УДК 332.146.2(571.51)

# ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЦИФРОВЫХ ТЕХНОЛОГИЙ В СИСТЕМЕ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ (НА ПРИМЕРЕ ВЕДОМСТВЕННОГО ЦЕНТРА ГОССОПКА КРАСНОЯРСКОГО КРАЯ)

**Рукосуев А.О., Аврамчикова Н.Т.**

*Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева, Красноярск, e-mail: avr-777@yandex.ru*

Реализация программы «Цифровая экономика Российской Федерации» имеет важное значение для развития каждого региона и успешного будущего всей страны. Цифровая экономика представляет собой хозяйственную деятельность, основанную на цифровых технологиях. При этом субъекты хозяйственной деятельности осуществляют свою операционную деятельность через Интернет. Масштабы цифровизации всех сфер общественной жизни, а также те возможности, которые несут за собой информация, знания и новые технологии, обуславливают необходимость применения цифровых технологий в системе государственного управления. В этой связи в рамках данного национального проекта необходимо реализовать программу по внедрению и освоению цифровых технологий в государственном управлении. Неотъемлемой частью данной программы является информационная безопасность, которая гарантирует информационную защиту интересов государства, бизнеса и отдельной личности. В статье отмечено, что при применении цифровых технологий в сфере государственного управления существует проблема информационной защищенности пользователей информации от информационных угроз при формировании механизмов информационного сотрудничества власти и бизнеса. Рассмотрены методы и формы организации информационной безопасности при осуществлении взаимодействия государства и предприятиями IT-отрасли на примере ведомственного центра ГосСОПКА в Красноярском крае и ее влияние на информационное будущее края и страны целом в рамках реализации программы «Цифровое государственное управление» как составляющей национального проекта «Цифровая экономика Российской Федерации». Применение программы приведет к улучшению функционирования органов государственной власти в регионах. В частности, построение ведомственного центра ГосСОПКА позволит предотвратить доступ к цифровым базам данных для недопущения их использования в целях модифицирования, копирования, распространения, блокирования или иных неправомерных действий.

**Ключевые слова: цифровая экономика, цифровые технологии в государственном управлении, национальная программа «Цифровая экономика РФ», IT-отрасль, информационная безопасность**

# INFORMATION SECURITY ENSURING DIGITAL TECHNOLOGY IN THE PUBLIC ADMINISTRATION (FOR EXAMPLE, A DEPARTMENTAL CENTRE GOSCOPE KRASNOYARSK REGION)

**Rukosuev A.O., Avramchikov V.M.**

*Reshetnev Siberian State University of Science and Technology, Krasnoyarsk, e-mail: avr-777@yandex.ru*

The implementation of the Digital economy of the Russian Federation program is important for the development of each region and the successful future of the entire country. The digital economy is a business activity based on digital technologies. At the same time, business entities carry out their operational activities via the Internet. The scale of digitalization of all spheres of public life, as well as the opportunities that information, knowledge and new technologies bring, make it necessary to apply digital technologies in the public administration system. In this regard, within the framework of this national project, it is necessary to implement a program for the introduction and development of digital technologies in public administration. An integral part of this program is information security, which guarantees information protection of the interests of the state, business and the individual. The article notes that when using digital technologies in the field of public administration, there is a problem of information security of information users from information threats in the formation of mechanisms for information cooperation between government and business. The methods and forms of organization of information security when implementing the interaction between the state and the enterprises of IT-industry on the example of departmental centre Goscopy in the Krasnoyarsk region and its impact on information future of the region and the whole country in the framework of the program «Digital public administration» as a component of the national project «Digital economy of the Russian Federation». The application of the program will lead to an improvement in the functioning of state authorities in the regions. In particular, the construction of the gossopka departmental center will prevent access to digital databases to prevent their use for modification, copying, distribution, blocking or other illegal actions.

**Keywords: digital economy, digital technologies in public administration, national program «Digital economy of the Russian Federation», business model in the IT industry, information security**

Цифровая экономика – это экономика, не имеющая жестких территориальных границ, что априори означает ее мировой масштаб [1]. В российских условиях обширности пространства применение цифровых технологий имеет особую значимость для отдаленных и труднодоступных регионов, обеспечивая связность территории [2]. Цифровая экономика качественно преображает экономическую деятельность

и образ жизни человека и формирует новые отношения в цифровом мире. При этом цифровые технологии обуславливают обеспечение информационной безопасности и акцентируют внимание на доверии между участниками трансакций. В реализации информационно-коммуникационных технологий формируются принципиально новые бизнес-модели, основанные на облачных технологиях, искусственном интеллекте и новой виртуальной реальности. Имеет место накапливание значительных объемов информационных данных (Big Data), которые являются важным капиталом нового «цифрового» качества.

На современном этапе развития экономики актуальным и востребованным является применение цифровых технологий как в организации бизнес-моделей в IT-отрасли, несущих практическую значимость для реализации задач региональной информатизации, так и в цифровизации функций и полномочий органов государственного управления по оказанию государственных и муниципальных услуг субъектам хозяйствования, реализующим IT-технологии. Однако при применении цифровых технологий в сфере государственного управления существует проблема информационной защищенности пользователей информации от информационных угроз при формировании механизмов информационного сотрудничества власти и бизнеса.

Цель исследования заключается в изучении применения цифровых технологий в государственном управлении при взаимодействии государства и предприятий IT-отрасли, несущих практическую значимость для реализации задач региональной информатизации и обеспечения их информационной безопасности, на примере построения ведомственного центра ГосСОПКА в Красноярском крае.

В соответствии с поставленной целью основными задачами определены теоретическое обоснование и разработка концептуального подхода к формированию основ применения цифровых технологий в государственном управлении применительно в региональной системе с учетом особенностей ее социально-экономического развития и обеспечение информационной безопасности и защищенности субъектов информационной среды, реализующих информационно-коммуникационные технологии.

*Теоретические основы цифровой экономики*

Применение термина «цифровая экономика» впервые было использовано в 1955 г. в научном труде Д. Тапскотта «Цифровая экономика: обещание и опасность в эпоху сетевого интеллекта». В данном исследовании впервые была предпринята попытка обоснования ведения бизнеса с помощью интернет-технологий. В современном мире подавляющее большинство населения планеты подключены к мобильным сетям, что оказывает существенное влияние на сферу предпринимательства и социальные коммуникации [3]. Массовое распространение и использование сетевых технологий обусловлено развитием цифровой экономики, позволяющей создавать и реализовывать цифровые технологии, генерировать новые и трансформировать имеющиеся производственные и коммуникационные технологии. На сегодняшний день в мире понятие «цифровая экономика» трактуется неоднозначно. В Указе Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» дано научно-практическое определение данному феномену: «Цифровая экономика – хозяйственная деятельность, в которой ключевым фактором производства являются данные в цифровом виде. Обработка больших объемов и использование результатов анализа по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг» [4]. Из данного определения следует, что цифровая экономика – это процессная деятельность, реализующая цифровые интернет-технологии по предоставлению онлайн-услуг в сфере финансов, торговле и других сферах, а также позволяющая наиболее успешно реализовать краудфандинговые технологии.

Бизнес-процессы значительно ускоряются при исключении промежуточных этапов передачи данных, а также унификации всей информационной среды, что возможно при объектно ориентированном подходе. Данный подход основан на введении в описание объектов их иерархии и отношений наследования между свойствами объектов разных иерархических уровней и используется при разработке информационных систем и программного обеспечения.

Цифровая экономика основана на информационно-коммуникационных технологиях, при этом субъекты хозяйственной деятельности осуществляют свою операционную деятельность дистанционно через Интернет. Соответственно компания будет называться цифровой, если она реализует свою деятельность в формате онлайн.

Формируют цифровую экономику предприятия, у которых в рамках цифровых

технологий реализуется функциональная деятельность в сфере предоставления услуг или доставки товаров, управления, логистики, контроля и анализа бизнеса, маркетинга и др. [5].

Концепция национального проекта «Цифровая экономика Российской Федерации» и его основные положения обеспечивают развитие цифровой экономики в период до 2024 г. по следующим направлениям:

1. Внедрение цифровых технологий и платформенных решений в сферу государственного управления и оказания государственных услуг, в том числе в интересах населения и субъектов хозяйственной деятельности.

2. Разработка и внедрение национального механизма осуществления согласованной политики государств – членов Евразийского экономического союза при реализации планов в области развития цифровой экономики.

В национальном проекте «Цифровая экономика Российской Федерации» определены приоритеты развития «сквозных» цифровых технологий (СЦТ-технологий), которые применяются для поиска, сбора, обработки, хранения, передачи и представления данных в электронном виде. Функционирование данных технологий основано на аппаратных и программных средствах и системах, которые изменяют бизнес-процессы, создают новые рынки, востребованные во всех секторах экономики [6].

На современном этапе органы государственного и муниципального управления оказывают государственные услуги населению, используя возможности цифровых технологий, позволяющих гражданам получить доступ к получению государственных услуг дистанционно. Наиболее распространенными являются услуги в сфере юридического электронного документооборота, оформления квалифицированной цифровой подписи, услуги, оказываемые населению в сложных жизненных ситуациях, и ряд других. Широко развит также межведомственный электронный документооборот между уровнями государственного управления. Цифровизация государственного управления позволяет значительно сократить время на предоставление государственных услуг и повысить их качество. В 2019 г. около 70 процентов населения взаимодействовали с государством через электронные услуги, что значительно выше уровня 2018 г. [7]. В этой связи особенно актуальной становится проблема обеспечения информационной безопасности дистанционного взаимодействия власти и бизнеса. Теоретические основы обеспечения информационной безопасности базируются на теоретических исследованиях в сфере цифровой экономики в социально-экономических процессах, в том числе в сфере государственного управления. При этом особое внимание уделяется информационной безопасности как составляющей программы «Цифровое государственное управление», которая гарантирует информационную защиту интересов государства, бизнеса и отдельной личности. При реализации данной программы выделены методы и формы организации информационной безопасности бизнес-процессов на примере ведомственного центра ГосСОПКА в Красноярском крае.

### *Обеспечение информационной безопасности цифровых технологий в сфере взаимодействия государства и бизнеса на примере ведомственного центра ГосСОПКА*

Переход к цифровым технологиям органов государственного управления ориентирован на повышение экономической и социальной эффективности организационных структур, внедрение информационно-коммуникационных технологий в деятельность государственных органов и должностных лиц. В настоящее время информационные технологии являются катализатором не только экономического роста, но и развития всех остальных сфер жизни общества. Формирование новых механизмов информационного сотрудничества власти и бизнеса путем реализации сервисов информационного обслуживания будет способствовать развитию новых технологий управления экономикой со стороны органов государственного управления, формированию новых мер институциональной поддержки, упрощению административно-управленческих процедур и, как следствие, улучшению предпринимательского климата.

Создание и распространение интернет-технологий, большого массива данных, развитие искусственного интеллекта и других цифровых технологий привели к модернизации традиционных математических моделей и развитию новых их направлений, обуславливающих необходимость развития цифровых технологий информационной безопасности, которые обеспечивают защищенность пользователей информации от внутренних и внешних информационных угроз. Повсеместное успешное использование информационных технологий обусловлено степенью их информационной безопасности и защищенности объектов и субъектов информационной системы от неправомерных действий пользователей.

Применение цифровых технологий информационной безопасности обеспечивает реализацию конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет и устойчивое социально-экономическое развитие Российской Федерации в условиях цифровой экономики [8].

В Красноярском крае в рамках реализации цифровых технологий в сфере информационной безопасности на базе краевого государственного казенного учреждения «Центр информационных технологий Красноярского края» (далее – КГКУ «ЦИТ») был создан проект «Система безопасности значимых объектов критической информационной инфраструктуры». Целями создания системы являются:

1. Обеспечение информационной безопасности электронного правительства Красноярского края, органов исполнительной власти Красноярского края и их подведомственных организаций.

2. Выявление значимых событий, способных повлиять на безопасность.

3. Адекватная и своевременная реакция по оценке информационных угроз на произошедшие события.

4. Устранение возможности возникновения информационных угроз. Восстановление функционирования информационных ресурсов в штатном режиме (в том числе при возникновении компьютерных атак).

5. Предотвращение повторения инцидентов.

Для создания Системы безопасности значимых объектов критической информационной инфраструктуры (далее – ЗОКИИ) КГКУ «ЦИТ» необходимо последовательное решение следующих задач:

1. Выполнить анализ угроз безопасности информации и разработать требования к обеспечению безопасности ЗОКИИ.

2. Разработать проект системы безопасности ЗОКИИ.

3. Регламентировать правила и процедуры обеспечения безопасности ЗОКИИ.

4. Осуществить построение ведомственного центра ГосСОПКА.

Решение данных задач обеспечит информационную безопасность на основе отечественных разработок по своевременному устранению угроз для критической информационной инфраструктуры.

Для построения ведомственного центра ГосСОПКА предполагается внедрение программных продуктов, обеспечивающих построение системы мониторинга, корреляции событий информационной безопасности в режиме реального времени, осуществления сбора и анализа событий безопасности из различных источников, сопоставления их с существующими правилами и производящих корреляцию событий безопасности из различных источников и конфигураций программно-аппаратных средств. Полученные данные позволяют сделать оценку защищенности с немедленным уведомлением ответственных сотрудников. При оценке защищенности объектов и субъектов информационной системы решаются следующие задачи: обеспечение инвентаризации и анализ конфигураций информационных активов; обнаружение и сбор событий информационной безопасности (ИБ) с элементов информационной системы (ИС); оперативный контроль защищенности элементов ИС; корреляция событий и обнаружение инцидентов ИБ; управление инцидентами ИБ; построение отчетов по результатам работы; обеспечение хранилища исходных и нормализованных событий информационной безопасности.

*Практическая значимость проекта*

Практическая значимость основных положений исследования заключается в возможности организации процесса расследования компьютерных инцидентов. Проект «Система безопасности значимых объектов критической информационной инфраструктуры» – это система управления инцидентами информационной безопасности в государственном секторе. Она автоматизирует процесс реагирования на инциденты и информирует о них Национальный координационный центр по компьютерным инцидентам (далее – НКЦКИ) – главный центр ГосСОПКА. Информация об инцидентах поступает из соответствующего программного продукта и от пользователей информационных систем. ВЦ ГосСОПКА решает следующие задачи: формирование и поддержание в актуальном состоянии сведений об информационных ресурсах КГКУ «ЦИТ»; формирование и поддержание в актуальном состоянии сведений о компьютерных инцидентах; формирование задач по расследованию компьютерных инцидентов; направление информации о компьютерных инцидентах в НКЦКИ; учет информации, направленной в НКЦКИ. Внедрение ВЦ ГосСОПКА позволит организовать процесс расследования компьютерных инцидентов; передавать сведения о расследовании компьютерных инцидентов в НКЦКИ в требуемом формате обмена; принимать из НКЦКИ методические рекомендации и информационные сообщения; проводить учет информации, направленной в НКЦКИ; проводить анализ результатов реагирования

на инциденты с помощью средств отчетности и визуализации.

Технологии информационной безопасности обуславливают применение специализированных систем обмена информации, обеспечивающих возможность взаимодействия участников в дистанционной среде как в автоматизированном режиме, так и в ручном режиме посредством действий оператора. Все взаимодействие ВЦ и главного центра ГосСОПКА в Интернете осуществляется с применением криптографических средств защиты информации. Для осуществления работы удостоверяющего центра должна быть получена лицензия Федеральной службы безопасности России на разработку средств защиты. Для реализации проекта необходима закупка услуг (в том числе по аутсорсингу) и ввод в промышленную эксплуатацию с подключением объектов, не связанных с министерством на основании соглашений. Необходимо также сформировать самостоятельное подразделение в составе профильного министерства правительства Красноярского края, разработать пакет организационной документации и закрепить полномочия в положении о министерстве и уставе организации.

## Заключение

Проведенное исследование позволяет сделать вывод о том, что реализация национального проекта «Цифровая экономика Российской Федерации» в значительной степени зависит от уровня информационной безопасности и защищенности субъектов информационной среды, реализующих информационно-коммуникационные технологии. Применение национальной программы «Цифровое государственное управление» приведет к повышению качества и оперативности предоставляемых государственных услуг и обеспечит их информационную безопасность, в том числе и на региональном уровне. Так, построение ведомственного центра ГосСОПКА в Красноярском крае обеспечит защиту информации от уничтожения, модифицирования, блокирования, копирования, предоставления и распространения, компьютерных атак, а также иных неправомерных действий пользователей.

Развитие и распространение интернет-технологий в социально-экономическом пространстве для реализации национального проекта «Цифровая экономика Российской Федерации» обуславливает повышение роли информационной безопасности и конфиденциальности баз данных субъектов интернет-взаимодействий. Это обеспечит дальнейшее поступательное развитие национального рынка в соответствии с мировыми вызовами и повысит конкурентоспособность страны на мировой арене в области внедрения информационных технологий.

## Список литературы

1. Аврамчикова Н.Т., Батукова Л.Р., Чувашова М.Н. Теоретические положения перехода отдаленных и слабозаселенных регионов к информационной экономике // Фундаментальные исследования. 2017. № 9. С. 117–121.

2. Аврамчикова Н.Т., Рожнов И.П., Волков Д.О. Проблемы государственной поддержки инновационного развития предприятий машиностроительного комплекса в ресурсно-ориентированном регионе (на примере Красноярского края) // Фундаментальные исследования. 2019. № 12. С. 9–13.

3. Щепина И.Н., Бородина А.А. Цифровая экономика как одна из моделей развития постиндустриального общества // Вестник ВГУ. Серия: Экономика и управление. 2019. № 2. С. 97–105.

4. Указ Президента Российской Федерации от 09.05.2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы». [Электронный ресурс]. URL: http://www.kremlin.ru/acts/bank/41919 (дата обращения: 05.01.2021).

5. Созыкина М.С. Понятие цифровой экономики в России // Достижения науки и образования. 2018. № 18 (40). С. 2–3.

6. Сидоренко Э.Л., Барциц И.Н., Хисамова З.И. Эффективность цифрового государственного управления: теоретические и прикладные аспекты // Вопросы государственного и муниципального управления. 2019. № 2. С. 93–111.

7. Абдрахманова Г.И., Вишневский К.О., Гохберг Л.М. и др., Что такое цифровая экономика? Тренды, компетенции, измерение. М.: Изд. дом Высшей школы экономики, 2019. 85 с.

8. Указ Президента Российской Федерации от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». [Электронный ресурс]. URL: http://www.kremlin.ru/acts/bank/41460 (дата обращения: 05.01.2021).