опыт США, Европы и России в области безопасности цифровой экономики. Объясняются способы измерения доли цифровой экономики.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ 7
1 Сферы деятельности государства с применением цифровой экономики 9
1.1 Государственные услуги и развитие цифровой экономики в России 9
1.2 Влияние цифровой экономики в банковской сфере 20
1.3 Цифровая экономика в платформах сети интернет 24
1.4 Проблемы цифровой экономики с позиции национальной безопасности 27
2 Современные подходы к регулированию деятельности платформ интернета государством 31
2.1 Опыт США 31
2.2 Опыт Европы 38
2.3 Опыт России 45
3 Укрепление национальной безопасности на базе цифровой экономики 49
3.1 Совершенствование нормативно законодательной базы 49
3.2 Контроль и мониторинг государства с использованием цифровых технологий 54
3.3 Способы измерения доли цифровой экономики 59
ЗАКЛЮЧЕНИЕ 63
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ 65

ВВЕДЕНИЕ

В настоящее время современное общество характеризуется стремительным переходом от индустриального к постиндустриальному, информационному типу, этапу. Данные изменения проявляются в ряде качественных преобразований человеческой жизни: информация становится предметом производства и объектом коммерческих сделок, первоосновой всех направлений деятельности человека-экономического, политического и других; государства и их отдельные структуры взаимодействуют между собой на основе информационных технологий и принимают активное участие в управлении информационным пространством (в тесном контакте с общественными организациями).

Цель настоящей работы заключается в том, чтобы рассмотреть государственный контроль над Интернет-ресурсами и выявить как возможные опасные последствия этого явления, так и наиболее оптимальные формы осуществления такого контроля путём сравнительно-правового анализа российского и зарубежного опыта в данной области.

Научная новизна настоящей работы обусловлена тем, что проблему государственного контроля над Интернетом невозможно исследовать полностью и всесторонне, так как развитие этой проблемы следует параллельно с развитием информационных технологий,— следовательно, она всегда будет представлять исследовательский интерес для любого поколения учёных.

Актуальность настоящей работы обусловлена именно тем фактором, о котором говорилось выше — бурным развитием информационной сферы, влекущим за собой увеличение дифференциации правоотношений в ней и повышение числа правовых инструментов в руках государства для их необходимого контроля.

Одним из условий стабильного развития производства в стране является обеспечение единства измерений. Данное условие реализуется путём обязательной периодической поверки средств измерений, используемых в сферах государственного регулирования обеспечения единства измерений, что определено в федеральном законе № 102. Из-за постоянного увеличения количества используемых средств измерений оформление и использование результатов значительно увеличивает сроки проведения поверки.

В связи с этим потребитель несёт убытки, связанные с отсутствием средств измерений на рабочих местах. Далее рассмотрены необходимые изменения в системе обеспечения единства измерений для повышения её эффективности.

Объект исследования - влияние цифровой экономики на обеспечение национальной экономической безопасности.

Предмет – особенности правового регулирования цифровой экономики на обеспечение национальной экономической безопасности.

В работе решаются следующие задачи:

- рассмотреть государственные услуги и развитие цифровой экономики в России;

- проанализировать влияние цифровой экономики в банковской сфере;

- рассмотреть цифровую экономику в платформах сети интернет;

-рассмотреть проблемы цифровой экономики с позиции национальной безопасности;

- проанализировать опыт США безопасности цифровой экономики;

- проанализировать опыт Европы безопасности цифровой экономики;

- проанализировать опыт России безопасности цифровой экономики

- рассмотреть совершенствование нормативно законодательной базы в сфере безопасности цифровой экономики;

- рассмотреть осуществление контроля и мониторинг государства м использованием цифровых технологий;

- проанализировать способы измерения доли цифровой экономики.

Границы исследования – Российская Федерация, государства Европы и США.

При написании работы использовались работы следующих авторов: Потапенкова И.В., Морщакова, Т., Кудрявцев В.Н., Трусов А.И., Литвинова И.В., Стогова Н.С.

Методы, использованные при написании работы – синтез, исторический, наблюдение, анализ.

Работа состоит из введения, трех глав, заключение и списка использованных нормативно-правовых актов и источников.

Первая глава посвящена теоретическим вопросам осуществления безопасности в сфере цифровой экономики.

Вторая глава посвящена рассмотрению особенностей безопасности цифровой экономики В США, странах Европы, России.

Третья глава рассматривает современные тенденции и развития информационной безопасности цифровой экономики в современной России.

1 Сферы деятельности государства с применением цифровой экономики

1.1 Государственные услуги и развитие цифровой экономики в России

С появлением ЭВМ, люди все чаще стали поручать важные задачи машине и с движением прогресса, передаваемых машинам задач стало больше, а их сложность росла в геометрической прогрессии.

Сегодня благодаря интернету и огромному потоку цифровой информации машины выполняют задачи, которые даже коллективному разуму будет сложно решить. Искусственный интеллект создал новую отрасль оцифровки и обработки данных. Во всем мире искусственный интеллект и цифровые технологии уже давно используются в экономике. Что касается нашей страны, то в 2016 году президент России Владимир Путин в своем послании Федеральному собранию предложил запустить масштабную системную программу экономического развития нового технологического поколения - цифровую экономику. Программа предусматривает меры по созданию законодательных, технических, организационных и финансовых условий для развития цифровой экономики в России. Таким образом, она официально признана важной частью государственного экономического развития.

В настоящее время цифровая экономика находится в стадии формирования, поэтому вполне естественно, что в мире не существует единого понимания, что такое цифровые технологии и что такое цифровизация экономики.

В Российской Федерации официальное государственное определение данному феномену появилось относительно недавно. Так в указе Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» дается следующее определение: «Цифровая экономика – хозяйственная деятельность, в которой ключевым фактором производства являются данные в цифровом виде, обработка больших объемов и использование результатов анализа которых по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг».[1]

Одним из самых ярких представителей цифрой экономики в России мы считаем Сбербанк. Он один из первых стал предлагать услуги интернет-банка и то, как быстро он внедряет новые технологии и чувствует волну модернизации, поражает. К сожалению, такая

[1] О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы [Электронный ресурс]: указ Президента РФ от 09.05.2017 № 203 // КонсультантПлюс: справочная правовая система. - URL: http://www.consultant.ru. (дата обращения: 15.04.2020)

глобальная оцифровка данных имеет свои недостатки. Достаточно вспомнить, что нет программы, которую нельзя взломать и то, что вся экономика и все возможности, связанные с обменом средств, проходят через интернет банки, свидетельствует о потенциале не только украсть данные о передаче и отслеживать их, но и повлиять на перевод средств. Прежде всего, стоит отметить, что контроль в сфере цифровых услуг снижается, а возможности случаев мошенничества увеличивается. Увеличивают риск утечки информации, что требует более высокого уровня защиты.

В глобальном плане из-за цифровой экономики общий экономический фон стал нестабилен, так как на рынке появилось множество цифровых валют, множество сервисов способных переводить физические ресурсы в реальные деньги, это очень сильно пошатнуло экономику многих стран. Всем известный биткоин по сей день приносит огромные доходы лицам, вовремя инвестировавшим в него, и превратился из средства расчета в способ сохранения и преумножения дохода.

Для того, чтобы оценить возможности и угрозы, сильные и слабые стороны процесса цифровизации экономики, была составлена матрица SWOT анализа (таб. 1)

Таблица 1 - SWOT анализ процесса цифровизации экономики

Сильные стороны цифровизации	Слабые стороны цифровизации
1. Экономия времени; 2. Возможности дистанционной работы; 3. Быстрота проведения операций и оказание услуг; 4. Исключение бумажного документооборота;	1. Опасность хранения данных; 2. Вымещение значительной части работоспособного населения с рынка; 3. Возможная утопия; 4. Прозрачность экономики;
Возможности цифровизации	**Угрозы цифровизации**
1. Расширение ассортимента товаров за счет скачкообразного развития интернет рынка; 2. Возможность глобального контроля средств; 3. Полный переход к безналичному расчету;	1. Рост продаж товаров-заменителей; 2. Замедление роста рынка угроза; 3. Появления новых конкурентов; 4. Действия хакеров;

Сильными сторонами цифровизации экономики, мы считаем:

1. Экономия времени - благодаря интернет рынку и всевозможным торговым площадкам;

2. Возможности дистанционной работы – цифровизация экономики делает возможным работу из дома.

3. Быстрота проведения операций и оказания услуг- благодаря почти моментальной передачи информации в любой уголок планеты.

4. Исключение бумажного документооборота – с приходом цифровой экономики необходимость в бумажном документообороте отпала.

Слабыми сторонами цифровизации экономики, мы считаем:

1. Опасность хранения данных – существует вероятность утечки информации, а также опасность ненадежности большинства ресурсов;

2. Вымещение значительной части работоспособного населения с рынка - обусловлена заменой их машинами, что в последствии сказывается на высоком уровне безработицы.

3. Возможная утопия - подразумевается, что развивающейся ИТ-технологии в скором времени позволят зарабатывать деньги из воздуха и влиять на экономику с такой силой, что физические ресурсы могут перестать иметь ценность;

4. Прозрачность экономики - потенциальная открытость информации о покупках предпочтениях и т.п., что сокращает поиск нужных данных, но приводит к контролю населения маркетологами, через определенное навязывание товара или даже доскональное изучение вкусов и поведения человека.

Возможности, которые открываются благодаря цифровизации экономики настолько обширны, что оценить ее влияние на изменение жизни общества в полной мере сегодня не представляет возможным. Возможно лишь некоторое «прощупывает» отдельных направлений.

Скачкообразное развитие интернет рынка, позволяет приобретать все нужные товары, не выходя из дома. И дело здесь не в лени, а в быстром темпе жизни человечества. К сожалению, с каждым годом мир становится все быстрее и быстрее, и человеку сложно в нем находится, и успевать заниматься тем, чем он хочет. Благодаря интернет операциям освобождается огромный отрезок времени. А в будущем с развитием интеллектуальной системы запросов и предложений, человеку не придется тратить время даже на поиск нужной информации и все будет доступно в "одной кнопке".

Цифровая экономика делает возможный глобальный контроль средств и полный переход к безналичному расчету. Имеется ввиду, что благодаря переходу к цифровой экономике и в будущем вероятнее всего произойдет отказ от наличных, затраты на производство купюр и прочие связанные с этим вещи больше будут не нужны. Теперь нужно

будет лишь глобально отслеживать поступающие средства с помощью искусственного интеллекта и контролировать все денежные операции, что бы избежать возможных махинаций. Это приведет к увеличению скорости проведения операций, упрощению процедуры выхода продукции на глобальные рынки и возможности новых способов заработка.

Безусловно возможности, цифровизации экономики могут значительно облегчить жизнь, но также не стоит забывать и об угрозах, вытекающих из перехода к "цифровой жизни".

Рост продаж товаров заменителей оказывает негативное влияние на экономический рост Российской Федерации, требует от государства больших финансовых затрат на поддержание экономики, а также влечет за собой замедление роста рынка;

Благодаря цифровизации экономики появилась возможность покупки товаров и заключение сделок с иностранными гражданами. Появления новых «игроков» приведет к снижению конкурентоспособности и может стать серьезной угрозой для российских компаний.

В современном мире все большее количество информации хранится в электронном виде и подвергается серьёзной угрозе со стороны киберпреступников. Основные атаки приходятся на мобильные устройства и финансовые мобильные приложения, связанные с дистанционным банковским обслуживанием.

Россия – страна, идущая по пути догоняющего развития в области внедрения ИТ-технологий. Однако, зарубежные аналитики считают, что у России есть потенциал развития цифровой экономики, и именно она может лечь в основу богатства страны. Соавтор программы социально-экономического развития России "Стратегия роста" Борис Титов считает, что Россия не должна отставать в развитии важнейших прорывов, а быть одной из ведущих держав со стороны технологического развития.

Так, уже сегодня на просторах нашей большой страны активно функционирует, и получила популярность электронная система государственных услуг на сайте www.gosuslugi.ru. Благодаря этому ресурсу, каждый гражданин может удаленно решить следующие вопросы: осуществить платежи, подать заявку в детский сад, записаться на приём к врачу и др. Ожидается, что к 2020 году доля граждан, использующих его возможности, достигнет 70%, а 95% населения страны будут подключены к всемирной сети. Специалистами отмечено, что зарождается система электронного правительства и развивается концепция открытых данных.

Для дальнейшего скачка в экономической и других сферах, России необходимо создавать собственные передовые разработки и научные решения. Нужны квалифицированные кадры, инженеры, рабочие, готовые выполнять задачи нового уровня и иметь способность к быстрой адаптации в цифровой среде. Для этого необходимо выстроить современную систему образования, организовать подготовку преподавателей на основе передовых международных стандартов и проводить всевозможные агитации и консультации школьников, для их понимания и представления себя в этом глобальном механизме. Основной упор нужно сделать на дополнительное бесплатное образование в виде курсов или занятий для обеспечения населения нужной информацией и подготовкой.

Предоставление государственных услуг в электронном виде являлось основным направлением реализации программы «Электронная Россия» начиная с 2002 г. Государственные услуги в электронном виде предоставляются через единый государственный портал государственных услуг www.gosuslugi.ru, а также через региональные порталы.

Подготовка Федеральной целевой программы «Электронная Россия (2002-2010 годы)» началась сразу после принятия главами государств «Группы восьми» Окинавской хартии Глобального информационного общества от 22.07.2000. Основная цель программы «Электронная Россия (2002-2010 годы)» заключалась в создании инфраструктуры электронного правительства.

Пункт 6 ст. 2 Федерального закона № 210-ФЗ определяет порядок предоставления государственных и муниципальных услуг в электронной форме, включая использование единого портала государственных и муниципальных услуг и (или) региональных порталов государственных и муниципальных услуг, а также использование универсальной электронной карты.

В рамках такого предоставления осуществляется электронное взаимодействие между государственными органами, органами местного самоуправления, организациями и заявителями. Одним из достоинств закона о государственных и муниципальных услугах является утверждение принципа «одного окна» при получении услуги и возможность ее оказания в электронной форме. Единой точкой доступа в России для физических и юридических лиц к информации о государственных услугах в электронном виде выступает «Единый портал государственных и муниципальных услуг». Прежде чем воспользоваться услугами портала, необходимо сначала зарегистрироваться, а потом получить пароль доступа. Чтобы выявить проблемы предоставления государственных услуг, рассмотрим предоставление электронных услуг.

Данная инфраструктура должна была быть направлена на реализацию открытости и доступности для граждан информации в электронном виде о деятельности и услугах государственных органов власти, межведомственный информационный обмен посредством ИТ, а также единый государственный надзор за эффективностью функционирования государственных органов власти, что в итоге поможет снизить уровень бюрократической нагрузки на граждан и бизнес. Программой предусматривалась разработка проекта долгосрочной целевой программы «Информационное общество (2011-2020 годы)». Основной целью данного проекта было создание целостной и эффективной системы использования информационных технологий, при которой граждане смогут получать максимум выгод. Однако, оказание государственных и муниципальных услуг с помощью ИТ (в электронной форме) оказалось осложнено по нескольким причинам, определившимся в ходе реализации концепции «Электронное правительство»:

1. На некоторые услуги поступает не более 2-3 заявок в год. Между тем затраты на них бюджет несет такие же, как и на популярные услуги. 20 представленных на портале услуг на настоящий момент удовлетворяют 80 % запросов пользователей.

2. Существенные различия информационных технологий, используемых различными государственными и муниципальными органами власти, в качественном и количественном отношении.

3. Недостаточно развита и проработана нормативно-правовая база предоставления электронных услуг гражданам, а также не до конца сформулированы стандарты и правила по предоставлению данных услуг с помощью ИТ.

4. Отсутствует надежная система, гарантирующая информационную безопасность в процессе взаимодействия государственных органов с общественными организациями и гражданами. Для анализа рассматриваемой авторами проблемы, выраженной в недостаточном уровне обеспеченности информационными технологиями различных уровней власти и недостаточном предоставлении населению качественных публичных услуг был использован метод ПЕСТ-анализа. Результаты такого анализа документируются в форме матрицы, по вертикали которой располагаются факторы макросреды, а по горизонтали сила их влияния, которую оценивают в баллах, рангах и иных единицах измерения. Проставленные в таблице баллы по факторам свидетельствуют о величине их влияния на развитие и внедрения «Электронного правительства», предоставления государственных и муниципальных услуг в Российской Федерации. Цель метода: отслеживание изменений макросреды по четырем узловым направлениям и выявление тенденций, неподконтрольных организации, но оказывающих влияние на результаты принятых стратегических решений.

Достоинства метода: наглядность, простота освоения и применения; позволяет определить бизнес-возможности и использовать их в полном объеме. Недостатки метода: доступ к внешним источникам данных может быть трудоемким и дорогостоящим; для обеспечения эффективности необходимо проводить его на регулярной основе.

Необходимо отметить, что среди основных политических факторов выделяется заинтересованность органов власти в формировании электронного общества в России, от которой зависит дальнейшее развитие информационных технологий в области деятельности государственных и муниципальных учреждений.

Масштаб, темп и география цифровой экономики не могут не впечатлять. Глобальная диджитализация привела к трансформации структуры экономики. Рост внутриотраслевой конкуренции, расширение рынка, повышение конкурентоспособности, доступность товаров и услуг, увеличение покупательной способности населения, и рост национальных экономик в целом – это результат освоения цифровых возможностей.

Действия в цифровой экономике осуществляются на абсолютно новых скоростях, а ограничением является лишь незнание ее реального потенциала. Скорость сегодня является во многом определяющим фактором. Само формирование инновационных волн происходит с ускорением, что оказывает на экономику все более ощутимый эффект.

На сегодняшний день рынок средств технической безопасности является относительно зрелым и характеризуется достаточно плотной конкуренцией, что требует от компаний постоянного поиска средств наращивания конкурентных преимуществ. Экспертами прогнозируется рост мирового рынка физической безопасности до $105,26 млрд к 2020 году, при среднем ежегодном росте 9,98%.

Рассмотрим факторы, которые обеспечат рыночный рост и определим возможные точки роста. Все большая значимость отводится возможности удаленного доступа с помощью мобильных устройств, а также управлению с их помощью не только системами безопасности и видеонаблюдения, но и другими электронными устройствами и системами обеспечения объекта.

Здесь, в сегменте обеспечения безопасности жилой недвижимости, среднегодовой темп роста за период с 2017 по 2020 гг. прогнозируется в размере 7%.[2] Драйвером роста рынка систем безопасности в жилом секторе будет являться обеспокоенность населения растущим уровнем преступности, терроризма. Свою нишу займут также удаленный доступ и Интернет вещей (IoT), как перспективный тенденции развития систем безопасности для жилых сооружений. Стремительное развитие прогнозируется и на рынке физической

[2]Интернет-портал систем безопасности [Электронный ресурс] - URL: http://www.techportal.ru (дата обращения: 01.04.2020)

безопасности в секторе розничной торговли, где среднегодовой темп роста за период с 2017 по 2020 гг. стабильно будет составлять 6%.

Причинами роста рынка физических систем безопасности в секторе рыночной торговли является растущее число розничных магазинов, а также эффективность контроля товарооборота с их помощью и уменьшение рисков потери вследствие краж и административных ошибок.

Одно из главных конкурентных преимуществ ИТ-компаний и главный тренд последних лет - это возможность предоставления комплексных решений под запросы различных групп потребителей - интеграция инженерных систем и систем безопасности.

Системы безопасности представляют собой как стандартные решения – охранная сигнализация, системы контроля и управления доступом (СКУД), системы пожаротушения, видеонаблюдение, так и специальные средства - детекторы веществ, досмотровые комплексы, тепловизоры, сканеры тела человека, устройства идентификации и пр., объединяемые понятием «комплексные системы безопасности» (КСБ). Интеграция систем в единую систему позволяет не только устранить локально недостатки каждой системы, но и организовать новую систему, представляющую собой единую информационную среду, реализующую функции получения, обработки и анализа информации, – системы, которая обладает способностью гибко реагировать на различные события. Интеграция ИТ-инфраструктуры, ИТ-сервисов и инженерных систем – это повышенная эффективность работы систем, но при этом сниженная себестоимость отдельных элементов.

На рынке технической безопасности прослеживается технологический тренд в применении систем биометрической идентификации. По данным S&P рост рынка систем биометрической идентификации в период 2017 – 2020 гг. составит более 25%.

В инженерной инфраструктуре все большее предпочтение отдают IP-технологиям и всевозможным системам виртуализации. Однако, если IP-технологии уже достаточно хорошо закрепились на рынке, то системы виртуализации еще совсем новый тренд для российского рынка технической безопасности.

На сегодняшний момент аналитики оценивают объём рынка виртуальной и дополненной реальности в выручке от продаж контента и устройств в несколько миллиардов долларов, однако, отмечают, что к 2020 году объем данного рынка будет составлять более $150 млрд.

Следует отметить, что виртуальная и дополненная реальность в области физической безопасности – это перспективный инструмент, повышающий эффективное время отклика. Так в компании S3 Security and Defense Consultants прошли тесты дополненной реальности

VuZix M100. Тестировалось время, например, для вызова плана здания по этажам, а также формирования самого быстрого и безопасного пути перемещения по объекту.

Оценить преимущества использования дополненной реальности можно и при монтаже и обслуживании систем безопасности. Также свои преимущества показывают фото и видеозахваты при использовании их для уменьшения времени реагирования на тревожное событие и с целью влияние графических эффектов на успешность переговоров с клиентом.

Потенциал данного сегмента рынка велик. Потенциалом развития технологии в отрасли безопасности эксперты отмечают также «рентгеновское зрение» и точное GPS позиционирование. Ожидается, что в следующие 20 лет может быть автоматизировано 47% всех рабочих мест. В условиях современной реальности не остается сомнений, что 80% работ в ИТ могут быть заменены автоматизацией. Рынок систем технической безопасности не исключение. Запуск данного процесса будет спровоцирован применением искусственного интеллекта (ИИ), являющего собой более эффективную замену человеку, способного работать с большими данными. Все большее количество процессов, за которые раньше отвечали только люди, теперь способны решать машины и делают это качественнее и во многих случаях дешевле.

В разработке ИИ существует обширная область, изучающая методы построения алгоритмов, способных самостоятельно обучаться — машинное обучение. Машинное обучение необходимо при отсутствии четкого решения какой-либо задачи. В данном случае целесообразным будет не поиск правильного решения, а создание механизма, способного самостоятельно придумать метод для его поиска. Нейросеть - это моделирование работы человеческой нервной системы, особенностью которой является способность к самообучению с учетом предыдущего опыта. Таким образом, каждый следующий раз ошибок у системы все меньше.

Подобно нашей нервной системе, нейросеть представляет собой отдельные вычислительные элементы – нейроны, расположенные на нескольких слоях. Данные, которые поступают на вход нейросети, проходят последовательную обработку на каждом слое сети. Следует отметить, что каждому нейрону соответствуют определенные параметры, изменяющиеся в зависимости от полученных результатов, что и представляет собой обучение сети.

Нейронные сети способны изменить работу целых отраслей. Однако, общество реагирует неоднозначно: одни испытывают восторг от возможностей нейросетей, а другие – сомневаются в их пользе как специалистов. Одно ясно абсолютно точно, потенциал нейронных систем огромен. Для рынка систем технической безопасности применение

нейронных сетей – это перспектива развития, а, возможно, внедрение нейронных сетей на рынок технической безопасности приведет к революции в отрасли. По оценкам ООН, к 2050 году 67% населения Земли будут проживать в городах.

На сегодняшний день уже существует проблема перенаселения некоторых мегаполисов. Очевидны несовершенства муниципальных служб: затруднения с уборкой мусора, неоднородность поставки коммунальных ресурсов и электроэнергии от района к району и т.д. С целью предоставления качественных городских услуг администрация все чаще внедряет различные информационные системы.

Проведение административной реформы в Российской Федерации вызвало появление в юридической теории и практике категории «государственные услуги». Административная реформа – комплексные изменения в системе государственного управления: как в функционировании самих органов администрирования (внутренние административные процессы и процедуры), так и в организации взаимодействия с гражданами и различными общественными институтами и организациями. [3]

Президент РФ в своих посланиях Федеральному Собранию РФ неоднократно, начиная с 2000 г., подчеркивал необходимость и значимость преобразований в сфере государственного управления. В качестве цели административной реформы Президентом называлось обеспечение безусловного исполнения и такой прямой обязанности государства как предоставление качественных публичных услуг; указывалось необходимость повышения качества предоставляемых населению государственных и муниципальных услуг. Прежде всего, отмечал Президент, это относится к столь значимым для общества сферам, как образование, здравоохранение и культура. От успешности действий в этих сферах непосредственно зависят условия жизни населения.

Как предусматривается ст. 4 Федерального закона «О порядке рассмотрения обращений граждан Российской Федерации» обращение граждан – это направленное в государственный орган, орган местного самоуправления или должностному лицу в письменной форме или в форме электронного документа предложение, заявление или жалоба, а также устное обращение гражданина в государственный орган, орган местного самоуправления.

Конституционный Суд Российской Федерации в абз. 4 п. 2 Постановления от 18 июля 2012 г. № 19-П «По делу о проверке конституционности части 1 статьи 1, части 1 статьи 2 и статьи 3 Федерального закона «О порядке рассмотрения обращений граждан

[3] Срибный В.И. Составляющие механизма обеспечения экономической безопасности Российской Федерации / В.И. Срибный // Институт финансово-кредитных отношений в условиях рыночных трансформаций: сборник статей научно-практического семинара (г. Симферополь, 30 ноября 2016 года). – Выпуск 4. – Симферополь: ООО «Антиква», 2017. – С. 409-412.

Российской Федерации» в связи с запросом Законодательного собрания Ростовской области» подчеркивается, что «право граждан на обращение, закрепленное Конституцией Российской Федерации (ст. 33), в совокупности с другими элементами правового статуса личности ….. является способом оптимизации деятельности органов публичной власти».

Таким образом, само появление в законодательстве понятия «государственные услуги», развитие правового регулирования процесса их оказания свидетельствует о новой, хочется надеяться – более качественной ступени развития взаимодействия органов власти и граждан. Термин «услуга» встречается как в сфере частного, так и публичного права. Оказание услуг представляет собой, во-первых, один из объектов гражданских прав (ст. 128 ГК РФ).

Гражданский кодекс РФ (ст. 779) подразумевает под услугой совершение определенного действия или осуществление определенной деятельности. В теории гражданского права предложено большое количество понятий услуги и единства мнений ученых по этому вопросу нет.

Приведем только одно определение, которое, на наш взгляд, более точно и полно отражает сущность услуги: услуга выражается «в виде определенной правомерной операции, т.е. в виде ряда целесообразных действий исполнителя либо в деятельности, являющейся объектом обязательства, имеющей нематериальный эффект, неустойчивый вещественный результат, либо овеществленный результат, связанный с другими договорными отношениями, и характеризующейся свойствами осуществимости, неотделимости от источника, моментальной потребляемости, неформализованности качества».

Таким образом, признаками услуги являются неотделимость ее результата (полезного эффекта) от личности исполнителя, отсутствие возможности накопления, хранения и гарантированности результата. Федеральный закон «Об организации предоставления государственных и муниципальных услуг» (подп 1. ст. 2) определяет государственную услугу как деятельность по реализации функций федерального органа исполнительной власти, государственного внебюджетного фонда, исполнительного органа государственной власти субъекта Российской Федерации, а также органа местного самоуправления, которая осуществляется по запросам заявителей в пределах установленных нормативными правовыми актами Российской Федерации и нормативными правовыми актами субъектов Российской Федерации полномочий органов, предоставляющих государственные услуги.

Особенности предоставления государственной услуги в электронном виде: заявитель может подать заявление с использованием электронной почты и (или) электронной

формы, размещенной на официальном сайте в сети Интернет, а также на Едином портале государственных и муниципальных услуг (www.gosuslugi.ru) Одним из наиболее эффективных способов организации предоставления государственных и муниципальных услуг в Российской Федерации сегодня признано оказание услуг с помощью специально оборудованных пунктов приёма и выдачи документов – многофункциональных центров предоставления услуг. Многофункциональные центры предоставления услуг (далее – МФЦ) – учрежденная и уполномоченная высшей исполнительной властью РФ организация, обеспечивающая предоставление государственных и муниципальных услуг федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации, органами местного самоуправления в режиме «одного окна».

1.2 Влияние цифровой экономики в банковской сфере

В ближайшее время очевидно получат новую форму и содержание основные сферы жизнедеятельности человечества – экономика и управление, наука и безопасность. Цифровые технологии проникают в нашу жизнь всё глубже, что является одной из характерных особенностей будущего мира.[4]

А в июле 2017 года Правительством РФ была уже разработана и утверждена программа развития цифровой экономики Российской Федерации до 2035 года.[5]

Процессы цифровизации наиболее наглядно отражаются в финансовой сфере, а именно в банковском секторе как главенствующем сегменте экономики любой страны. К примеру, в РФ в Центральном банке России создан «Департамент финансовых технологий, проектов и организации процессов».[6] В конце 2016 года по инициативе Банка России и ключевых участников отечественного финансового рынка была создана Ассоциация «ФинТех».

Это уникальная площадка для конструктивного диалога регулятора с представителями бизнеса, а ее целями являются: создание условий для цифровизации экономики и разработка и внедрение новых технологических решений в целях обеспечения развития финансового рынка РФ. В неё вошли самые крупные представители финансового

---

[4] Майоров А.В., Еремеев С.Г., Волкова А.М., Потапов А.Д. Цифровые технологии в управленческой деятельности: философско-антропологический и прикладной аспекты // Вестн. Ленингр. гос. ун-та им. А.С. Пушкина. – 2019. – № 1. – С. 34–48.

[5] Программа развития цифровой экономики в Российской Федерации до 2035 года. – С. 19–20 // Ассоциация электронных торговых площадок [Электронный ресурс]. – URL: http://www.aetp.ru/news/item/410256 (дата обращения: 15.04.2020)

[6] Космачева Н.М., Стецюнич Ю.Н. Оценка качества управления кредитными рисками в банках по критерию просроченной задолженности // Экономика нового мира. – 2018. – № 4 (12). – С. 47–58.

сектора страны – Банк России, Сбербанк, Газпромбанк, ВТБ, РоссельхозБанк, Альфа-Банк и другие.

Мировой банковский мир стремительно меняется, так же, как и пересматриваются подходы в регулировании, и самое главное – окончательно изменился банковский клиент, который оказался перед невероятно большим числом предложений со стороны финансовых технологий (совр.: финтех). Проблема в погоне за качественной, не дорогой, а самое главное удобной услугой решается благодаря появлению необанков или как мы привыкли их называть онлайн-банков.

Характерными плюсами, в пользу необанков клиенты считают:

1. Совершенно прозрачные операции
2. Никаких скрытых комиссий
3. Возможность отслеживания текущих операций в режиме онлайн
4. Минимальная плата за обслуживание
5. Поддержка в формате 24/7

В IBM (International Business Machines – один из крупнейших производителей электроники, компьютерной техники и программного обеспечения) считают, что существующие новые банки, можно разделить на четыре модели, по степени проникновения цифровых технологий и организации бизнес-процессов. (таб.2)

Таблица 2 – Модели новых банков по стремени проникновения цифровых технологий[7]

Модели	Описание
«Модель А»	Цифровой банковский бренд, выделенный из «материнского» классического банка. Некоторые банки «Модели А», создают попутные торговые марки цифровых банков. Банкиры этой группы считают, что создание нового бренда с уникальным ценностным предложением и продуктами, является более безопасной стратегией. Эти цифровые бренды могут продаваться как новый банк, но обычно используют инфраструктуру своих родительских банков.

[7] Американский финансово-экономический журнал Forbes / Официальный сайт [Электронный ресурс]. – URL: https://www.forbes.ru/biznes/371421-ibm-predlozhil-novuyu-klassifikaciyu-cifrovyhbankov (дата обращения: 26.04.2020).

Окончание таблицы 2

«Модель B»	Банки с цифровыми дистанционными каналами. Цифровые банки «Модели B» полагают, что превосходный пользовательский опыт должен выходить за рамки брендинга и может быть достигнут путем предоставления новых мобильных и онлайн-приложений, ориентированных на пользовательский опыт. Вместо того чтобы создавать банк с нуля (что дорого), эти банки перепродают продукты реального банка и должны перераспределять средства клиентов на застрахованные счета реального банка.
«Модель C»	Цифровая «дочка» классического банка. Это синтез пользовательского опыта и новых бизнес-процессов. Банки «Модели C» те, кто понимает, что их существующие системы и бизнес-процессы слишком инертны для кардинальных и быстрых изменений. Банки этой модели создаются с нуля в качестве нового цифрового банка. Банки «Модели C» полагаются на более гибкие и модульные бэкэнд-системы, чтобы предоставить клиентам оптимизированное сквозное взаимодействие. Новые серверные системы также позволяют этим цифровым банкам внедрять инновации на уровне продуктов.
«Модель D»	На 100% цифровой банк. Это полноценные банки, которые строят свои основные ценностные предложения вокруг цифровых технологий[8]

Переход на цифровые технологии значительно упрощают работу сотрудникам банков, предлагая дистанционное обслуживание, что позволяет значительно сэкономить время клиента. Ведь благодаря им пользоваться многими услугами можно без посещения офиса банка. В настоящее время банки предлагают клиентам услугу Мобильный банк, которая позволяет держателем платежных карт посредством мобильной связи совершать ряд операций. С помощью данной услуги можно осуществлять денежные переводы, погашать кредиты[9], выполнять платежи со счета банковской карты на счета организаций, состоящие в партнерских отношениях с банком, блокировать банковские карты в случае утраты и многое

[8] Самочетова Н.В. Цифровой банкинг как новое направление развития банковского дела [Электронный ресурс] // Междунар. науч.-практ. журнал «Экономика и социум». – №3(34). – Электрон. дан. – 2017. – URL: https://www.iupr.ru/ (дата обращения: 27.04.2020).

[9] Космачева Н.М., Стецюнич Ю.Н. Оценка качества управления кредитными рисками в банках по критерию просроченной задолженности // Экономика нового мира. – 2018. – № 4 (12). – С. 47–58.

другое. Основными сегментами области финансовых технологий на данный момент являются: платежи и переводы, краудфандинг, управление активами, финансовый маркетплейс, блокчейн.[10]

Самым важным предвещающим вход РФ в эпоху цифровой экономики, стал тот факт, что именно в России в 2006 г. открылся один из первых цифровых банков – Тинькофф Банк. На официальном сайте данного банка говорится: «Тинькофф Банк – первый и единственный в России полностью онлайн – банк, обслуживающий около 8,5 миллиона клиентов.

У банка нет отделений: все клиенты обслуживаются дистанционно через онлайн – каналы и контакт-центр. В облачном кол-центре банка работает более 10 000 сотрудников, что делает его одним из самых крупных в Европе. Собственная сеть представителей из 2 500 человек по всей России позволяет доставлять продукты уже на следующий день после заявки. Тинькофф Банк был признан лучшим розничным онлайн – банком мира в 2018 году и лучшим розничным онлайн – банком России в 2018 и 2016 годах по версии Global Finance».[11]

Таким образом, можно сделать вывод о том, что в настоящее время происходят существенные изменения в сфере финтеха – выход за рамки стандартных платежей и кредитов.[12] Развитие новых технологий дает больше возможностей для кардинальных изменений инфраструктуры и функционирования всего финансового сектора экономики. На сегодняшний день так же происходит широкое внедрение искусственного интеллекта.

Среди них чат-боты для обслуживания клиентов, роботизированные игроки на биржах, машинное обучение и анализ больших данных для принятия решения по кредиту для клиента.[13] Лидером применения искусственного интеллекта в банковском секторе является «Сбербанк».

Все это дает нам надежду не только на рост качества оказываемых нам банковских услуг, но и на то, что российские банки смогут возглавить высокотехнологичное направление развития мирового банкинга.

---

[10] Стецюнич Ю.Н. Трансформация рынка ипотеки в условиях цифровой экономики // Профессиональное образование, наука и инновации в XXI веке: сб. трудов XII С.-Петерб. конгресса (Санкт-Петербург, 12–30 ноября 2018 г.). – Петербургский государственный университет путей сообщения Императора Александра I. – С. 228–229.

[11] Российский коммерческий банк «Тинькофф Банк» // Официальный сайт Тинькофф Банк. – URL: https://www.tinkoff.ru\ (дата обращения: 28.04.2020)

[12] Стецюнич Ю.Н. Трансформация рынка ипотеки в условиях цифровой экономики // Профессиональное образование, наука и инновации в XXI веке: сб. трудовXII С.-Петерб. конгресса (Санкт-Петербург, 12–30 ноября 2018 г.). – Петербургский государственный университет путей сообщения Императора Александра I. – С. 228–229.

[13] Космачева Н.М., Стецюнич Ю.Н. Оценка качества управления кредитными рисками в банках по критерию просроченной задолженности // Экономика нового мира. – 2018. – № 4 (12). – С. 47–58.

1.3 Цифровая экономика в платформах сети интернет

Цифровая экономика включает в себя количественное программное обеспечение, электронное производство, электронное управление и называется по-разному: интернет-экономика, новая экономика, экономика знаний, интеллектуальная экономика, смарт экономика, 3D-Printing economy и веб-экономика сотрудничества (APEC) отмечают, что цифровая экономика резко изменит базовые понятия производительности труда, стоимости и разделения продукции, а также действует как главный двигатель экономического роста и создания новых рабочих мест.

Исключительность цифровой экономики будет основана на высокотехнологичной индустрии, международном транспорте, международном расчете, высокой степени мобильности банков и финансов. Благодаря средним и высокоскоростным сетевым услугам в университетах высокого уровня была создана система электронного. Наряду с малыми и средними производителями, они стали развиваться с помощью электронной коммерции b-to-b (business-to-business). Эта революция в технологии информационных технологий резко расширила рынок труда, создав больше предприятий и услуг. Электронная коммерция, или электронный бизнес, включена в международную и ежедневную торговлю.[14]

Индекс развития информационно-коммуникационных технологий (ICT Development Index)– это комбинированный показатель, характеризующий достижения стран мира с точки зрения развития информационно-коммуникационных технологий (далее – ИКТ).

Рассчитывается по методике Международного союза электросвязи (International Telecommunication Union), специализированного подразделения ООН, определяющего мировые стандарты в области ИКТ. По Индексу развития информационно-коммуникационных технологий Исландия занимает первое место в мире, далее идут Южная Корея и Швейцария. Эти исследования были проведены в 176 странах мира. Современная цифровая экономика – это результат развития информационных технологий за последние 30 лет. Цифровое экономическое развитие можно разделить на три этапа.

Первый этап: становление цифровой экономики с середины 1980-х гг. XX в. обеспечили основу, благодаря которой была создана глобальная сеть Интернет.

Второй этап: 1994 г. – начало 2000-х гг. Производство цифровой экономики встало на одно из первых мест для большинства стран.

[14] Зенкина 2019 – Зенкина Е.В. Международная валютно-финансовая система: Учеб. М.: Инфра-М, 2019. – С. 152-153.

Были запущены интернет-магазины, система интернет-банкинга. Третий этап: начало нового тысячелетия, широкий спектр электронных продуктов и валют. К ним относятся электронные услуги и (онлайн) интенсивное развитие электронной торговли.

Томас Мезенбург, экономист из США, выделяет три компонента цифровой экономики:

–инфраструктура Supporting: (оборудование, программное обеспечение, Телекоммуникации, сети, ЕТК);

– электронный бизнес;

– Е-торговля.

Канадский инженер-экономист Дон Тапскотт определяет 12 характеристик цифровой экономики: Знания и информация; Цифровизация; Виртуализация; Разделы; Интеграция; Медиация; Инновация; Портал; Гипотезы; Скорость; Глобализация; Конфликт.

Теоретическая основа экономической безопасности государства исследовалась в трудах многих отечественных и зарубежных ученых-экономистов. Так, С. Афанасьев[15]рассматривает экономическую безопасность как совокупность внешних и внутренних факторов, которые благоприятно влияют на развитие национальной экономики, ее способности удовлетворять потребности государства и всех экономических субъектов, а также способствуют снижению внешних и внутренних угроз на уровне государства.

В.К. Сенчагов[16] определяет экономическую безопасность как достижение национальных интересов, а также экономическое развитие государства при самых неблагоприятных условиях функционирования государства. Е.А. Срибная, О.А. Андронова отмечают, что «покрытие внешнего государственного долга РФ является основной статьей бюджета страны. В РФ по сравнению с другими государства внешний государственный долг достаточно небольшой, что является большим преимуществом для экономического развития страны».[17]

В.И. Срибный утверждает, что «основной проблемой в обеспечении безопасности государства на современном этапе развития экономики является сложность в выявлении

[15] Афанасьев С. Дискуссионные проблемы концепции национальной экономической безопасности / С. Афанасьев // Россия XXI. – 2016. – №2.- С. 1-2.

[16] Экономическая безопасность России: Общий курс: учебник / под ред. В.К. Сенчагова. – М.: Дело, 2015. – С. 426-429.

[17] Срибная Е.А., Андронова О.А. Долговая устойчивость как основа обеспечения экономической безопасности Российской Федерации / Е.А. Срибная, О.А. Андронова // Институт финансово-кредитных отношений в условиях рыночных трансформаций: сборник статей научно-практического семинара (г. Симферополь, 30 ноября 2016 года). – Выпуск 4. –Симферополь: ООО «Антиква», 2017. – С. 405-409.

внешних и внутренних угроз на ранней стадии или их предупреждение, а также четкая классификация данных угроз экономической безопасности».[18]

Характерными чертами цифровой экономики в современных условиях развития государства являются:

1. Интеллектуальный капитал в условиях цифровой экономики начинает преобладать над финансовым капиталом и насилием. Он становится одним из основных инструментов власти как на государственном, так и на уровне предприятий.

2. Повышенный интерес инвесторов как зарубежных, так и отечественных в новых технологиях, новых разработках, ноу-хау по сравнению с реальным инвестированием, что объясняется в сотни раз превышающей долей прибыли от успешно реализованных новых технологий.

3. Оценка стоимости компаний на сегодняшний день может предусматривать не только реальный капитал компании, но и на прогнозах по разработке и реализации новых технологий.

4. Преобладание во всех сферах экономики государства обмена информацией над реальным обменом, что заставляет повышать уровень информационной безопасности как на уровне компаний, так и на уровне государства. Обеспечение информационной безопасности становится одним из основных составляющих экономической безопасности государства.

5. Все большее развитие таких понятий как интеллектуальная собственность, патенты и т.д., что требует о государства пересмотра законодательства, а также разработку новых инструментов и методов, которые бы позволяли защищать интеллектуальную собственность.

6. Интернет становится основным средством коммуникаций и информационного обмена. Телефоны и планшеты становятся неотъемлемой частью работы всех без исключения работников практически всех сфер экономики государства. Обмен информации через интернет, также как и деловая переписка являются на сегодняшний день более быстрым и эффективным способом делового общения.

7. Малые организации являются более адаптивными к изменяющимся условиям рынка, более эффективными, более чувствительными к факторам внешней и внутренней среды. Многие крупные компании стараются сокращать уровни иерархии, делая свою организационную структуру более гибкой и эффективной.

---

[18] Срибный В.И. Составляющие механизма обеспечения экономической безопасности Российской Федерации / В.И. Срибный // Институт финансово-кредитных отношений в условиях рыночных трансформаций: сборник статей научно-практического семинара (г. Симферополь, 30 ноября 2016 года). – Выпуск 4. – Симферополь: ООО «Антиква», 2017. – С. 409-412.

8. Малый и средний бизнес является в современных условиях развития экономики более гибким и эффективным, поэтому на уровне государства происходит сокращение крупных компаний и преобразование их более мелкие и средние.

9. Информационный обмен переходит из регионального и государственного уровня в глобальный или мировой. Поэтому компании, которые имеют доступ к информации на мировом уровне являются более совершенными и эффективными.

Только учитывая перечисленные черты цифровой экономики в современных условиях развития государства, можно добиться обеспечения экономической безопасности Российской Федерации.

Стоит отметить, что внешние и внутренние угрозы экономической безопасности Российской Федерации растут с каждым днем. И на сегодняшний день они дополняются еще и военно-политическими угрозами, что требует от Российской Федерации дополнительных мер по обеспечению безопасности государства.

С целью обеспечения экономической безопасности Российской Федерации необходимы грамотные, своевременные и эффективные меры и действия органов государственного управления на всех уровнях государственной власти, а также разработка мероприятий по профилактике и снижению воздействия внешних и внутренних угроз экономической безопасности государства в будущем.

1.4 Проблемы цифровой экономики с позиции национальной безопасности

Формирование сегментов цифровой экономики практически во всех отраслях экономики и сферах жизнедеятельности актуализирует проблему обеспечения экономической безопасности. Наряду с возможностями значительного сокращения затрат и увеличения прибыли в условиях цифровой экономики появляются дополнительные риски, возникающие в ходе обработки, хранения и передачи данных. Таким образом, в условиях цифровизации экономики повышаются информационные риски, которые при определенных условиях могут перерастать в угрозы.

В Стратегии экономической безопасности Российской Федерации до 2030 года в качестве угрозы выделяется отставание в области разработки и внедрения новых и перспективных технологий цифровой экономики. Отставание от ведущих иностранных государств в развитии конкурентоспособных информационных технологий определено в качестве угрозы цифровой экономики также в программе "Цифровая экономика Российской

Федерации". Таким образом, в программных документах акцентируется внимание на технологических угрозах.

Состояние технологической базы цифровой экономики во многом определяется уровнем развития электронной промышленности.

Для реализации возможностей цифровой экономики необходимо приоритетное внимание уделить ее технологическому аспекту: повышение конкурентоспособности российских компаний, осуществляющих деятельность в области цифровых технологий; снижение уровня зависимости отечественной промышленности от зарубежных технологий и комплектующих; преодоление технологической отсталости российских компаний и повышение уровня их цифровизации.

За последние несколько лет идеи цифровой экономики начали выходить за рамки коммерческой стороны сделок (покупок и продаж) в отношении электронных товаров в Интернете. В настоящий момент эта концепция также пользуется виртуальными процессами в деятельности различных крупных компаний. Помимо использования этой идеи в деятельности фирм, она также внедряется во внутреннюю работу правительства для реализации транзакций. Современное состояние цифровой экономики в России можно охарактеризовать как стремительное развитие. Подтверждением данного факта, прежде всего, является то, что по поручению Президента РФ Федеральное Собрание должно было разработать программу развития цифровой экономики. Данное поручение Путин В.В. высказал в декабре 2016 года. И основным принципом данного документа должно было стать то, что между российской виртуальной экономикой и этой же сферой Евразийского экономического союза должна происходить полная интеграция.

Целями государственной программы являются прекрасные перспективы внедрения цифровых технологий во все сферы жизни. Управление ресурсами (водными, энергетическими, топливными) планируется проводить с помощью интегрированных цифровых платформ. Они позволят объединить в информационной среде всех участников рынка, снижая транзакционные издержки и изменяя систему разделения труда. Планируется создание 50 «умных городов», в которых будет проживать 50 000 000 человек. «Умные города» благодаря комплексу технических и организационных мероприятий создают комфортные условия для проживания и бизнес-деятельности.

Государство обязуется создать особые технологические медицинские центры, оснащенные по последнему слову техники, в которых будет оказываться квалифицированная помощь.

Переход на документацию электронного вида, которая вошла в обыденную жизнь населения, планируется развивать и дальше. Доля межведомственного документооборота должна составить до 90% от общей массы. Количество услуг, которое должно предоставлять государство в онлайн-режиме должно составлять около 80% к 2025 году, и подавляющее большинство населения России должно дать положительную оценку их качеству. «Поэтому неудивительно, что российский президент сегодня рассуждает о том, что драйвером роста необходимо сделать так называемую цифровую экономику. И действительно, она может дать наиболее широкие перспективы к росту, чем наши традиционные сектора.

Активное развитие цифровой экономики во всех сферах деятельности человека обуславливает актуальность обеспечения информационной безопасности данного процесса. Правительство РФ проводит политику по укреплению информационной безопасности.

Именно по этой причине, 18 декабря 2017 года был утвержден план действий по направлению «Информационная безопасность» программы «Цифровая экономика Российской Федерации» на 2018-2024 годы. Данный план был утвержден Правительственной комиссией по использованию информационных технологий для того, чтобы улучшить качество жизни населения и условия ведения предпринимательской деятельности. По итогам данной программы должны быть достигнуты целевые значения информационной безопасности на сетях связи и в российском сегменте интернета. Также должна быть создана система стимулов для приобретения и использования серверного, компьютерного и телекоммуникационного оборудования российского производства.

Планируется обеспечить контроль обработки информации и доступа к персональным данным. В соответствии с этим планом страна к 2024 году должна достигнуть следующие цели в отношении информационной безопасности: срок простоя государственных информационных систем должен быть снижен; доля граждан, которая повысила грамотность в сфере информационной безопасности должна увеличиться; доля внутреннего сетевого трафика сети «Интернет», проходящая через иностранные серверы, должна составлять не более 5%; доля субъектов, использующих стандарты безопасного информационного взаимодействия государственных и общественных институтов, должна составлять не менее 75%.

Цифровая экономика на данном этапе развития оказывает положительное влияние на состояние экономики России в целом.

Вывод: Таким образом, важнейшим инструментом обеспечения национальной безопасности России является формирование эффективной цифровой экономической среды, основанной на современных знаниях и технологиях. Исходя из вышесказанного, для

развития цифровой экономики страны необходимо создание условий и инфраструктуры логистики, поддержка НИОКР и формирование соответствующей нормативно-правовой базы.

2 Современные подходы к регулированию деятельности платформ интернета государством

2.1 Опыт США

Интернет радикально и в трансграничном масштабе изменил взаимодействие государств и лиц, расширив их коммуникативные возможности и сферы их «цифрового присутствия». Вряд ли будет подвергнут сомнению тот факт, что за последнюю четверть века интенсивное расширение социальных сфер применения Интернета диверсифицировало правовую регламентацию целого ряда отношений.

Киберпространство, данные (в их «широком» значении, охватывающем данные личного характера/ персональные данные), информация и т.д. стали самостоятельными объектами правового регулирования.[19] Более того, в нынешних условиях выбор стратегического вектора социально-экономического развития современных государств ориентирован на «цифровую экономику», реализация которой без применения Интернета недостижима.[20]

Безусловно, становится очевидным, что те трансграничные коммуникативные возможности, которые возникли в связи с применением Интернета, стали определяющими в обусловленности сопряжения, в частности, национально-правовых и международно-правовых интересов государств при формировании их подходов правового регулирования использования Интернета в целом.

В сентябре 2018 г. Соединенные Штаты Америки приняли важный документ – Национальную киберстратегию США (National Cyber Strategy of the United States of America).[21] Содержательный анализ этого документа со всей очевидностью свидетельствует о том, киберпространство рассматривается как критически важный объект национальных интересов США, а его безопасное использование объективно предопределяет необходимость международно-правого сотрудничества. Предваряя обращение к содержанию названного документа (далее – «Киберстратегия США»), целесообразно отметить два, как представляется, принципиальных момента.

Первый момент. При «оценке» Киберстратегии США логично учесть, что первоначально, еще в 2011 г. (т.е. при предыдущей Администрации США), была принята «Международная стратегия США в отношении киберпространства. Процветание,

[19] Архипов В.В. Проблема квалификации персональных данных как нематериальных благ в условиях цифровой экономики, или Нет ничего более практичного, чем хорошая теория // Закон. 2018. № 2.- С. 52-68.

[20] Стратегия Единого цифрового рынка Евросоюза (EU Digital Single Market strategy). 6 May 2015. – URL:https://eur-lex.europa.eu/(Дата обращения: 09.09.2018);

[21] National Cyber Strategy of the United States of America (September 2018). – URL: https://www.whitehouse. gov/wp-content/uploads/2018/09/National-CyberStrategy.pdf (Дата обращения: 09.05.2020)

безопасность и открытость сетевого мира» (International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World).[22] Принятие названного документа (далее – «Международная Стратегия киберпространства США») во многом было обусловлено пониманием правительством США того, что технологические, правовые, политические и прочие вызовы так или иначе будут сопровождать функционирование, а также перспективы развития сетевых технологий и Интернета как их центрального звена. Именно с этой точки зрения в Международной Стратегии киберпространства США были сформулированы семь стратегических направлений регулирования киберпространства, требующих совместных усилий государств, при сотрудничестве с технологическим, гражданским, научным сообществом, в содействии построения и поддержания открытых, функционально совместимых (интероперабельных), безопасных и надежных сетей внутри США и за их пределами.

В качестве стратегических взаимосвязанных направлений в Международной Стратегии киберпространства США были определены: «Экономика: укрепление международных стандартов и инноваций, открытые рынки»; «Защита наших сетей: усиление безопасности, надежности и отказоустойчивости»; «Правопорядок: расширение сотрудничества и правовое регулирование»; «Военная сила: подготовка к вызовам безопасности XXI века»; «Управление использованием Интернета: содействие эффективным и всеобъемлющим структурам»; «Международное сотрудничество: потенциал, безопасность и процветание»; «Свобода Интернета: защита основных свобод и частной жизни».

Обозначенные семь направлений Международной Стратегии киберпространства США, помимо их взаимосвязанности, с одной стороны, представляли не конкретные инструкции, но скорее широкие принципы, обрисовывающие приоритеты Правительства США в сфере киберпространства; с другой стороны, определяли сферы, в каждой из которых правительство США предполагало необходимость сотрудничества на международном, региональном и двустороннем уровнях. В общем плане взаимосвязанные стратегические направления были призваны продемонстрировать «национальный и международный» вектор действий правительства США в сфере киберпространства.

Второй момент. Внимательный анализ Международной Стратегии киберпространства США дает основание говорить об изменении позиции США к международному праву в «пользу уважительного отношения» к нему и необходимости использования его правового инструментария. На этот факт, в силу его принципиального

[22] International Strategy for Cyberspace. Prosperity,Security and Openness in a Networked World. –URL: ttp://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (Дата обращения: 09.05.2020)

характера, следует обратить внимание, поскольку ретроспективный взгляд на подходы США, сложившиеся к моменту принятия Международной Стратегии США в международно-правовом плане, позволял говорить о том, что именно международное право было той сферой, к которой в США относились нередко «скептически».

Американские юристы консервативного толка зачастую игнорировали «авторитет международного права», несмотря на Статью VI Конституции Соединенных Штатов, которая наделяет акты международного права той же силой и теми же приоритетами, что и федеральные законы; «американский подход» к роли международного права достаточно долгое время отражал «крайне-правые» доктринальные взгляды. По мнению ряда американских юристов-международников, негативное отношение к международному праву и международным институтам коренится в традиционных для США ценностях. Например, Майкл Гленнон (Michael J Glennon) отмечал, что поскольку международное право не смогло выполнить своей основной задачи, а именно предотвратить использование силы в отношениях между странами, дальнейшее соблюдение США ограничений, накладываемых международным правом, было бы пагубным для США.

Рядом юристов-консерваторов в области международного права. К примеру, Джек Голдсмит (Jack L. Goldsmith) и Эрик Познер (EricA. Posner) утверждали, что национальные государства не «интернационализировали» международное право и не придерживаются его, а «действуют, исходя из собственных интересов»; соответственно, международное право – это набор правил, которые можно использовать, когда удобно, и проигнорировать или даже преобразовать их, когда они мешают.[23]

Джек Голдсмит (Jack Goldsmith) и Тим Ву (Tim Wu) в своей работе «Кто контролирует Интернет?: иллюзии безграничного Мира» отмечали, что недостаточность международных соглашений в сфере управления Интернетом отражает слабость международного права и его неспособность предложить эффективные решения по этому вопросу.

В контексте сказанного сам факт принятия Международной Стратегии киберпространства США, а также закрепления в этом документе правительством США необходимости международного сотрудничества в киберпространстве и его развития – стал важным фактором понимания США того, что Интернет не является «территорией вне права», в т.ч. международного права.

[23] Jack L. Goldsmith & Eric A. Posner, The Limits of International Law 225-26 (2005). Анализ работы Jack L.Goldsmith & Eric A. Posner, The Limits of InternationalLaw (2005) см Paul Schiff Berman «Seeing Beyond the Limits of International Law» – URL: http://www.papers.ssrn.com/sol3 (Дата обращения: 09.09.2018);

Безусловно, с «позиций» 2019 г. Международную Стратегию киберпространства США важно воспринимать с учетом временных параметров ее принятия, включая внутринациональную политико-экономическую ситуацию в США, а также международно-правовой, геополитический и т.д. контексты, существовавшие в 2011 г., которые по сути и определили ее содержательный формат.

Вместе с тем, оценивая Киберстратегию США, целесообразно отметить, что в новых, значительно изменившихся за последние восемь лет социально-политических, экономических, международно-правовых и т.д. условиях.

Отметим, что Киберстратегия США 2018 г. основывается, во-первых, на Стратегии Национальной Безопасности США (National Security Strategy of the United States of America), которая была принята после 11 месяцев начала работы нынешней администрации президента США, т.е. в декабре 2017 г.13; во-вторых, на административном распоряжении президента США (Executive Order, EO) 13800 «Об усилении кибербезопасности федеральных сетей и критической инфраструктуры» (Executive Order, «Strengthening of Federal Networks and Critical Infrastructure»). Киберпространство, так же как и в рассмотренной ранее Международной Стратегии киберпространства США, продолжает позиционироваться США как критически важный объект, требующий сохранения его природы, совместных международных усилий по снижению возникающих угроз и вызовов, связанных с опасностью его фрагментации, подрыва открытого, функционально совместимого (интероперабельного), безопасного, транспарентного применения Интернета как основы киберпространства.

Несмотря на то что Киберстратегия США формально не ссылается на рассмотренную ранее Международную Стратегию киберпространства США, однако и в предметном, и содержательном плане ключевые подходы, в т.ч. понятийно-терминологический ряд (кибербезопасность, процветание, интероперабельность, транспарентность и т.д.) остаются неизменными, равно как неизменной остается и приверженность к стратегическим целям и задачам, которые сопрягаются с необходимостью (неизбежностью) обеспечения совместных усилий государств, технического, гражданского, академического сообщества и т.д. для поддержания функционирования и использования киберпространства

Киберстратегию США предваряет обращение президента США, в котором обозначены следующие ключевые направления укрепления потенциала кибербезопасности и обеспечения защиты США от киберугроз и вызовов: защита США посредством сохранения сетей, систем, функциональных элементов и данных; содействие американскому

благоденствию посредством содействия безопасной, процветающей цифровой экономике и стимулирования сильных внутристрановых инноваций; сохранение мира и безопасности посредством укрепления способности США сдерживать и, в случае необходимости, принимать меры воздействия на тех, кто использует киберинструменты в злонамеренных целях, при этом такие замыслы осуществляются во взаимодействии с союзниками и партнерами; усиление американского влияния за рубежом, с тем чтобы расширить основополагающие принципы открытого, функционально совместимого, интероперабельного, надежного и безопасного Интернета.

Киберстратегия США не только опирается на Стратегию Национальной Безопасности США 2017 г., но и структурно коррелирует с ней, о чем свидетельствует даже рубрикация обоих документов и названия разделов. Киберстратегия США, так же как и Стратегия Национальной Безопасности США 2017 г., структурно содержит 4 исходные опоры (Pillars) или основополагающих элемента, формулировки которых идентичны. При этом, в отличие от соответствующих основополагающих направлений Международной Стратегии киберпространства США и Национальной Безопасности США 2017 г., в каждой из четырех опор Киберстратегии США сформулирована конкретная цель, а также соответствующие приоритетные действия.

Во введении Киберстратегии США дважды упоминается Россия, однако данное упоминание осуществлено в контексте таких стран, как Китай, Иран и Северная Корея. При этом во Введении также дважды упомянут Китай, при этом один раз в контексте обозначенных стран (Россия, Иран и Северная Корея) и один раз отдельно от этих стран, в качестве страны, которая занималась «киберподдержкой экономического шпионажа и кражей триллион-долларовой интеллектуальной собственности».

Целесообразно в общем плане обозначить четыре опоры Киберстратегии США, цели, а также содержательные разделы, определяющие приоритетные направления и действия.

Опора I: Защитить американский народ, Отечество и американский образ жизни формулирует ключевую цель – управлять рисками кибербезопасности для повышения защиты и устойчивости информации граждан США и информационных систем. Этот основополагающий элемент охватывает три раздела.

Раздел первый – обеспечение безопасности федеральных сетей и информации, предполагающий приоритетные действия: дальнейшую централизацию управления и надзора за федеральной гражданской безопасностью; согласование управления рисками и деятельностью в сфере информационных технологий; совершенствование управления

рисками федеральной системы снабженческих цепочек; усиление кибербезопасности федеральных подрядчиков; обеспечение лидирующих позиций правительства США по лучшим и инновационным практикам.

Раздел второй – защита критической инфраструктуры охватывает следующие приоритетные действия: совершенствование распределения функций и сфер ответственности; определение приоритетов действий в зависимости от характера идентифицированных национальных рисков; привлечение провайдеров информационно-коммуникационных технологий как посредников кибербезопасности; защиту американской демократии; создание благоприятных условий для инвестиций в кибербезопасность; определение приоритетов национальных исследований и содействие развитию инвестиций; улучшение транспортной, морской и космической кибербезопасности.

Раздел третий – борьба с киберпреступностью и улучшение отчётности об инцидентах предусматривает такие приоритетные действия: меры по улучшению отчетности и реагирования на инциденты; улучшение электронного надзора, а также совершенствование права о компьютерных преступлениях; снижение угроз от транснациональных преступных организаций в киберпространстве; улучшение задержания преступников, находящихся за рубежом; укрепление потенциала правоохранительных органов стран-партнеров в борьбе с преступной кибердеятельностью.

Опора II: Содействие американскому процветанию в качестве ключевой цели определяет сохранение влияния США в технологической экосистеме, а также развитие киберпространства в качестве открытого двигателя экономического роста, инноваций и эффективности. В этот основополагающий элемент включены три раздела.

Раздел первый – содействие развитию жизнеспособной и устойчивой цифровой экономики направлено на такие приоритетные действия, как: стимулирование гибкой и защищенной технологической торговли; определение приоритета инноваций; инвестирования в инфраструктуру следующего поколения; содействие свободному трансграничному потоку данных; поддержание лидерства США в передовых технологиях; содействие полному жизненному циклу кибербезопасности.

Раздел второй – поощрение и обеспечение изобретательности США предполагает, что приоритетные действия – это обновление механизмов обзора иностранных инвестиций и деятельности в США; поддержание сильной и сбалансированной системы защиты интеллектуальной собственности; защита конфиденциальности и целостности американских идей.

Раздел третий – создание высококлассного штата сотрудников кибербезопасности подразумевает следующие приоритетные действия: создание и поддержание кадрового резерва; расширение возможности переподготовки и образования для американских служащих и рабочих; увеличение кадрового персонала кибербезопасности федерального уровня; использование исполнительных органов для выявления и поощрения талантливых кадров.

Опора III: Сохранение мира посредством силы в качестве ключевой цели формулирует выявление, противодействие, пресечение, ослабление интенсивности, а также сдерживание действий в киберпространстве, которые дестабилизирует и противоречат национальным интересам США, с сохранением превосходства США в киберпространстве и посредством киберпространства. Данный основополагающий элемент охватывает два раздела.

Раздел первый – повышение киберстабильности посредством норм ответственного поведения государств в качестве приоритетных действий предполагает поощрение всеобщей приверженности нормам, действующим в киберпространстве.

Раздел второй – сдерживание неприемлемого поведения в киберпространстве направлено на необходимость таких приоритетных действий, как руководство заявленными целями, а также взаимодействие с разведывательными органами; введение соответствующих мер воздействия за негативные последствия в киберпространстве; создание киберсдерживающих инициатив; противодействие вредоносному кибервлиянию и информационным операциям.

Во-первых, в настоящее время, когда выбор стратегического вектора социально-экономического развития современных государств ориентирован на «цифровую экономику» и Россия не является в этом плане исключением, усиливается конфликт между национально-правовыми подходами регулирования применения Интернета и достаточно сильно различающимися, а нередко и противоположными, интересами государств с учетом трансграничных коммуникативных возможностей Интернета.

Несомненно, средства, методы национально-правовые подходы разрешения этого конфликта, а также меры правовой защиты и т.д. будут претерпевать радикальные изменения и варьироваться в зависимости от специфики национальных правопорядков государств.

Во-вторых, в настоящее время положительный ответ на вопрос о применимости международного права к киберпространству, регулированию применения Интернета и т.д. не вызывает сомнений, однако остаются открытыми вопросы относительно того, каковы формы и методы такого применения, как они соотносятся с национальными интересами государств.

Кроме того, существующая реальность не подтвердила доктринальных предположений о том, что регулирование отношений в сфере Интернета настолько многообразно и «породит такие синергетические» связи, которые могут трансформировать роль суверенных государств как субъектов международного права.

В-третьих, целый ряд государств, включая Российскую Федерацию, достаточно скептически относится к необходимости международного сотрудничества в киберпространстве по «широкому кругу вопросов», и вектор правового регулирования переносится исключительно в сферу национального права. Применительно к Российской Федерации следует сказать, что определенные «надежды» связываются с тем фактом, что она принимала активное участие в обсуждении новой редакции Конвенции № 108 Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data).[24]

2.2 Опыт Европы

В Великобритании в 2007 г. была введена в действие третья часть так называемого «Закона о регулировании следственных действий»[25] (Regulation of Investigatory Powers Act 2000) (далее – RIPA), которая направлена на регулирование в том числе круга вопросов, связанных с передачей следственным органам криптографических ключей и, шире, с информационной безопасностью. RIPA отменяет ранее действовавший Акт контроля и перехвата сообщений (The Interception of Communications Act) (далее – IOCA) и регулирует деятельность различных юридических агентств (что отсутствовало в IOCA) в части получения доступа к средствам связи и использования персональных данных.[26]

Согласно этому акту оговоренные лица обязаны передавать информацию в расшифрованном виде и/или криптографические ключи, способные расшифровать информацию, представителям власти без постановления суда. Также этот закон предусматривает полномочие органов государственной власти требовать от компаний связи установить оборудование для контроля и блокировки сообщений. Впервые этот акт был применен уже в ноябре 2007 г. По отношению к группе зоозащитников.[27] Важно отметить,

---

[24] Конвенции № 108 Совета Европы о защите физических лиц при автоматизированной обработке персональных данных. [Электронный ресурс] – URL: https://search.coe.int/directorate_of_communications/Pages/result_ details.aspx?ObjectId=09000016808ac976 (Дата обращения: 09.05.2020).

[25] Regulation of Investigatory Powers Act 2000 [Электронный ресурс]: The official home of UK legislation. URL: http://www.legislation.gov.uk/ukpga/2000/23/pdfs/ukpga_20000023_en.pdf (дата обращения: 01.05.2020).

[26] Лебедева Н. Н. Право. Личность. Интернет: учебное пособие. – М., 2014. – С. 232.

[27] Campaigners hit by decryption law [Электронный ресурс]: BBC News. URL:

что отказ в передаче необходимой информации влечет за собой ответственность, максимальный предел которой – 2 года лишения свободы (или 5 лет в случае, если речь идет о материалах, содержащих детскую порнографию).

Так, в 2010 г. на основании RIPA был осужден на 16 недель лишения свободы 19-летний житель Ланкашира за отказ передать полиции «ключ» от документа на компьютере. Ранее, в 2008 г., аналогичным образом был осужден на 13 месяцев лишения свободы житель Лондона.

Нельзя не отметить, что в сравнении с IOCA RIPA имеет несколько более узкую направленность регулирования, а также намного большую детализацию. Впрочем, с 2017 г. На территории Великобритании будет действовать акт, который существенно расширит полномочия органов исполнительной власти в этой сфере.

Схожие тенденции по усилению контроля в информационной сфере можно видеть и в других странах: Австралия (The Cybercrime Act 2001 No. 161), ЮАР (RICA Act of 2002) и др. Например, ст. 125k (в совокупности со ст. 125i и 125j) Уголовно-процессуального кодекса Нидерландов (Wetboek van Strafvordering) позволяет следователю при условии наличия ордера получить доступ к информации, хранящейся у операторов связи.

Кроме того, 26 сентября 2016 г. в Швейцарии на референдуме было принято решение расширить полномочия специальных правительственных служб (например, Федеральной разведывательной службы), в том числе в сфере контроля интернет-пространства.

Страны континентальной Скандинавии1 (Швеция, Норвегия, Дания, Финляндия) одни из первых в мире вступили на путь внедрения цифровых систем в различные сферы жизни общества.

Их по праву можно отнести к пионерам освоения цифрового общественного пространства. Именно поэтому опыт цифровизации этих стран (от социально-экономических условий, в которых возникли и развиваются цифровые процессы, специфики их протекания до реальных и потенциальных проблем и рисков) становится столь значимым для понимания происходящих «цифровых» процессов не только в их национальных границах, но и в масштабе мира в целом.

Первые государственные программы, касающиеся электронного правительства и цифровой экономики, в скандинавских странах были приняты еще в конце в 1990-х гг. На тот момент перед государством стояли задачи повышения эффективности работы сложной разветвленной системы государственного аппарата: прежде всего, налоговых органов.

---

http://news.bbc.co.uk/2/hi/technology/7102180.stm (дата обращения: 01.05.2020).

Подобный фокус отнюдь не случаен, т. к. традиционно именно налоговые отчисления составляют около половины ВВП стран региона.

Успешному старту внедрения цифровых технологий способствовал целый ряд социально-экономических и политико-административных условий, выделяющих страны Скандинавского региона даже на фоне других высокоразвитых стран Западной Европы.

Так, низкая численность населения скандинавских стран (в самой крупной стране Скандинавии – Швеции – число ее жителей в конце 1990-х гг. составляло лишь около 9 млн чел.; в Норвегии и Финляндии – по 5,5 млн чел. в Дании – 5 млн чел.), как ни парадоксально, стала конкурентным преимуществом в вопросе внедрения цифровых технологий. Немалую роль сыграл высокий уровень урбанизации (свыше 80% населения Скандинавии проживает в городах), т. к. именно города становятся основными полигонами для внедрения инноваций. Кроме количественных характеристик и особенностей территориального размещения, большое значение имели и качественные показатели человеческих ресурсов. Население Скандинавии традиционно имеет один из самых высоких уровней образования в мире. Еще в начале XX в. в Швеции, Дании, Норвегии уровень безграмотности был близок к нулевой отметке.

И в конце XX в. по числу граждан со средним специальным и высшим образованием, эти страны (включая и догнавшую, а в ряде аспектов и перегнавшую их Финляндию) относятся к числу мировых лидеров. Высокий базовый уровень образования позволил населению в короткие сроки получить достаточные «цифровые компетенции» для внедрения и последующего развития цифровых технологий в различных сферах. Кроме того, высокие реальные доходы населения создавали необходимый материально-финансовый фон, при котором подавляющее большинство жителей могли позволить себе покупку дорогостоящих технических устройств, наличие которых является необходимым условием цифровизации. Таким образом, фактор ограниченного числа участников цифрового развития, обладающих необходимыми устойчивыми навыками пользования технологиями и финансовыми ресурсами, в совокупности с высокой степенью их территориальной концентрации обусловил таргетированный эффект цифровизации и, таким образом, способствовал достижению значимых успехов в вопросе внедрения цифровых инноваций.

Не менее благоприятные условия были созданы и в политико-экономической среде. Несмотря на то, что решение о развитии цифровой экономики первоначально принималось на уровне каждой их стран (национальные программы по цифровизации к началу 2000-х были приняты уже во всех странах Скандинавского региона), в течение короткого периода цифровизация приобрела характер региональной стратегии. Общую координацию действий

по развитию цифровой сферы взяло на себя специально созданное подразделение при Совете Северных стран (Nordic Council of Ministers for Digitalisation (MR-DIGITAL)). Это позволило добиться синергетического эффекта в использовании различных технологических решений, учитывать как положительный, так и отрицательный опыт процесса цифровизации стран-членов, динамично внедряя успешные решения и минимизируя возможные негативные последствия.

Развитие информационных и телекоммуникационных технологий (ИКТ) с момента их появления оценивалось как приоритетное направление экономики скандинавских стран. Именно поэтому сфера научно-исследовательских и опытно-конструкторских работ (НИОКР) являлась и продолжает являться важным реципиентом бюджетных средств. В конце 2000-х гг. доля расходов на НИОКР в Финляндии достигала рекордных 3,7% ВВП, в Швеции – 3,6%, в Дании – 3,1%. Несмотря на то, что во второй половине 2010-х гг. произошло некоторое снижение долевых показателей, Швеция, Дания и Финляндия по-прежнему остаются в группе мировых лидеров.

Страны Скандинавского региона обладают разветвленной сетью технопарков от локального до международных масштабов. Помимо государства, значимую роль здесь играет частный бизнес. Практически каждое крупное предприятие ориентировано на создание собственного исследовательского центра или же работу в тесной связи с научными и исследовательскими центрами, лабораториями, институтами. Эта система обеспечивает сокращение временного периода внедрения инноваций, т. е. пути от изобретения до его коммерциализации. В регионе действуют крупные компании-локомотивы, на которые приходится львиная доля достижений в области ИКТ: в частности, Nokia (Финляндия) и Ericsson (Швеция) специализируются на разработке и производстве телекоммуникационного оборудования для мобильных, фиксированных, широкополосных и IP-сетей; Hexagon (Швеция) – один из мировых лидеров по разработке и производству комплексных решений для развития «умных» систем различных уровней: от отдельных устройств (например, измерительных приборов) до секторов экономики (smart energy, smart transport) и «умных городов» (smart cities); Telenor Group (Норвегия) – одна из крупнейших мировых телекоммуникационных компаний, Telia Company (Швеция) – региональный лидер рынка сотовой связи и др. Наличие современных модернизованных оптико-волоконных линий позволяет обеспечить доступ к высокоскоростному Интернету на территории практически всего региона. Широкое покрытие сетью мобильной связи делает доступным мобильную связь с повышенными требованиями не только четвертого (4G), но и пятого поколения (5G). По данным аналитического агентства GSMA Intelligence страны Северной Европы являются

мировыми лидерами по числу мобильных соединений, относящихся к категории широкополосных (Mobile Economy Europe…). Таким образом, совокупность благоприятных социальных, экономических и политико-административных условий определила положение Швеции, Норвегии, Дании и Финляндии в авангарде мировой цифровизации.

По данным исследования Digital Economy and Society Index (DESI) (Приложение А1), оценивающего уровень цифровизации стран-членов Евросоюза и ряда других стран Западной Европы, в 2019 г. Дания, Норвегия, Финляндия и Швеция занимали верхние строчки рейтинга, демонстрируя наивысшие показатели развития цифровой экономики. Индекс DESI – это комплексный агрегированный показатель, учитывающий такие объективные параметры как распространение широкополосной связи, «цифровые компетенции» населения, активность Интернет-пользователей, степень интеграции цифровых технологий в бизнесе и цифровые государственные услуги.

Все описанные выше случаи свидетельствуют об определенной тенденции роста полномочий государств в рамках интернет-пространства, профилактики киберпреступлений и терроризма. Не отстает от подобной тенденции и Российская Федерация. В июле 2016 г. вступили в силу два федеральных закона, получивших в общественных дискуссиях и средствах массовой информации неофициальное название «Пакет Яровой» – в соответствии с фамилией одного из депутатов, внесших на рассмотрение в Государственную Думу Российской Федерации соответствующие законопроекты.

Указанными законами предусматривается комплексное реформирование в сфере противодействия терроризму. В частности: один из федеральных законов среди прочих мер, таких как установление полномочий органов местного самоуправления в области противодействия терроризму, особенностей производства отдельных видов оружия, определение статуса миссионерской деятельности и других, предусматривает ряд новелл и в усилении контроля информационной среды, а именно: законодательно оформляет новое оперативно-розыскное мероприятие – получение компьютерной информации.

Также для операторов связи и организаторов распространения информации в сети Интернет введены новые обязанности. Во-первых, хранить на территории Российской Федерации информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, текстовых сообщений, изображений, звуков, видео- или иных сообщений пользователей услугами связи или сети Интернет – в течение 3-х лет с момента окончания осуществления таких действий (1 года, если такие действия были совершены в сети Интернет); текстовые сообщения пользователей услугами связи, голосовую информацию, изображения, звуки, видео-, иные сообщения пользователей услугами связи – до 6 месяцев с

момента окончания их приема, передачи, доставки и (или) обработки. Во-вторых, предоставлять указанную информацию компетентным органам, в том числе (в необходимых случаях) – программное обеспечение для ее дешифровки.

Другой федеральный закон из названного «пакета» опять - таки, помимо ряда общих изменений уголовного законодательства, связанных с понижением возраста уголовной ответственности за некоторые преступления, введением нескольких новых составов уголовных преступлений террористической и экстремистской направленности, предусматривает и изменение уголовно-процессуального кодекса, в соответствии с которым, при наличии достаточных оснований полагать, что сведения, имеющие значение для уголовного дела, могут содержаться в электронных сообщениях или иных передаваемых по сетям электросвязи сообщениях, следователем по решению суда могут быть проведены их осмотр и выемка.

Необходимо отметить, что требования о хранении организаторами распространения информации в сети Интернет и операторами связи на территории Российской Федерации текстовых сообщений пользователей услугами связи, голосовой информации, изображений, звуко-, видео-, иных сообщений пользователей услугами связи вступают в силу с 1 января 2018 г., таким образом, заинтересованным лицам предоставлено время для организации надлежащего технического обеспечения новых обязанностей.

В качестве наиболее частых критических суждений относительно принятых федеральных законов можно отметить такие, как большие финансовые затраты на реализацию указанных положений отдельными хозяйствующими субъектами (организаторами распространения информации в сети интернет и операторами связи), ограничение конституционных прав на тайну переписки, частную жизнь и некоторых других. Вопросы экономического обеспечения выполнения новых вмененных обязанностей требуют отдельного исследования. На анализе некоторых юридических аспектов хотелось бы остановиться подробнее.

Указанные нововведения предусматривают, как и любые меры по борьбе с терроризмом, определенные новые ограничения некоторых конституционных прав и свобод человека и гражданина, что явилось причиной негативной реакции части общественности на принятие подобного законодательного регулирования. Однако сама Конституция Российской Федерации устанавливает возможность ограничения основных прав и свобод общего характера, касающихся конституционно-правового статуса личности и определяющих допустимые пределы изъятий из основных прав и свобод и цели, которым такие изъятия должны быть соразмерны. В частности, согласно ч. 3 ст. 55 Конституции Российской

Федерации права и свободы человека и гражданина могут быть ограничены федеральным законом только в той мере, в какой это необходимо в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Безусловно, что цели ограничения прав и свобод должны быть не только юридически, но и социально оправданны, а сами ограничения – им адекватны, а также отвечать требованиям справедливости. Ограничения прав и свобод возможны только федеральным законом, причем на федеральном законодателе лежит обязанность обеспечивать соразмерность ограничения прав и свобод конституционно закрепленным целям. Однако в рассматриваемом случае все формальные критерии для подобного ограничения соблюдены.

Кроме того, не стоит забывать, что любая переписка итак потенциально становится известна соответствующему оператору связи, организатору распространения информации в сети Интернет. Действующее законодательство предусматривает достаточно жесткие требования, связанные с сохранением информации и обеспечением нераспространения полученных сведений третьим лицам.

Фактически принятый пакет законов в данном аспекте акцентировал внимание на возможности доступа по судебному решению уполномоченных органов к указанной информации и обеспечил гарантии ее сохранения в течение длительного времени для такого доступа. Вопрос о том, кто из специальных субъектов: уполномоченный государственный орган, призванный обеспечивать безопасность, или хозяйствующая организация, имеющая целью получение прибыли, потенциально более надежен с точки зрения выполнения вмененных публично-правовых обязанностей, в том числе – обеспечения информационной безопасности находящихся в их ведении данных, хотя и относится к разряду риторических, однако обнажает ряд новых проблем. В частности, о характере информации, которую законопослушный гражданин готов доверить оператору связи, но по каким-либо причинам опасается – уполномоченному органу.

Достаточно сложно однозначно установить, насколько принятые меры отвечают критерию соразмерности – это прерогатива компетентного правоприменителя, в то же время представляется, что законопослушным гражданам, которые не замышляют ничего предосудительного, введение подобных дополнительных мер контроля должно только подкрепить уверенности в обеспечении их собственной безопасности и безопасности государства в целом.

2.3 Опыт России

На сегодняшний день в нашей стране сформирована достаточно серьезная законодательная база, регулирующая распространение информации в российском сегменте Интернета – Рунете.

Следует отметить, что в силу особой специфики объекта регулирования законодательство в информационной сфере нуждается в постоянном обновлении и совершенствовании, что обусловливает динамичность и высокую частоту внесения изменений в нормативно-правовые акты.

При этом важно понимать, что данные изменения опираются на базовый в этой области документ – Стратегию развития информационного общества в Российской Федерации на 2017–2030 годы (далее – Стратегия). Красной нитью через весь документ проходит идея необходимости совершенствования законодательного регулирования в информационной сфере. Так или иначе все изменения в законодательстве в этой сфере осуществляются с опорой на п. 24 Стратегии: «Целями формирования информационного пространства, основанного на знаниях (далее – информационное пространство знаний), являются обеспечение прав граждан на объективную, достоверную, безопасную информацию и создание условий для удовлетворения их потребностей в постоянном развитии, получении качественных и достоверных сведений, новых компетенций, расширении кругозора».[28]

Еще в 2012 г. в контексте законодательного регулирования интернет-активности был задан общий вектор, направленный на создание эффективного юридического и политического инструментария, предназначенного для установления контроля над интернет-пространством. Сегодня данный вектор остается актуальным.

В ряде случаев такие инициативы представляются особенно актуальными и востребованными обществом. Так, отличительной чертой любого демократического государства является необходимость защиты подрастающего поколения своих граждан от непроверенной, спорной, а порой и вовсе опасной информации. Наличие этой объективной потребности стало причиной принятия 18 декабря 2018 г. федерального закона, в соответствии с которым были внесены изменения в федеральные законы «Об информации» и «О защите детей от вредной информации».[29] Был значительно расширен перечень

[28] О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы [Электронный ресурс]: указ Президента РФ от 09.05.2017 № 203 // КонсультантПлюс: справочная правовая система. - URL: http://www.consultant.ru. (дата обращения: 08.05.2020).

[29] О внесении изменений в статью 15.1 Федерального закона “Об информации, информационных технологиях и о защите информации” и статью 5 Федерального закона “О защите детей от информации, причиняющей вред их

запрещенных для распространения среди детей видов информации. Более того, теперь блокировке подлежат не только сами информационные ресурсы, распространяющие вредоносную информацию, например нацеленную на привлечение лиц, не достигших 18 лет, к участию в противоправных деяниях, но и любой контент, склоняющий к действиям, опасным для жизни или здоровья самих детей либо других людей. Постоянное увеличение числа блогеров, интернет-медиа издательств, занимающихся в т.ч. распространением критических воззрений на политические действия представителей российской власти, спровоцировало принятие ряда законов, предусматривающих определенную ответственность за отказ от удаления той или иной информации, способной нанести репутационный и другие виды урона тем или иным лицам.

Так, в апреле 2018 г. был принят закон о внесении изменений в федеральный закон «Об исполнительном производстве» и федеральный закон «Об информации», который наделял судебных приставов правомочием принимать решение об ограничении доступа к сайтам за отказ удалять сведения, порочащие честь и достоинство гражданина или деловую репутацию юридического лица.[30]

В сентябре 2018 г. был принят еще один закон, в соответствии с которым были внесены изменения в Уголовный кодекс РФ, а также Кодекс об административных правонарушениях РФ. Изменения заключаются в ужесточении наказания за неисполнение требований решений судов, обязывающих прекратить распространение незаконной информации, и, более того, подразумевают наступление и уголовной ответственности для тех лиц, которые уже подвергались ранее административному наказанию за соответствующее правонарушение, с наказанием в форме ареста на срок до 3 месяцев или лишения свободы на срок до 2 лет.[31] В конце сентября 2018 г. вступил в силу закон о штрафах для поисковиков за неисполнение закона о регулировании VPN, прокси, анонимайзеров и поисковиков. Игнорирование закона о запрете обхода блокировок теперь грозит операторам административной ответственностью.[32]

здоровью и развитию" [Электронный ресурс]: Федеральный закон от 18.12.2018 N 472-ФЗ. – Собрание законодательства РФ. 24.12.2018. N 52. // КонсультантПлюс: справочная правовая система. - URL: http://www.consultant.ru/document/cons_doc_LAW_313684/ (дата обращения: 09.05.2020).

[30] О внесении изменений в Федеральный закон "Об исполнительном производстве" и статью 15.1 Федерального закона "Об информации, информационных технологиях и о защите информации" [Электронный ресурс]: Федеральный закон от 23.04.2018 N 102-ФЗ – Собрание законодательства РФ. 30.04.2018. N 18.- URL: https://www.glavbukh.ru/npd/edoc/99_557240591 (дата обращения: 09.05.2020).

[31] О внесении изменения в статью 315 Уголовного кодекса Российской Федерации [Электронный ресурс]: Федеральный закон от 02.10.2018 N 348-ФЗ. – Собрание законодательства РФ. 08.10.2018. N 41. // КонсультантПлюс: справочная правовая система. - URL: http://www.consultant.ru/document/cons_doc_LAW_307994/ (дата обращения: 10.05.2020).

[32] О внесении изменений в Кодекс Российской Федерации об административных правонарушениях [Электронный ресурс]: Федеральный закон от 27.06.2018 N 155-ФЗ. – Собрание законодательства РФ.

В данном контексте нелишним будет вспомнить о таких принципах информационной политики в России, обозначенных в Стратегии, как обеспечение прав граждан на доступ к информации и обеспечение свободы выбора средств получения знаний при работе с информацией. На наш взгляд, рассмотренные изменения в российском законодательстве не в полной мере соответствуют названным принципам.

Комплекс законов и подзаконных актов, известный как пакет Яровой, также получил свое развитие в 2018 г. Так, пакет антитеррористических законов, принятый в июле 2016 г., обязал операторов связи и интернет-компании хранить информацию о содержании разговоров и переписки пользователей, включая фото-, видео- и звуковые файлы, с последующим предоставлением их при необходимости по запросу спецслужб. 1 июля 2018 г. эти нормы вступили в силу: операторы связи и интернет-компании теперь обязаны хранить весь трафик в течение полугода.[33]

Процесс реализации пакета Яровой уже привел к росту тарифов на все виды связи. Если принять во внимание непростую экономическую обстановку в стране, а также негативную реакцию бизнес-сообщества, простых граждан и частоту внесения изменений в данный комплекс законов и подзаконных актов, становится очевидной слабость качественной составляющей прогноза последствий, привнесенных процессом реализации пакета Яровой.

Еще одна проблема связана с уголовным преследованием интернет-пользователей за репосты и лайки в социальных сетях, что вызвало в 2018 г. Широкий общественный резонанс.

Данная проблема освещалась всеми российскими СМИ и была предметом дискуссии в социальных сетях в течение более полугода. Российские власти не могли не отреагировать, и уже в октябре 2018 г. президент РФ внес в Госдуму два законопроекта, подразумевавших частичную декриминализацию ст. 282 УК РФ «Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства».[34] Так, в соответствии с внесенными по инициативе главы государства поправками, экстремистские высказывания в Интернете теперь влекут за собой административную, а не уголовную ответственность, а в КоАП была включена соответствующая статья 20.31 «Возбуждение ненависти либо вражды,

---

02.07.2018. N 27. // КонсультантПлюс: справочная правовая система. - URL: http://www.consultant.ru/document/cons_doc_LAW_301055/ (дата обращения: 10.05.2020).

[33] О внесении изменений в Федеральный закон "О противодействии терроризму" [Электронный ресурс]: Федеральный закон от 06.07.2016 N 374-ФЗ // КонсультантПлюс: справочная правовая система. - URL: http://www.consultant.ru/document/cons_doc_LAW_201078/ (проверено 02.05.2020).

[34] Уголовный кодекс Российской Федерации [Электронный ресурс]: Федеральный закон от 13.06.1996 N 63-ФЗ. // КонсультантПлюс: справочная правовая система. - URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 12.05.2020).

а равно унижение человеческого достоинства».[35] Уголовная же ответственность наступит только в случае, если лицо уже привлекалось к административной ответственности за аналогичное деяние в течение одного года.

Важно отметить, что названные законы о декриминализации ст. 282 УК РФ наделены обратной силой. Следовательно, все текущие уголовные дела за лайки и репосты будут рассматриваться с учетом внесенных поправок, а все вступившие в силу приговоры по ст. 282 УК РФ будут пересмотрены.

Говоря о законодательном регулировании интернет-пространства, сказать следует и о не менее нашумевшем в конце 2018 г. законопроекте, нацеленном на обеспечение безопасного и устойчивого функционирования сети Интернет на территории РФ (спонсорами законопроекта выступили члены Совета Федерации Андрей Клишас и Людмила Бокова, а также депутат Госдумы Андрей Луговой). В пояснительной записке к законопроекту указывается, что акт «подготовлен с учетом агрессивного характера принятой в сентябре 2018 года Стратегии национальной кибербезопасности США». 12 февраля 2019 г. законопроект был принят Государственной думой в первом чтении: за принятие проекта закона проголосовали 334 депутата, против – 47. Среди проголосовавших против есть представители всех фракций, кроме «Единой России».[36]

Вывод: Важнейшая роль Интернета сегодня не столько информационная, сколько коммуникативная. Безусловно, в условиях глобальных информационных войн любому государству необходимы инструменты для эффективной защиты населения от негативного информационного влияния. Вместе с тем не стоит забывать, что, возможно, лучший метод защиты – не возведение «цифровых» защитных сооружений, но просвещение, повышение информационной грамотности населения страны.

---

[35] О внесении изменений в Кодекс Российской Федерации об административных правонарушениях [Электронный ресурс]: Федеральный закон от 27.12.2018 N 521-ФЗ. – Собрание законодательства РФ. 31.12.2018. N 53, ч. I. // КонсультантПлюс: справочная правовая система. - URL: http://www.consultant.ru/document/cons_doc_LAW_314662/ (дата обращения: 12.05.2020).

[36] Справка о результатах голосования по вопросу (первое чтение) о проекте федерального закона № 608767-7 «О внесении изменений в некоторые законодательные акты Российской Федерации» (в части обеспечения безопасного и устойчивого функционирования сети Интернет на территории Российской Федерации). – Государственная Дума. / Официальный сайт. – Электрон. дан. – URL: http://vote.duma.gov.ru/vote/107004 (дата обращения: 12.05.2020).

3 Укрепление национальной безопасности на базе цифровой экономики

3.1 Совершенствование нормативно законодательной базы

В целях стимулирования российской экономики в 1998 году было принято Постановление Правительства РФ от 31.03.1998 №374 «О создании условий для привлечения инвестиций в инновационную сферу».[37] Цель данного постановления – снизить зависимость от зарубежных технологий, построить российский национальный рынок. Это стало одним из первых шагов в создании независимой и ведущей в мире российской цифровой экономики.

На сегодняшний день прогноз стратегических экономических планов правительства позволяет прогнозировать, что к 2025 году цифровая экономика в России увеличит национальный ВВП до 8,9 трлн рублей.

Указом Президента Российской Федерации №203 определена Стратегия развития информационного общества в Российской Федерации на период с 2017 по 2030 год.[38] Этот указ определяет цифровую экономику как всю экономическую деятельность, в которой ключевыми факторами производства являются цифровые. По сравнению с традиционными формами экономики цифровая экономика обеспечивает более эффективное производство, технологию, поставку, хранение, продажу и доступ к товарам и услугам.

Согласно данной программе, российское правительство финансирует следующие секторы цифровой экономики: образование и человеческие ресурсы, кибербезопасность, исследования и ИТ-инфраструктуру.

Доля России в цифровой экономике составляет 2,1% – в 1,3 раза больше, чем пять лет назад, но в 3 раза меньше, чем в ведущих странах, таких как США. Россия занимает шестое место в мире и первое место в Европе по количеству пользователей Интернета. Интернет-потребление в России за последние пять лет стремительно выросло, в среднем на 27% в год, и достигло 2 трлн рублей в 2015 году.

В 2015 и 2016 годах Российская Федерация оставалась на 41-м месте в индексе сетевой готовности, занимая третье место по готовности, использованию и воздействию. Улучшения этих рейтингов ожидаются в результате более благоприятного законодательного климата 2018 года. Поскольку мобильные и фиксированные тарифы на Интернет очень доступны, индивидуальное использование Интернета продолжает расти, оставляя Россию на 40-м месте в этой категории.

---

[37] О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы [Электронный ресурс]: указ Президента РФ от 09.05.2017 № 203 // КонсультантПлюс: справочная правовая система. - URL: http://www.consultant.ru. (дата обращения: 15.04.2020)

[38] О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы [Электронный ресурс]: указ Президента РФ от 09.05.2017 № 203 // КонсультантПлюс: справочная правовая система. - URL: http://www.consultant.ru. (дата обращения: 15.04.2020)

Однако инфраструктура не успевает за спросом: доступная в России пропускная способность Интернета на одного пользователя снижается.

Тем не менее каждый из этих рейтингов формируется на счет различных статистических данных и показателей, беря за основу оценки различные аспекты цифровизации. В результате этих различных подходов Бостонская Консалтинговая группа определяет место России на уровне 39-го, а Всемирный экономический форум или глобальный институт McKinsey – 14-е место.

Рейтинги определяют уровень доступа к международному сотрудничеству и в целом к инвестициям в цифровую экономику. Рейтинги представляют собой оценки того, кто лидирует на пути к экономике знаний, и прогноз того, кто находится на самом быстром пути к достижению намеченного результата. Рейтинги предполагают, что это всего лишь индикаторы. Необходимо обеспечить понимание реального содержания киберпространства для широкой аудитории, чтобы потребители могли участвовать в цифровой производительности.

Цифровая экономика была введена президентом России в качестве формально-правовой концепции как новый инструмент развития государства, экономики, бизнеса и общества. Программа «Цифровая экономика Российской Федерации»[39] определила этапность развития цифровой экономики; цели должны быть достигнуты в 2018, 2020 и 2024 годах. Однако по состоянию на данный момент данная программа была отменена.[40]

В России инвестиции частных компаний, ориентированных на цифровизацию, составляют 2,2% ВВП. Для сравнения: США удерживают самый высокий уровень в мире на уровне 5%, с Западной Европой на втором месте на 3,9% и Бразилией на третьем на 3,6%. В настоящее время Россия на 5–8 лет отстает от стран, возглавляющих рейтинг по общему уровню цифровизации. Уровень развития инфраструктуры в России по-прежнему выше, чем в других странах БРИКС, хотя Китай и Бразилия активно сокращают разрыв, менее чем в 1,6– 1,2 раза за пять лет.

Если Россия привлечет внутренние государственные средства для увеличения своих инвестиций в информационно-коммуникационные технологии (ИКТ), чтобы соответствовать среднему уровню рассмотренных выше конкурентов, то цифровая экономика в России

---

[39] Паспорт национальной программы «Цифровая экономика Российской Федерации» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 24.12.2018 № 16) [Электронный ресурс] // КонсультантПлюс: справочная правовая система. – URL http://www.consultant.ru/document/cons_doc_LAW_319432/ (дата обращения: 16.05.2020)

[40] О признании утратившим силу Распоряжения Правительства РФ от 28.07.2017 №1632-р [Электронный ресурс]: Распоряжение Правительства РФ от 12.02.2019 №195-р // Собрание законодательства РФ. – 25.02.2019. – №8. // КонсультантПлюс: справочная правовая система. – URL http://www.consultant.ru/document/cons_doc_LAW_318450/ (дата обращения: 16.05.2020)

вырастет до 5,9% ВВП. Сорок процентов цифровой экономики России в настоящее время сосредоточено в Москве. Цифровое управление в Москве и Санкт-Петербурге (за которое Москва заняла первое место по итогам 2017 года у «активных граждан» благодаря электронному управлению) способствует укреплению позиций России как мирового лидера в области оцифровки. Восемьдесят процентов государственных расходов на информационные технологии сосредоточено в 86 регионах. Россия занимает высокое место в мировой телекоммуникационной отрасли.

К 2019 году Россия заняла первое место в Европе по количеству абонентов ТВ с 9-процентным увеличением абонентов в 2019 году до 55-процентного уровня насыщенности ТВ. Россия заняла первое место в Европе по количеству пользователей широкополосного Интернета с более чем 27 миллионами абонентов в 2019 году, достигнув 49-процентного уровня насыщенности (от 60% до 80% в крупных городах и более 50% в городах с населением в полмиллиона человек).

Россия занимает первое место в мире по насыщенности услугами сотовой связи с уровнем насыщенности 166% по количеству SIM-карт и 110% по активным абонентам. Россия занимает первое место в Европе и третье место в мире по количеству пользователей интернет-видео. По состоянию на февраль 2019 года российская база пользователей Интернета занимает первое место в Европе и шестое место в мире с 66,8 млн уникальных посетителей.

С 2013 году эта отрасль была законодательно закреплена как радиоэлектронная экономика[41], относящаяся к передаче информации посредством радиоволн. Радиоэлектронная экономика входит в цифровую экономику.

Со времени принятия в 2003 году законодательства, содействующего технологическому прогрессу, был достигнут значительный прогресс.

Россия приняла активные меры по законодательному закреплению использования новых технологий для расширения возможностей своей экономики и граждан внутри страны. Россия стремится закрепить практику цифровой сферы через международное право и организации понимают, почему государство и академически созданные НИОКР не перешли в потребительскую экономику, квалификация должна быть сделана: Россия имеет технологии связи и цифровой сферы, но ее относительно небольшой внутренний рынок создает мало коммерческих стимулов.[42] Поэтому эти технологии использовались в

[41] Южаков В.Н. Направления совершенствования правового регулирования в сфере стимулирования развития информационных технологий / В.Н. Южаков, А.А. Ефремов // Право и информационные технологии. – 2017. – №5. – С. 17–20.

[42] Данилин А.В. Электронные государственные услуги и административные регламенты: от политической задачи к архитектуре «электронного правительства». – М.: Инфра-М, 2018. – С 244-246.

некоммерческих целях в государственном секторе, а не в качестве потребительских товаров. Развитие российской цифровой экономики было эволюционным, тогда как в Китае оно считалось революционным.

Размер внутреннего рынка страны определяет темпы роста цифровой промышленности этой страны. Именно поэтому интернационализация российской промышленности имеет столь высокий приоритет. Точно так же, как в постсоветскую эпоху капитал был ограничен, а кризисные периоды ограничивали инвестиции в обрабатывающую промышленность, санкции сейчас создают такие же препятствия для промышленности. Устранение блочной структуры экономики и облегчение сетей – часть цифровой революции.

Тем не менее, некоторые, особенно в области устойчивого развития Интернета, предположили, что Россия разработала новые преимущества и стремится регулировать использование цифровых и кибер-инструментов в международной сфере. Дигитальные сценарии для России в начале 2019 года показали, что Россия находится на пути к преобразованиям, подобным тем, которые происходят в Азии.

Создание российских инноваций и стимулирование внедрения российских разработок в национальные и международные потребительские товары – задача непростая. Запад выступил против глобальной интеграции России. Мотивация западных государств-политическая и экономическая, поскольку российские предприниматели становятся конкурентами уже сложившимся транснациональным корпорациям. Политическая дестабилизация и экономические санкции ограничивают глобализацию российского рынка. Въездной барьер для российских предпринимателей высок. Санкции могут быть преодолены с помощью цифровых решений, которые обеспечивают надежное взаимодействие.

При этом как российский, так и европейский бизнес смогут найти новые методы ведения бизнеса друг с другом, при условии возможности создания новых трансграничных стоимостных связей с Россией как де-факто обширным приграничным регионом между Китаем и ЕС.

Современное законодательство в области развития цифровой экономики предполагают самостоятельное развитие.

Сейчас санкции создают препятствия для экономики. В то время как Россия доказала свое ноу-хау в разработке информационных систем, преодоление политической стигматизации за рубежом является проблемой. Укрепление политического доверия является одним из аспектов, однако сила цифровых инструментов и программ сама по себе будет успешной. Завершение процесса создания экономически жизнеспособных и передовых информационных систем на национальном уровне является необходимым условием для

создания глобального присутствия. Уровень цифрового управления Москвы и Санкт-Петербурга способствует установлению уровня высоких достижений в мировом лидерстве в области цифровизации. Российская цифровая экономика также смягчит экономическое давление от санкций, так как прогнозируется увеличение ВВП до 8,9 трлн руб. к 2025 году.

Цифровое потребление в России уже превысило уровень в 2 трлн рублей в 2015 году. Если Россия увеличит объем своих инвестиций в ИКТ, в том числе за счет бюджетов домохозяйств, инвестиционных компаний и государства, до среднего уровня рассмотренных выше конкурентов, то доля цифровой экономики в России вырастет до 5,9% ВВП.

Эти товары, услуги и инструменты полезны для изменения структуры глобальной инфраструктуры Интернета, поскольку многие страны настаивают на построении своей инфраструктуры в соответствии с принципами, которые отличаются от тех, которые управляли первой и второй волнами инвестиций в США.

Доступ к новым технологиям, а также интеграция в глобальное общество знаний были ключевыми движущими силами перехода, начатого в 1980-х годах.

Для стимулирования инноваций необходимо защищать права интеллектуальной собственности на цифровые товары и услуги. Наибольшие проблемы связаны с защитой цифровой среды от киберпреступности, преодолением цифрового разрыва и защитой прав интеллектуальной собственности как средства создания ценности. Для реализации необходимых программ должна быть достигнута гармонизация и сотрудничество между министерствами. Тогда региональная интеграция через единую цифровую платформу ЕАЭС должна быть запущена с оптимальными условиями для технологической предпринимательской деятельности.[43]

В то время как основное внимание уделялось экономической ценности цифровой экономики, отличительной особенностью нашего времени является то, что практически все отрасли науки и техники, в том числе науки о жизни, интегрированы в цифровую среду.

Впоследствии расходы общества могут быть значительно сокращены за счет сокращения расходов на медицинское страхование или энергоснабжение. Переход к цифровому обществу трансформирует издержки, с которыми сталкивается общество, структуру налогообложения, а также характер рынка, в том числе труда, позволяя осуществлять индивидуальные сделки. В результате должны измениться границы между государственной и частной инфраструктурой, а также характеристики управления и ценообразования на инфраструктуру Интернета.

[43] Добролюбова Е.И. Совершенствование правового регулирования информационного обеспечения государственного управления // Государственная власть и местное самоуправление. – 2017. – №2. – С. 24–28.

Россия является мировым лидером в регулировании социальных последствий цифровой экономики как инструмента расширения возможностей и источника опасности. Масштабы цифровой трансформации российской экономики были образцовыми и получают обновленное государственное руководство. Цифровая экономика должна быть дополнительно спонсирована как возможность увеличения государственных доходов для российского правительства. Горизонт цифрового сектора бесконечен, и многие из будущих инноваций выходят за рамки нынешнего воображения.

Дигитализация – это, на самом базовом уровне, информация, записанная в атомах. Как и электроны в электрическом токе, информация передается в сетях непрерывных потоков через виртуальную и физическую инфраструктуру. Слияние содержания и материи в виртуальное, такое как криптовалюты или электронная валюта, подкрепленное стоимостью электричества, связывает денежное с его средствами видения в мире. Инновации являются движущей силой развития цифровой экономики.

3.2 Контроль и мониторинг государства с использованием цифровых технологий

Еще в начале 2018 года в РФ была проведена экспертная дискуссия, основной темой которой стало изменение в методологии государственного контроля и надзора в экономической среде. Вопрос глобальной цифровизации всей экономической среды стал наиболее актуальным и значимым в ходе проведения дискуссии. Так, были рассмотрены фундаментальные инновации в сфере государственного финансового контроля, в том числе, была дана оценка мониторингу функционирования банковской сферы и осуществления бюджетного надзора в условиях цифровой экономики.

На сегодняшний день в России разработан целый ряд стратегических документов, затрагивающих цифровизацию и развитие цифровой экономики в целом. К ним относятся:

1. Национальная программа «Цифровая экономика Российской Федерации».

2. Государственная программа «Информационное общество (2011-2020 годы)».

3. Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы.

4. Стратегия развития отрасли информационных технологий в Российской Федерации на 2014 – 2020 годы и на перспективу до 2025 года.

5. Стратегия инновационного развития Российской Федерации на период до 2020 года.

28 июля 2017 года Председатель Правительства РФ Медведев Д.А. утвердил программу «Цифровая экономика Российской Федерации» в целях дополнения Указа Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы». Так, премьер-министр поручил Минэкономразвития России подготовить проект создания национальной системы управления данными на базе Росстата.

Система призвана обеспечить полную цифровизацию процессов сбора и обработки данных на основе единых методологических и технологических подходов. Конечной целью является формирование единого информационного пространства данных в России для государства, бизнеса и граждан. Данная программа призвана увеличить степень информированности и цифровой грамотности, улучшить доступность и качество государственных услуг для граждан, в том числе способствовать повышению безопасности как внутри страны, так и за ее пределами. К 2025 году национальная система управления данными должна реализовать следующие ожидаемые результаты:

– сокращение отчетности и переход к первичным данным с соответствующим снижением транзакционных издержек бизнеса;

– повышение качества данных и выполнение массовой программы интеграции не менее 60% государственных информационных систем;

– интеграция коммерческих и государственных данных. Субъектами процесса государственного финансового контроля, с одной стороны, выступают различные бенефициары ресурсов казны (как финансово-бюджетных, так и, в частности, материальных), с другой стороны – различные специализированные институты – контрольно-надзорные органы.[44] К первым можно отнести органы государственной власти и местного самоуправления, казенные и бюджетные учреждения, а также иные юридические и физические лица, получающие финансовые средства из федерального и субфедеральных бюджетов. Контрольно-надзорными органами в области финансовых отношений в России выступают Счетная палата РФ и Федеральное казначейство, а также иные правоохранительные и контрольно-надзорные органы.

До 02 февраля 2016 года надзор осуществляла упраздненная ныне Служба финансово-бюджетного надзора (Росфиннадзор). Функции по контролю и надзору в финансово-бюджетной сфере переданы Федеральному казначейству.

В соответствии со статьей 256 Бюджетного кодекса РФ «государственный (муниципальный) финансовый контроль осуществляется в целях обеспечения соблюдения

[44] Прокофьев С.Е. Новации в сфере государственного финансового контроля, осуществляемого казначейством России // Финансы и кредит. – 2017. – № 10 (634). – С. 2-11.

бюджетного законодательства Российской Федерации». К полномочиям соответствующих органов внутреннего государственного (муниципального) финансового контроля относится проверка соблюдения финансовыми органами (главными распорядителями (распорядителями) и получателями средств бюджета, которому предоставлены межбюджетные трансферты) целей, порядка и условий предоставления межбюджетных трансфертов, бюджетных кредитов, а также достижения ими показателей результативности использования указанных средств, соответствующих целевым показателям и индикаторам, предусмотренным государственными программами (пп. «б» п. 7 Правил № 1092).

Вместе с тем внутренний финансовый контроль в условиях цифровизации является не только средством контроля, но и гибким инструментом для повышения функционирования и оперативного решения текущих и стратегических задач.

Отсюда следует, что основная идея цифровизации – исключение всех рутинных процессов из деятельности человека, серьезное повышение эффективности работы, в том числе контрольной деятельности.

Говоря о внутреннем финансовом контроле на уровне государства, нельзя не выделить ряд важнейших вопросов, возникающих при его регулировании: как, кто и каким образом будет строить цифровое государство, и каково место и роль контрольной функции в этой системе.

В условиях цифровизации повышается ответственность контролера. Увеличение объемов данных для анализа должно способствовать проведению более глубокого, детального и всестороннего анализа, что обеспечит получение более точной информации. Поэтому в случае негативной ситуации возрастает спрос не только к тому, чьими действиями эта ситуация спровоцирована, но и к контролеру, который, видя негативные тенденции, их не предотвратил. В таком случае можно говорить о том, что контролер становится соучастником бизнес-процесса. Отсюда возникают новые механизмы и инструменты контроля.

Стоит отметить, что Казначейство является не только контролирующим органом, но и выполняет функции кассира, главного бухгалтера и, в некотором роде, IT-менеджера, являясь оператором крупнейших информационной систем, в частности, zakupki.gov.ru. В ближайшем будущем будут максимально автоматизированы массовые казначейские операции, все документы и процессы станут подписываться электронной подписью, и не смогут быть изменены в процессе реализации. Впоследствии они будут продолжительное время храниться в электронном архиве, к которому при необходимости можно обратиться в любое время. Результатом таких реформ должно стать снижение трудозатрат на проведение

внутреннего государственного финансового контроля, повышение точности и качества анализа, генерация необходимой отчетности, а также применения принципов управления рисками. Все это позволит повысить прозрачность деятельности подведомственных организаций, что сократит количество предписаний контрольных органов.

Современные информационные и телекоммуникационные технологии предоставляют реальные инструменты для развития и совершенствования процессов внутреннего государственного контроля.

Однако наиболее общественно значимые результаты в указанной сфере, как правило, достигаются за счет вовлечения в управленческий оборот агрегированных и структурированных ресурсов. Обычно до фазы принятия того или иного государственного решения соответствующий орган власти должен производить анализ огромного массива различных данных. Зачастую эти информационные базы ведомственно разобщены и не интегрированы между собой, что затрудняет как доступ, так и работу с ними. В этой связи первоочередной задачей выступает стандартизация аналитических процессов, связанная, прежде всего, со стандартизацией системы показателей, однозначностью их экономической интерпретации и методов их аналитической обработки.

На практике, государство сталкивается с рядом проблем, препятствующих быстрой реализации поставленных целей на государственном уровне. Согласно опросу Центра стратегических разработок, около 80% сотрудников госаппарата РФ занимаются не стратегическими вопросами, а выполнением текущих задач.

Также отсутствует система проверки работы госслужащих. На сегодняшний день, на них еще не распространилась система ключевых показателей эффективности (KPI), которая могла бы стать движущей силой на пути к цифровизации. Одной из важнейших проблем можно назвать низкую скорость принятия решений. Служащие госаппарата могут отвечать на запросы в течение одного или нескольких месяцев, хотя технически сократить сроки принятия решений вполне возможно. В качестве положительного примера можно привести опыт работы самого богатого человека в Китае, предпринимателя Д. Ма, основателя и председателя совета директоров компании Alibaba Group, который установил для своего банка обязательный для всех сотрудников принцип: 310. Его расшифровка заключается в следующем: 3 – это три минуты, которые должны уходить у клиента на заполнение своего запроса, 1 – это одна секунда на прием запроса, 0 – никакой ручной работы при исполнении. В условиях цифровизации возникают новые составляющие профессии контролера – финансовые технологи, которые занимаются анализом бизнес-процессов, и аналитики, которые через механизм бюджетного мониторинга своевременно

выявляют риски и управляют ими. Говоря о перспективах сохранения профессий под воздействием цифровизации, можно предположить, что ни профессия казначея, ни профессия государственного финансового контролера не исчезнут, а только поднимутся на новый уровень эволюции.

При этом специалист, соответствующий задачам цифровизации и создания единых информационных систем, должен обладать глубокими знаниями и в юриспруденции, и в экономике, и в IT-технологиях. Это ставит перед образовательной средой задачи совершенно другого уровня подготовки специалистов, которые будут отвечать требованиям цифровой экономики. Очевидно, что для совершенствования качества внутреннего государственного финансового контроля в условиях цифровизации необходимо:

– внедрять новые информационные технологии и системы в работе министерств и ведомств, которые будут коррелировать между собой;

– повышать открытость и уровень доверия между гражданами и государством;

– сокращать избыточные контрольно-надзорные функции, которые являются одним из следствий недостатка такого доверия, заменив их автоматизированными системами контроля;

– создание совершенно нового уровня подготовки специалистов, которые будут отвечать требованиям цифровой экономики;

– использование опыта зарубежных стран в создании цифрового государства. Современный инструментарий государственного финансового контроля должен рассматриваться как совокупность автоматизированных и в максимальной степени не коррупционных операций, основанных на интеграции его субъектов в единое информационное и транзакционное пространство. При этом необходимо параллельно развивать также инфраструктуру общественного и ведомственного контроля, что позволит гражданскому обществу и государственным институтам более эффективно сотрудничать в этой сфере.

Несмотря на все сложности, связанные с разработкой и внедрением цифровых технологий, цифровизация экономики приобретает масштабный характер, затрагивая все сферы народного хозяйства. И уже сегодня становится понятным, что без эффективных элементов государственного управления, в том числе внутреннего государственного финансового контроля, построить эффективную передовую экономику не получится.

3.3 Способы измерения доли цифровой экономики

Развитие цифровых технологий создаёт новые возможности и делает доступным большое количество видов экономической деятельности. Принимая во внимание растущую вследствие этого экономическую значимость, измерение экономического роста в цифровой экономике является первоочередной задачей. Однако здесь существует немало сложностей (см. Таблица 3)

Таблица 3 - Проблемы измерения цифровой экономики

Проблема	Суть проблемы
Определение рамок цифровой экономики	Определения цифровой экономики весьма разнообразны и подчас не совпадают друг с другом. Само по себе это не делает измерение цифровой экономики сложным, однако затрудняет сравнительный анализ. Те же определения, которые не могут провести четкую грань между традиционной и цифровой экономикой, затрудняют и исходные измерения.
Проблема качества данных	В настоящий момент, особенно в развивающихся странах, существует фундаментальная проблема с собираемыми данными – они либо отсутствуют, либо недостоверны. Это усугубляется дальнейшим развитием инноваций – сбор данных всегда остается позади технического прогресса.
Виртуальность цифровой экономики	Многие типы цифровой экономической деятельности не сразу создают готовый продукт. Некоторые услуги такого типа могут иметь промежуточный характер на уровне «бизнес – бизнес» или на уровне потребителей; могут возникать трудности с подсчетом добавленной стоимости; кроме того, цифровые услуги оказываются в виртуальном пространстве, следовательно, их бывает непросто отследить, особенно если имеет место трансграничная электронная торговля.

Проблемы, связанные с точной оценкой объема цифровой экономики, заключаются в том, что не существует каких-либо специальных методов, позволяющих это сделать, однако имеется возможность дать хотя бы приблизительную оценку. Важно отметить, что базой для оценки служит объем цифрового сегмента экономики (ИТ-сектора);

Рассмотрим метод «интернет-экономики», который основывается на доле ВВП, создаваемой экономической деятельностью с использованием Интернета. Метод представляет собой срез трех уровней анализа, представленных на рисунке 1, за

исключением некоторых элементов цифрового сектора, а также видов деятельности, не связанных с интернетом из цифровой и цифровизированной экономики (например, товаров и услуг из сегмента мобильных устройств). Иной подход основывается на оценке сектора мобильных устройств и услуг, они представлены как часть цифрового сектора, частично отнесенных к цифровой экономике. (см. Рисунок 1)

Рисунок 1 – Уровни цифровой экономики

Принимая во внимание существование мобильных устройств с доступом в Интернет, со временем мобильный и интернет-сегменты будут до определенной степени перекрывать друг друга при оценке масштабов интернет-экономики.

В настоящее время для оценки уровня цифровизации экономики Российской Федерации рассчитывается индекс «Цифровая Россия». Данный индекс отражает наличие и успешность инициатив, связанных с цифровизацией на региональном уровне, основываясь на событиях, которые имеют отношение к процессу цифровизации регионов, отраженных в открытых источниках. Если та или иная инициатива имеет конкретные действия не противоречит государственному стратегическому взгляду и имеет положительные социально-экономические и бизнес эффекты, она получает 100 баллов. Индекс рассчитывается в целом по стране и по всем 85 ее субъектам.

Результаты расчета индекса выявили существенное различие уровня цифровизации по федеральным округам и субъектам РФ. 1-е место по цифровизации экономики занимает Уральский федеральный округ, на последнем — Северо-Кавказкий округ (см. Таблица 4). Однако темпы цифровизации у «аутсайдера» выше, чем у лидирующего. Высокие темпы внедрения цифровых технологий демонстрируют Приволжский и Сибирский федеральные округа.

Таблица 4 – Динамика индекса «Цифровая Россия» по федеральным округам

Федеральный округ		Значение индекса				Темп Роста, %
		2017	Место	2018	Место	
1	Уральский	57,17	1	65,81	1	115,1
2	Центральный	50,05	3	59,82	2	119,5
3	Приволжский	46,93	4	59,55	3	126,9
4	Северо-Западный	50,90	2	58,95	4	115,8
5	Сибирский	41,91	7	53,48	5	127,6
6	Дальневосточный	44,20	5	52,28	6	118,3
7	Южный	43,06	6	51,35	7	119,3
8	Северо-Кавказский	33,37	8	43,44	8	130,2

Разрыв значений индексов «Цифровая Россия» у лидеров и аутсайдеров цифровизации достигает двукратной величины (см. Таблица 5). Отклонение значений субъектов-лидеров от среднего уровня цифровизации составляет 1,45–1,3, а у субъектов-аутсайдеров — 1,73–1,41 раза. Правда, необходимо отметить сокращение разрывов в 2018 г. по сравнению с 2017 г. по всем показателям цифровизации.

Таблица 5 - Пропорции цифровой трансформации в субъектах РФ

Показатель	Итоговый средний индекс «Цифровая Россия»	
	2017	2018
10 лидеров цифровизации	66,66	72,73
Медианное значение	45,92	55,94
10 аутсайдеров цифровизации	26,62	39,50
Отклонение лидеров от медианы, раз	1,45	1,30
Отклонение медианы от аутсайдеров, раз	1,73	1,41
Отклонение лидеров от аутсайдеров, раз	2,50	1,84

Сегодня цифровизация экономики играет большую роль и в транзитном мире. По данным Boston consulting group (см. Рисунок 2) абсолютными лидерами по доле цифрового ВВП являются Великобритания с показателем 12,4% и Южная Корея с показателем 8%, Россия же занимает 16 место по доли цифровой экономики страны с показателем 2,8%.

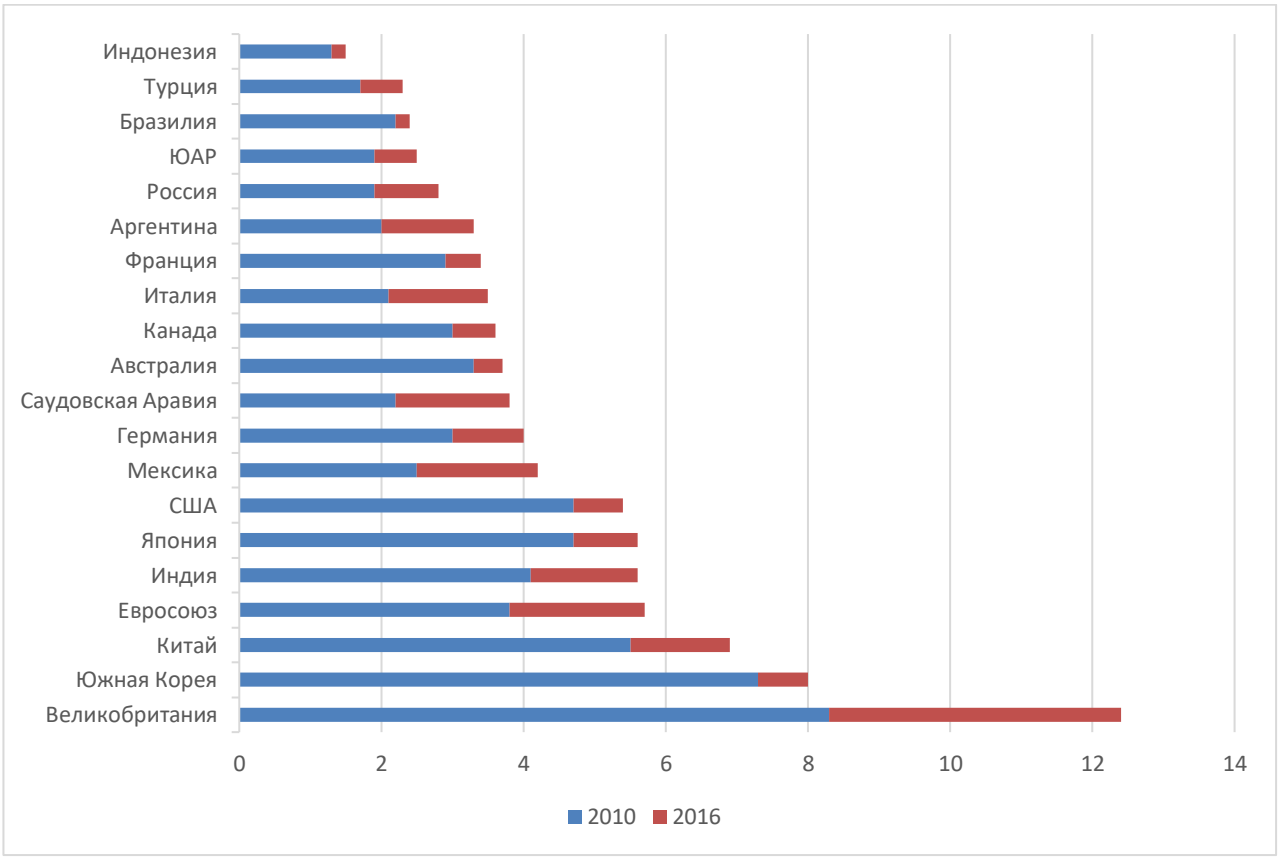

Рисунок 2 - Рост доли цифровой экономики в ВВП стран

ЗАКЛЮЧЕНИЕ

Цифровая экономика, по различным оценкам, несет в себе достаточно ощутимые изменения для более 50 % разных отраслей, а именно из-за того, что информационные технологии кардинально меняют бизнес-модели, которые повышают их эффективность, при устранении посредников и оптимизации. Специалисты Всемирного банка выяснили, что при росте числа пользователей высокоскоростного Интернета на 10 %, увеличится ежегодный прирост ВВП от 0,4 до 1,4 %.

Очень важно то, что в цифровой экономике достаточно быстро расширяются новые возможности для занятия предпринимательской деятельностью и самостоятельной занятостью. Переход к цифровой экономике в России будет одним из основных факторов роста ВВП – по оценкам, до 2035 года цифровые технологии обусловят от 19 до 34 % от всего увеличения ВВП. В настоящее время в России наблюдается быстрое развитие цифровой экономики.

Во многих случаях вложение инвестиций в развитие информационных технологий позволяют получить дивиденды в виде:

– экономического роста;

– создания новых рабочих мест;

– появления новых видов услуг для населения и бизнеса;

– сокращение издержек на государственное управление в рамках

проектов электронного правительства.

Основным приоритетом развития России сегодня является переход на цифровую экономику.

В программе «Цифровая экономика России» до 2035 года указаны показатели, которые необходимо достичь за период ее реализации. А именно, к этому сроку 97 % домашних хозяйств в России должны иметь доступ к широкополосному интернету – 100 Мбит/с, а города миллионники должны быть обеспечены устойчивым покрытием сети 5G и выше. Система управления программой предполагает, что после согласования этого плана с ведомствами он должен быть рассмотрен сначала на подкомиссии по цифровой экономике, потом должен быть утвержден комиссией по информационным технологиям. В то же время поправки к бюджету 2018 года, которые правительство будет направлять в парламент, в Думу, формируются еще до того, как план утвержден.

При этом план предполагает не только те мероприятия, которые уже заложены в бюджете, но и новые. По разделу инфраструктура на 2018 год планируется продолжение

программы устранения цифрового неравенства – на это мероприятие в программе заложено 12,5 млрд. руб.

Также план предусматривает подключение больниц к интернету, на это предлагается выделить 14,6 млрд. руб. Достаточно большой раздел плана посвящен формированию у нас в стране платформ по работе с геоданными, данными дистанционного зондирования земли – на эти цели Минкомсвязь предлагает выделить около 10 млрд. руб.

Также ведомство предусмотрело необходимость провести ряд научно-исследовательских работ, в том числе в области исследования радиочастотного спектра, которые нужны для планирования сетей пятого поколения. На эти работы запланировано 285 млн. руб. По результатам исследований планируется подготовка изменений регулирования для скорейшего развития сетей 5G. Организации, которые будут проводить исследования, будет определены в ходе конкурсов.

К 2025 году цифровизация экономики России позволит увеличить ВВП страны на 4,1-8,9 трлн. руб., утверждают авторы исследования, проведенного консалтинговой компанией McKinsey. В ближайшем будущем конкурентоспособность компаний будет определяться уровнем их цифровизации. Понимая это, ведущие игроки активно внедряют цифровые инструменты в самых разных секторах экономики. Подводя итог, стоит отметить, что мир вошел в цифровую эпоху, когда новые технологии стремительно развиваются и меняют привычный уклад жизни, формируются новые отрасли и профессии, открываются новые возможности для развития. Наступила «новая эра» – эра высоких технологий и коммуникаций. Программа «Цифровая экономика Российской Федерации» направлена на формирование в России благоприятной регуляторной среды для применения цифровых технологий в экономике, наращивание компетенций в области цифровых технологий российских предприятий, развитие инфраструктуры обработки данных, подготовку достаточного количества качественных кадров.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. Уголовный кодекс Российской Федерации [Электронный ресурс]: Федеральный закон от 13.06.1996 N 63-ФЗ. (ред. От 27.12.2018) (с изм. и доп., вступ. в силу с 08.01.2019). – Собрание законодательства РФ. 17.06.1996. N 25. Ст. 2954; 31.12.2018. N 53, ч. I. Ст. 8495. // КонсультантПлюс: справочная правовая система. - URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 12.05.2020).

2. О внесении изменений в статью 15.1 Федерального закона “Об информации, информационных технологиях и о защите информации” и статью 5 Федерального закона “О защите детей от информации, причиняющей вред их здоровью и развитию” [Электронный ресурс]: Федеральный закон от 18.12.2018 N 472-ФЗ. – Собрание законодательства РФ. 24.12.2018. N 52. // КонсультантПлюс: справочная правовая система. - URL: http://www.consultant.ru/document/cons_doc_LAW_313684/ (дата обращения: 09.05.2020).

3. О внесении изменений в Кодекс Российской Федерации об административных правонарушениях [Электронный ресурс]: Федеральный закон от 27.12.2018 N 521-ФЗ. – Собрание законодательства РФ. 31.12.2018. N 53, ч. I. // КонсультантПлюс: справочная правовая система. - URL: http://www.consultant.ru/document/cons_doc_LAW_314662/ (дата обращения: 12.05.2020).

4. О внесении изменений в Федеральный закон “Об исполнительном производстве” и статью 15.1 Федерального закона “Об информации, информационных технологиях и о защите информации” [Электронный ресурс]: Федеральный закон от 23.04.2018 N 102-ФЗ – Собрание законодательства РФ. 30.04.2018. N 18.- URL: https://www.glavbukh.ru/npd/edoc/99_557240591 (дата обращения: 09.05.2020).

5. О внесении изменения в статью 315 Уголовного кодекса Российской Федерации [Электронный ресурс]: Федеральный закон от 02.10.2018 N 348-ФЗ. – Собрание законодательства РФ. 08.10.2018. N 41. // КонсультантПлюс: справочная правовая система. - URL: http://www.consultant.ru/document/cons_doc_LAW_307994/ (дата обращения: 10.05.2020).

6. О внесении изменений в Кодекс Российской Федерации об административных правонарушениях [Электронный ресурс]: Федеральный закон от 27.06.2018 N 155-ФЗ. – Собрание законодательства РФ. 02.07.2018. N 27. // КонсультантПлюс: справочная правовая система. - URL: http://www.consultant.ru/document/cons_doc_LAW_301055/ (дата обращения: 10.05.2020).

7. О внесении изменений в Федеральный закон "О противодействии терроризму" [Электронный ресурс]: Федеральный закон от 06.07.2016 N 374-ФЗ // КонсультантПлюс:

справочная правовая система. - URL: http://www.consultant.ru/document/cons_doc_LAW_201078/ (проверено 02.05.2020).

8. Об электронной подписи [Электронный ресурс]: Федеральный закон от 06.04.2011 N 63-ФЗ // Парламентская газета. – 2011. – № 17. // КонсультантПлюс: справочная правовая система. - URL: http://www.consultant.ru/document/cons_doc_LAW_112701/ (дата обращения 26.05.2020)

9. Об обеспечении единства измерений [Электронный ресурс]: Федеральный закон от 26.06.2008 № 102-ФЗ // Собрание законодательства РФ. – 2008. – № 26. – ст. 3021. // КонсультантПлюс: справочная правовая система. - URL: http://www.consultant.ru/document/cons_doc_LAW_77904/ (дата обращения 26.05.2020)

10. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы [Электронный ресурс]: указ Президента РФ от 09.05.2017 № 203 // КонсультантПлюс: справочная правовая система. - URL: http://www.consultant.ru. (дата обращения: 15.04.2020)

11. О признании утратившим силу Распоряжения Правительства РФ от 28.07.2017 №1632-р [Электронный ресурс]: Распоряжение Правительства РФ от 12.02.2019 №195-р // Собрание законодательства РФ. – 25.02.2019. – №8. // КонсультантПлюс: справочная правовая система. – URL http://www.consultant.ru/document/cons_doc_LAW_318450/ (дата обращения: 16.05.2020)

12. Об утверждении программы «Цифровая экономика Российской Федерации» [Электронный ресурс]: Распоряжение Правительства РФ от 28.07.2017 N 1632-р // Собрание законодательства РФ. – 2017. – № 32. – ст. 5138. // КонсультантПлюс: справочная правовая система. - URL:http://www.consultant.ru/document/cons_doc_LAW_221756/ (дата обращения 26.05.2020)

13. Афанасьев С. Дискуссионные проблемы концепции национальной экономической безопасности / С. Афанасьев // Россия XXI. – 2016. – №2. – 317 с.

14. Архипов В.В. Проблема квалификации персональных данных как нематериальных благ в условиях цифровой экономики, или, нет ничего более практичного, чем хорошая теория // Закон. 2018. № 2. – 210 с.

15. Американский финансово-экономический журнал Forbes / Официальный сайт [Электронный ресурс]. – URL: https://www.forbes.ru/biznes/371421-ibm-predlozhil-novuyu-klassifikaciyu-cifrovyhbankov (дата обращения: 26.04.2020).

16. Восканян Е., Кривошапка И. Цифровизация экономики: влияние на управление [Электронный ресурс] / Восканян Е., Кривошапка И / СРРМ. – 2016. –№6 (99). – URL:

https://cyberleninka.ru/article/n/tsifrovizatsiya-ekonomiki-vliyanie-na-upravlenie (дата обращения: 16.05.2020)

17. Добролюбова Е.И. Совершенствование правового регулирования информационного обеспечения государственного управления / Добролюбова Е.И. / Государственная власть и местное самоуправление. – 2017. – №2. – 250 с.

18. Данилин А.В. Электронные государственные услуги и административные регламенты: от политической задачи к архитектуре «электронного правительства». – М.: Инфра-М, 2018. – 334 с.

19. Ершов И.А., Стукач О.В. Использование корректного нормирования статистических данных в кластерном анализе // Современные технологии поддержки принятия решений в экономике: сб. тр. Всероссийской научнопрактической. г. Юрга, 19-20 ноября 2015 г. – Национальный исследовательский Томский политехнический университет, 2015. – С. 32–34. – URL: http://elibrary.ru/item.asp?id=25334287. (дата обращения 29.04.20).

20. Зенкина Е.В. Международная валютно-финансовая система: Учеб. М.: Инфра-М, 2019. - 190 с.

21. Космачева Н.М., Стецюнич Ю.Н. Оценка качества управления кредитными рисками в банках по критерию просроченной задолженности // Экономика нового мира. – 2018. – № 4 (12). – С. 58-60.

22. Конвенции № 108 Совета Европы о защите физических лиц при автоматизированной обработке персональных данных. [Электронный ресурс] – URL: https://search.coe.int/directorate_of_communications/Pages/result_details.aspx?ObjectId=09000016808ac976 (Дата обращения: 09.05.2020).

23. Лебедева Н. Н. Право. Личность. Интернет: учебное пособие. – М., 2014. – С. 232.

24. Майоров А.В., Еремеев С.Г., Волкова А.М., Потапов А.Д. Цифровые технологии в управленческой деятельности: философско-антропологический и прикладной аспекты // Вестн. Ленингр. гос. ун-та им. А.С. Пушкина. – 2019. – № 1. – С. 34–48.

25. Меликсетян С.Н. Роль органов государственного финансового контроля в обеспечении финансовой безопасности России // Международный бухгалтерский учет. – 2018. – №13-14. – 256 с.

26. Нечаев К.А., Стукач О.В. Система поддержки производства полупроводниковых приборов как часть интернета вещей // Вестник науки Сибири / Томский политехнический университет (ТПУ). – Томск, 2018. – N 4(10). – С. 132–135.

27. Прокофьев С.Е. Новации в сфере государственного финансового контроля, осуществляемого казначейством России // Финансы и кредит. – 2017. – № 10 (634). – С. 2-11.

28. Программа «Цифровая экономика» Российской Федерации 2017 г. (утверждена распоряжением Правительства РФ от 28.07.2017 № 1632-р) [Электронный ресурс] // КонсультантПлюс: справочная правовая система. - URL: http://www.consultant.ru (дата обращения: 15.04.2020)

29. Программа развития цифровой экономики в Российской Федерации до 2035 года. – С. 19–20 // Ассоциация электронных торговых площадок [Электронный ресурс]. – URL: http://www.aetp.ru/news/item/410256 (дата обращения: 15.04.2020)

30. Паспорт национальной программы «Цифровая экономика Российской Федерации» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 24.12.2018 № 16) [Электронный ресурс] // КонсультантПлюс: справочная правовая система. – URL http://www.consultant.ru/document/cons_doc_LAW_319432/ (дата обращения: 16.05.2020)

31. Рощектаева У.Ю., Рощектаев С.А. Внутренний государственный (муниципальный) финансовый контроль в контексте становления институциональной структуры // Научный вестник Южногоинститута менеджмента. – 2018. – № 3. – 82 с.

32. Российский коммерческий банк «Тинькофф Банк» // Официальный сайт Тинькофф Банк. – URL: https://www.tinkoff.ru\ (дата обращения: 28.04.2020)

33. Стецюнич Ю.Н. Российский коммерческий банк «Тинькофф Банк» // Официальный сайт Тинькофф Банк. – URL: https://www.tinkoff.ru\ (дата обращения: 28.04.2020)

34. Самочетова Н.В. Цифровой банкинг как новое направление развития банковского дела [Электронный ресурс] // Междунар. науч.-практ. журнал «Экономика и социум». – №3(34). – Электрон. дан. –2017. – URL: https://www.iupr.ru/ (дата обращения: 29.04.2020).

35. Срибный В.И. Составляющие механизма обеспечения экономической безопасности Российской Федерации / В.И. Срибный // Институт финансово-кредитных отношений в условиях рыночных трансформаций: сборник статей научно-практического семинара (г. Симферополь, 30 ноября 2016 года). – Выпуск 4. – Симферополь: ООО «Антиква», 2017. – С. 409-412.

36. Срибная Е.А., Андронова О.А. Долговая устойчивость как основа обеспеченияэкономической безопасности Российской Федерации / Е.А. Срибная, О.А. Андронова // Институт финансово-кредитных отношений в условиях рыночных

трансформаций: сборник статей научно-практического семинара (г. Симферополь, 30 ноября 2016 года). – Выпуск 4. – Симферополь: ООО «Антиква», 2017. – С. 405-409.

37. Срибный В.И. Составляющие механизма обеспечения экономической безопасности Российской Федерации / В.И. Срибный // Институт финансово-кредитных отношений в условиях рыночных трансформаций: сборник статей научно-практического семинара (г. Симферополь, 30 ноября 2016 года). – Выпуск 4. – Симферополь: ООО «Антиква», 2017. – С. 409-412.

38. Справка о результатах голосования по вопросу (первое чтение) о проекте федерального закона № 608767-7 «О внесении изменений в некоторые законодательные акты Российской Федерации» (в части обеспечения безопасного и устойчивого функционирования сети Интернет на территории Российской Федерации). – Государственная Дума. / Официальный сайт. – Электрон. дан. – URL: http://vote.duma.gov.ru/vote/107004 (дата обращения: 12.05.2020).

39. Стратегия Единого цифрового рынка Евросоюза (EU Digital Single Market strategy). 6 May 2015. – URL: https://eur-lex.europa.eu/(Дата обращения: 09.09.2018).

40. Трансформация рынка ипотеки в условиях цифровой экономики // Профессиональное образование, наука и инновации в XXI веке: сб. трудов XII С.-Петерб. конгресса (Санкт-Петербург, 12–30 ноября 2018 г.). – Петербургский государственный университет путей сообщения Императора Александра I. – 229 с.

41. Чумакова Н.А., Адамян Ж.А. Электронный документооборот и электронная отчетность: тенденции развития в бухгалтерском учете // Научный вестник Южного института менеджмента. – 2017. – № 4. –57 с.

42. Экономическая безопасность России: Общий курс: учебник / под ред.В.К. Сенчагова. – М.: Дело, 2015. – 896 с.

43. Южаков В.Н. Направления совершенствования правового регулирования в сфере стимулирования развития информационных технологий / В.Н. Южаков, А.А. Ефремов // Право и информационные технологии. – 2017. – №5. – 356 с.

44. National Cyber Strategy of the United States of America (September 2018). – URL: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-CyberStrategy.pdf (Дата обращения: 09.05.2020)

45. Kolmykov A.U., Vasilyev, N.P. Two-and threedimensional algoritms for hashing and pseudo random number generation targeted to CUDA implementation // International Journal of Applied Engineering Research. - 2016. - Vol. 11. - Iss. 9. - p. 6840-6845.

46. International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World. –URL: ttp://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (Дата обращения: 09.05.2020)

47. Jack L. Goldsmith & Eric A. Posner, The Limits of International Law 225-26 (2005). Анализ работы Jack L.Goldsmith & Eric A. Posner, The Limits of InternationalLaw (2005) см Paul Schiff Berman «Seeing Beyond the Limits of International Law» – URL: http://www.papers.ssrn.com/sol3 (Дата обращения: 09.09.2018);

48. Regulation of Investigatory Powers Act 2000 [Электронный ресурс]: The official home of UK legislation. URL: http://www.legislation.gov.uk/ukpga/2000/23/pdfs/ukpga_20000023_en.pdf (дата обращения: 01.05.2020).

49. Campaigners hit by decryption law [Электронный ресурс]: BBC News. URL: http://news.bbc.co.uk/2/hi/technology/7102180.stm (дата обращения: 01.05.2020).

50. Enerchain: A Decentralized Market on the Blockchain for Energy Wholesalers [Электронный ресурс]. – URL: https://spectrum.ieee.org/energywise/energy/thesmarter-grid/enerchain-a-decentralized-market-onthe-blockchain-for-energy-wholesalers (дата обращения 13.05.20).

51. Blockchains Will Allow Rooftop Solar Energy Trading for Fun and Profit [Электронный ресурс]. –URL: https://spectrum.ieee.org/computing/networks/blockc hains-will-allow-rooftop-solar-energy-trading-forfun-and-profit (дата обращения 13.05.20).

АНТИПЛАГИАТ
ТВОРИТЕ СОБСТВЕННЫМ УМОМ

Отчет о проверке на заимствования №1

Федоров Евгений Олегович fedorovTEO@gmail.com / ID: 7004560
Проверяющий: Федоров Евгений Олегович (fedorovTEO@gmail.com / ID: 7004560)

Отчет предоставлен сервисом «Антиплагиат» - https://users.antiplagiat.ru

ИНФОРМАЦИЯ О ДОКУМЕНТЕ

№ документа: 30126
Начало загрузки: 14.06.2020 22:19:55
Длительность загрузки: 00:00:29
Имя исходного файла: ВЛИЯНИЕ ЦИФРОВОЙ ЭКОНОМИКИ НА ОБЕСПЕЧЕНИЕ НАЦИОНАЛЬНОЙ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ Федоров ЕО.doc

Название документа: ВЛИЯНИЕ ЦИФРОВОЙ ЭКОНОМИКИ НА ОБЕСПЕЧЕНИЕ НАЦИОНАЛЬНОЙ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ Федоров ЕО.doc
Размер текста: 1 кБ
Символов в тексте: 145743
Слов в тексте: 17241
Число предложений: 1058

ИНФОРМАЦИЯ ОБ ОТЧЕТЕ

Последний готовый отчет (ред.)
Начало проверки: 14.06.2020 22:20:24
Длительность проверки: 00:00:08
Комментарии: не указано

Модули поиска: Цитирование, Модуль поиска Интернет

ЗАИМСТВОВАНИЯ	САМОЦИТИРОВАНИЯ	ЦИТИРОВАНИЯ	ОРИГИНАЛЬНОСТЬ
15.66%	0%	0.7%	83.64%

Заимствования — доля всех найденных текстовых пересечений, за исключением тех, которые система отнесла к цитированиям, по отношению к общему объему документа. Самоцитирования — доля фрагментов текста проверяемого документа, совпадающий или почти совпадающий с фрагментом текста источника, автором или соавтором которого является автор проверяемого документа, по отношению к общему объему документа.
Цитирования — доля текстовых пересечений, которые не являются авторскими, но система посчитала их использование корректным, по отношению к общему объему документа. Сюда относятся оформленные по ГОСТу цитаты; общеупотребительные выражения; фрагменты текста, найденные в источниках из коллекций нормативно-правовой документации. Текстовое пересечение — фрагмент текста проверяемого документа, совпадающий или почти совпадающий с фрагментом текста источника.
Источник — документ, проиндексированный в системе и содержащийся в модуле поиска, по которому проводится проверка.
Оригинальность — доля фрагментов текста проверяемого документа, не обнаруженных ни в одном источнике, по которым шла проверка, по отношению к общему объему документа.
Заимствования, самоцитирования, цитирования и оригинальность являются отдельными показателями и в сумме дают 100%, что соответствует всему тексту проверяемого документа. Обращаем Ваше внимание, что система находит текстовые пересечения проверяемого документа с проиндексированными в системе текстовыми источниками. При этом система является вспомогательным инструментом, определение корректности и правомерности заимствований или цитирований, а также авторства текстовых фрагментов проверяемого документа остается в компетенции проверяющего.

№	Доля в отчете	Источник	Ссылка	Актуален на	Модуль поиска
[01]	4.21%	http://naukaip.ru/wp-content/uploads/2018/01/%D0%9C%D0%9A-261-%D0%A7%D0%B...	http://naukaip.ru	26 Мар 2018	Модуль поиска Интернет
[02]	0.74%	https://naukaip.ru/wp-content/uploads/2018/12/%D0%9C%D0%9A-452-%D0%A7%D0%...	https://naukaip.ru	09 Янв 2019	Модуль поиска Интернет
[03]	0%	https://naukaip.ru/wp-content/uploads/2018/12/%D0%9C%D0%9A-452-%D0%A7%D0%...	https://naukaip.ru	26 Апр 2020	Модуль поиска Интернет
[04]	1.09%	Скачать	http://psu.ru	22 Янв 2020	Модуль поиска Интернет
[05]	1.4%	https://narfu.ru/upload/medialibrary/870/SBORNIK-1-nauchnoy-konf-ekonomika-upr-p...	https://narfu.ru	15 Сен 2018	Модуль поиска Интернет
[06]	1.08%	Сборник материалов конференции - часть II (2/2)	http://isiedo.ru	03 Сен 2019	Модуль поиска Интернет
[07]	0.12%	не указано	http://isef-kursk.ru	26 Дек 2018	Модуль поиска Интернет
[08]	0%	не указано	http://isef-kursk.ru	23 Мая 2019	Модуль поиска Интернет
[09]	0%	не указано	http://isef-kursk.ru	19 Июн 2019	Модуль поиска Интернет
[10]	0.81%	Новости в области развития малого предпринимательства: статистика, адреса стру...	https://rosmsp.ru	12 Ноя 2018	Модуль поиска Интернет
[11]	1.05%	Прокофьев С.Е. Новации в сфере государственного финансового контроля, осущес...	http://fa.ru	11 Ноя 2016	Модуль поиска Интернет
[12]	0.25%	https://guu.ru/wp-content/uploads/forum_bl_v33.pdf	https://guu.ru	20 Июн 2019	Модуль поиска Интернет
[13]	0.75%	ПРЕДОСТАВЛЕНИЕ ГОСУДАРСТВЕННЫХ УСЛУГ В ЭЛЕКТРОННОМ ВИДЕ: ПРОБЛЕМЫ...	https://sibac.info	09 Мая 2019	Модуль поиска Интернет
[14]	0.02%	О Стратегии развития информационного общества в Российской Федерации на 20...	http://docs.cntd.ru	19 Июн 2019	Модуль поиска Интернет
[15]	0.89%	текст	http://ngonb.ru	11 Мар 2018	Модуль поиска Интернет