Министерство науки и высшего образования Российской Федерации

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«БАШКИРСКАЯ АКАДЕМИЯ ГОСУДАРСТВЕННОЙ СЛУЖБЫ И
УПРАВЛЕНИЯ ПРИ ГЛАВЕ РЕСПУБЛИКИ БАШКОРТОСТАН»

Кафедра государственного и муниципального управления

Я.В. Ободец, Ф.З. Забихуллин

Цифровое государственное управление

УЧЕБНОЕ ПОСОБИЕ

Уфа 2025

УДК 35(075.8)
ББК 66.33.141я73
Ц75

Рецензенты:

Филиппова Анна Сергеевна, доктор технических наук, профессор, профессор кафедры «Информационные технологии» ГБОУ ВО «Башкирский государственный педагогический университет им. М.Акмуллы»

Тисунова Виктория Николаевна, доктор экономических наук, профессор, заведующая кафедрой менеджмента и экономической безопасности ФГБОУ ВО «Луганский государственный университет имени Владимира Даля»

Ободец, Яна Викторовна **Цифровое государственное управление: учебное пособие** / Я.В. Ободец, Ф.З. Забихуллин**. –** ГБОУ ВО «БАГСУ», 2025. – 147 с.

В учебном пособии рассматриваются основные теоретические положения развития цифрового государственного управления, а также определены его стратегические ориентиры развития.

Рассмотрены практические аспекты цифровой трансформации государственного управления, в частности цифровые платформы и экосистемы, изучена практика применения искусственного интеллекта в государственном управлении, а также представлены инструменты цифрового маркетинга и аналитики в государственном управлении.

Данное учебное пособие может быть использовано студентами, магистрантами, аспирантами, а также в качестве дополнительной литературы.

Рекомендовано учебно-методическим советом ГБОУ ВО «БАГСУ» в качестве учебного пособия для обучающихся по направлениям подготовки 38.03.04 и 38.04.04. Государственное и муниципальное управление

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В современном мире цифровизация охватывает все сферы жизни, включая государственное управление. Переход к цифровым технологиям становится не просто трендом, а необходимостью для повышения эффективности, прозрачности и доступности государственных услуг. В условиях глобальных вызовов, таких как пандемия, экономические кризисы и изменения в общественных потребностях, цифровое государственное управление играет ключевую роль в обеспечении устойчивости и адаптивности государственных институтов.

Настоящее учебное пособие посвящено изучению цифрового государственного управления и состоит из двух глав, каждая из которых освещает важные аспекты этой темы. Первая глава «Теоретические основы развития цифрового государственного управления» рассматривает ключевые концепции, модели и подходы, лежащие в основе цифровизации государственного управления. Рассмотрены основные стратегические ориентиры развития цифрового государственного управления, а также представлена роль информационной безопасности в государственном управлении.

Вторая глава «Практические аспекты цифровой трансформации государственного управления» сосредоточена на развитии цифровых платформ и экосистем, а также представлена роль клиентоцентричности в развитии цифровых технологий. Рассмотрены инструменты и практики внедрения технологий искусственного интеллекта в государственном управлении, а также технологии цифрового маркетинга и аналитики, которые используются для оптимизации процессов, повышения качества обслуживания граждан и улучшения взаимодействия между государственными органами и обществом.

После каждой главы представлены задания для самостоятельного выполнения, а также ситуационные задачи, которые направлены на закрепление полученных знаний и разработку практических навыков.

Данное пособие предназначено для студентов, преподавателей, исследователей и практиков в области государственного управления, а также всех заинтересованных в вопросах цифровизации и её влияния на современное общество.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ РАЗВИТИЯ ЦИФРОВОГО ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

1.1. Цифровое государство: понятия, принципы, механизмы реализации

Усложнение экономических, социальных, политических, демографических и иных процессов требует как новых подходов к государственному управлению, так и новых методов и технологий анализа и обработки информации, формирования стратегического видения и определения приоритетов.

На смену электронному правительству в рамках парадигмы открытого государственного управления приходят технологии цифрового правительства, призванного преодолеть недостатки поверхностной информатизации государства и перейти к управлению на основе данных. Общий вектор трансформации государственного управления в Российской Федерации соответствует мировому тренду и направлен на построение цифрового государства, способствующего поддержанию социально–политической стабильности и развитию цифровой экономики России.

Цифровизация – это процесс внедрения современных цифровых технологий в некоторую отрасль хозяйства (цифровизация экономики) либо сферу жизнедеятельности (цифровизация публичного управления), характеризующийся замещением разрозненных информационных систем интеграционными цифровыми платформами [61].

Как отмечено в работе [61] «…Предпосылки для цифровизации и управления создаются, прежде всего, за счет бурного развития информационных технологий и их трансформации в цифровые технологии. Это способствует многократному увеличению скорости и повышению точности обработки данных. В результате снижается трудоемкость решения рутинных задач…». Сегодня понятие цифровизации относится к разным секторам

экономики и сферам жизнедеятельности. Нельзя забывать, что массовое внедрение цифровых технологий требует постоянного совершенствования системы правового обеспечения.

Цифровизация множества отраслей, которые не относятся к информационной среде, но относится к традиционным сферам жизнедеятельности общества и является цифровой трансформацией экономики, управления и общества в целом.

Тогда, цифровую трансформацию следует рассматривать как качественное изменение отношений между субъектами и различными отраслями экономики и сферах жизнедеятельности общества как результат широкого внедрения цифровых технологий.

Существенными признаками цифровой трансформации являются:

1. Влияние цифровых продуктов и услуг на традиционные сферы жизнедеятельности и секторы экономики;

2. Комплексные преобразования процессов управления государством и бизнесом с учетом функционала внедряемых цифровых технологий;

3. Существенное изменение функциональных ролей экономических агентов (производителя, потребителя, посредника);

4. Изменение формы, масштабов и характера конкуренции;

5. Рост потребности в развитии цифровых компетенций специалистов различного профиля, а не только работающих в сфере информационных технологий.

Различия между цифровизацией и цифровой трансформаций состоят в механике этих процессов. Если первым из них управляют люди, принимая соответствующие решения, то второй возникает как закономерная реакция общества на создание его информационной версии.

Цифровизация предполагает улучшение существующих процессов путем внедрения информационных технологий, таких как реинжиниринг процессов, использование данных для принятия решений, сокращение производственных

издержек. Цифровая трансформация запускает новые процессы и позволяет получать новые продукты.

Цифровизация, как отмечено в работе [61], относится к отдельной сфере жизнедеятельности, а цифровая трансформация – ко всей социально–экономической и политической системе. Если цифровизация добавляет в жизнь человека альтернативные, более быстрые и рациональные способы удовлетворения его потребностей, то цифровая трансформация коренным образом меняет структуру потребностей и подходы к их удовлетворению.

Цифровизация улучшает качество государственного управления и доступность предоставляемых населению государственных услуг. Кроме того, цифровизация государственных органов открывает возможности для появления новых видов услуг для населения.

В условиях кризисов, в частности, пандемии COVID–19, экологических, социальных и геополитических рисков, цифровизация повышает возможности государственного сектора по принятию своевременных и обоснованных решений.

Цифровизация повышает прозрачность процесса принятия решений государственными органами, что в свою очередь усиливает подотчетность и целостность госуправления.

Цифровизация государственного управления, в отличии от частного сектора, должна соответствовать ряду ключевых условий:

1. Универсальность государственных услуг. Частный сектор ориентирует или адаптирует свои продукты и услуги под определенные запросы групп населения. В свою очередь, государственные услуги предназначены для использования всеми без исключения гражданами и должны отвечать потребностям всего населения, а также быть удобными в получении.

2. Более широкий набор сфер применения. В отличие от частного сектора, государство предоставляет услуги практически во всех сферах, частично

выступая конкурентом частного сектора, и в то же время является поставщиком услуг в тех отраслях, которые недоступны частным компаниям.

3. Больше критериев оценки успешности цифровизации. В отличие от частных компаний, успешность которых измеряется категориями «издержек–выгод», набор критериев эффективности для госуслуг включает не только удовлетворенность граждан предоставляемыми услугами, доступность этих услуг и т.д., но и соответствие стратегическим целям национального развития, которые, как и предпочтения граждан, могут меняться в зависимости от политической конъюнктуры.

4. Высокие требования к надежности и безопасности. Помимо изначально высоких требований к надежности, качеству, доступности и эффективности предоставление государственных услуг является объектом пристального внимания представительных органов законодательной власти и высших органов аудита.

Кроме того, непосредственный процесс цифровой трансформации органов государственной власти практически всегда сталкивается с рядом наиболее характерных вызовов:

1. Ограниченные бюджеты на цифровую трансформацию, в особенности на критически важные технологии и решения;

2. Строгие правила и процедуры регулирования использования данных препятствуют быстрому внедрению новейших технологий;

3. Основной приоритет в разработке продуктов и технологий – вопросы кибербезопасности, а не удобство пользования и повышение эффективности;

4. Невозможность успешной цифровизации отдельных органов госуправления – для успешного взаимодействия и слаженной работы требуется цифровизация всего госсектора на основе единых или схожих решений и платформ;

5. Выраженный «разрыв поколений» между руководством и сотрудниками органов государственной власти в условиях централизованного

принятия решений в значительной степени препятствует быстрой цифровизации госуправления.

Цифровая трансформация государственных органов требует предварительной просветительской и технологической работы по развитию восприимчивого внутреннего рынка и сокращению «цифровых разрывов» (digital divides).

В результате реализация ключевых компонентов цифровой трансформации госструктур сильно зависит от политической воли руководства, выраженной в национальных стратегических и программных документах.

Цифровизация государственного управления является одним из наиболее актуальных и важных направлений развития в современном мире. Она позволяет упростить и улучшить процессы взаимодействия государства и граждан, повысить эффективность работы органов власти, обеспечить более прозрачное и открытое управление.

Цифровизация государственного управления – это процесс применения информационно–коммуникационных технологий для повышения эффективности и прозрачности государственной деятельности. В последние годы этот процесс приобретает все большее значение, поскольку многие страны признают необходимость использования современных технологий в государственном секторе [16].

По мнению Шашковой Н.И. «…Цифровое государственное управление можно охарактеризовать как концепцию применения информационных и коммуникационных технологий в деятельности государственных органов и учреждений для оптимизации процессов, повышения качества предоставляемых услуг и улучшения взаимодействия с гражданами, бизнесом и другими заинтересованными сторонами. Это целостный подход к управлению, ориентированный на использование современных цифровых технологий для достижения эффективности и прозрачности в работе государственных структур [64].

Цифровое государственное управление играет огромную роль в развитии страны, которая заключается в:

1. Повышение эффективности работы государственных органов. Цифровые технологии позволяют автоматизировать процессы, ускорить доступ к информации и оптимизировать ресурсы, что способствует повышению эффективности работы государственных органов.

2. Улучшение качества государственных услуг. Цифровое государственное управление делает возможным предоставление государственных услуг онлайн, что упрощает процедуры, уменьшает «бумажный документооборот», сокращает временные затраты для юридических и физических лиц. Это также способствует более прозрачному и доступному взаимодействию между государством и обществом.

3. Прозрачность и открытость. Благодаря цифровым технологиям обеспечивается более открытое и прозрачное управление, предоставляется доступ гражданам к информации о деятельности государственных органов, расходах бюджета и принимаемых решениях. Это помогает предотвращать коррупцию, улучшает контроль за деятельностью государственных структур и способствует укреплению доверия между правительством и населением.

4. Активизация процесса вовлечения граждан. Цифровое государственное управление способствует расширению участия граждан в процессах принятия решений через электронные платформы для обратной связи, голосования, общественных обсуждений и участия в онлайн–консультациях.

5. Использование данных для принятия решений. Цифровое государственное управление предоставляет возможность сбора, хранения и анализа больших объемов данных для выявления тенденций и принятия обоснованных решений на основе фактов и статистики.

6. Кризисное управление. В условиях кризисных ситуаций, таких как природные катастрофы, пандемии или террористические угрозы, цифровое

государственное управление может обеспечить более оперативное реагирование и координацию действий.

7. Сокращение расходов на обслуживание государственного аппарата и успешное внедрение проектов на национальном уровне при минимизации затрат на их имплементацию [64].

Цифровое государство обладает рядом преимуществ:

1. Улучшение эффективности и прозрачности государственного управления; цифровые технологии позволяют автоматизировать и ускорить процессы государственного управления (упростить выдачу различных разрешений и лицензий, а также повысить прозрачность в принятии решений);

2. Удобство для граждан (цифровые государственные сервисы позволяют гражданам получать и отправлять различные документы и заявления онлайн, что экономит время и упрощает взаимодействие с государственными органами);

3. Сокращение бюрократии (автоматизированные системы позволяют упростить множество административных процедур и уменьшить бумажную работу, что снижает количество бюрократических процессов и улучшает их эффективность);

4. Улучшение качества предоставляемых государством услуг (цифровизация государственных услуг позволяет повысить их доступность и качество, ускорить процессы обработки заявлений и запросов, а также снизить вероятность ошибок) [17];

5. Усиление кибербезопасности (цифровое государство должно уделять особое внимание кибербезопасности, что позволяет снизить риски хакерских атак и защитить государственную информацию и персональные данные граждан);

6. Сокращение затрат (цифровые технологии могут помочь снизить затраты на бумажные документы, печать, хранение и передачу информации, что может привести к экономическим выгодам для государства);

7. Развитие инноваций и технологического сектора (цифровое государство способствует развитию технологического сектора и стимулирует инновации, что, в свою очередь, создает новые рабочие места и способствует социально–экономическому развитию страны) и другие.

Одним из основных принципов цифровизации государственного управления является построение единого электронного правительства, то есть все административные органы должны быть связаны через Интернет и иметь доступ к единой базе данных. Такой подход позволяет оперативно передавать информацию между различными ведомствами, минимизируя время на выполнение процедур и повышая качество предоставляемых гражданам услуг.

Еще один важный принцип – централизация данных. Цифровая платформа должна обеспечивать хранение и обработку информации в едином формате. Это позволит избежать дублирования данных, упростить доступ к информации и снизить вероятность ошибок. Централизованная система также позволяет отслеживать изменения в законодательстве и быстро адаптироваться к новым требованиям [26].

Преимущества цифровизации государственного управления ощущаются и на уровне граждан. Онлайновые сервисы и порталы позволяют им получать доступ к информации и услугам без необходимости посещать государственные учреждения. Граждане могут платить налоги, получать справки или подавать заявления в режиме онлайн в любое время суток и из любой точки мира. Это экономит время и силы всех заинтересованных сторон.

Еще одним преимуществом цифровизации является повышение открытости и прозрачности работы правительства. С помощью цифровых систем легче отслеживать процессы принятия решений, проверять коррупционные схемы, контролировать расходование бюджетных средств. Это также способствует укреплению доверия граждан к государственным институтам и повышению эффективности всей системы.

Следует отметить, что цифровизация государственного управления имеет свои сложности и вызывает определенные опасения, однако при соблюдении и правильной реализации основных принципов можно значительно улучшить процессы внутри управления, повысить удобство граждан и обеспечить прозрачное функционирование государства в целом [65].

Таким образом, основными принципами цифровизации государственного управления являются создание единого электронного правительства, централизация данных и повышение открытости работы административных органов. Выгоды от этих изменений видны на всех уровнях – от повышения эффективности до улучшения качества обслуживания граждан. Однако необходимо помнить о трудностях, которые могут возникнуть при реализации этого процесса, и работать над их преодолением.

Одним из основных инструментов цифровизации государственного управления является электронное правительство (e–government) – концепция, основанная на использовании интернет–технологий для обеспечения доступа к информации о деятельности государства и предоставления гражданам, бизнесу и другим заинтересованным сторонам различных онлайн–сервисов. С помощью электронного правительства можно проводить онлайн–голосование, подавать заявления и документы в органы власти, получать информацию о процессах законотворчества и принятия решений [27].

Другим важным инструментом цифровизации является автоматизация бизнес–процессов (АБП). Она позволяет автоматизировать рутинные операции и задачи, сокращая время на их выполнение и снижая вероятность ошибок. BPA позволяет создавать электронные рабочие процессы, которые автоматически распределяют задания между исполнителями, контролируют их выполнение и предоставляют отчеты о проделанной работе.

Системы электронного документооборота также играют важную роль в оцифровке государственного управления: они позволяют перейти от бумажных документов к электронным форматам, что значительно упрощает обработку и

передачу информации. Электронный документооборот обеспечивает сохранность документов, их доступность для различных пользователей и возможность быстрого поиска необходимой информации.

Кроме того, цифровизация государственного управления предполагает использование аналитических инструментов для обработки больших данных (big data). Анализ больших объемов информации позволяет выявлять тенденции и закономерности в работе государственных органов, прогнозировать потребности граждан и бизнеса, принимать обоснованные решения на основе реальных данных.

Кибербезопасность также является важным фактором цифровизации государственного управления. С развитием цифровых технологий возрастает и угроза кибератак и хакерских атак на государственные системы. Правительствам необходимо активно внедрять меры по защите информации, использовать новейшие технологические решения для обнаружения и предотвращения киберугроз, а также обучать сотрудников методам обеспечения кибербезопасности.

Таким образом, важную роль в повышении эффективности работы государственных учреждений играют средства и технологии цифровизации государственного управления, позволяющие автоматизировать процессы, улучшить доступ к информации и услугам, обеспечить безопасность данных. Внедрение этих инструментов требует выработки правильной стратегии развития цифрового правительства и обучения сотрудников использованию новых технологий.

Цифровая трансформация госуправления требует новых подходов, отличающихся от инициатив по созданию электронного правительства.

Приоритетами цифровой трансформации в современных условиях являются: внедрение платформенных решений, использование технологий искусственного интеллекта (ИИ) и блокчейна, повышение цифровой зрелости населения, оказание цифровых услуг на основе инструментов анализа данных.

Цифровое правительство открыто и доступно для участия всех заинтересованных сторон. Цифровые платформы используются не только для информирования, но и для привлечения граждан к процессу принятия решений и преодоления бюрократических барьеров в межведомственном взаимодействии.

Цифровая трансформация государственного управления невозможна без развития соответствующей информационно–коммуникационной или цифровой инфраструктуры. Развитие цифровой инфраструктуры обеспечивает не только функционирование государственных цифровых сервисов, но и непрерывную связь с основными пользователями и потребителями услуг, а также оперативный сбор и анализ необходимых данных. Кроме того, непрерывное совершенствование и развитие цифровой инфраструктуры позволяет своевременно адаптировать систему государственного управления и правительственные сервисы под потребности граждан. Наконец, развитие цифровых сервисов и инфраструктуры повышает прозрачность и подотчетность государственного управления, тем самым способствуя устойчивому развитию государственного управления.

К цифровой инфраструктуре относят:

- физическое оборудование;

- программное обеспечение;

- производственные помещения и здания, где располагается соответствующая инфраструктура;

- информационные сети;

- серверы;

- дата–центры.

Также в рамках цифровой инфраструктуре выделяют:

- традиционную инфраструктуру (включает все вышеперечисленное);

- облачную инфраструктуру (допускает удаленное использование компонентов инфраструктуры).

IT–инфраструктура является одним из основных компонентов затрат на цифровизацию госуправления.

Помимо тренда на рост расходов на цифровую инфраструктуру в целом наблюдается рост инвестиций правительств в облачные сервисы. Это вызвано в том числе общим ростом числа и популярности облачных сервисов, а также возможностью оптимизации расходов по сравнению с традиционным подходом к цифровой инфраструктуре (рисунок 1).

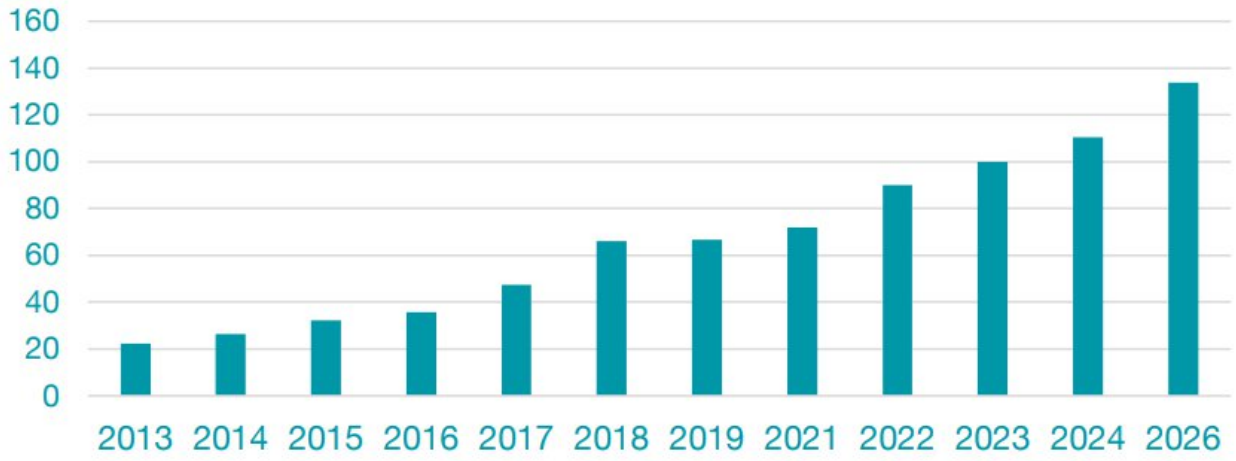

Рисунок 1 – Мировые расходы на облачную IT–инфраструктуру в млрд долл. США [15]

В России активно ведется работа по переводу государственного управления в цифровой формат, и примеры таких проектов наглядно демонстрируют преимущества оцифровки. Одним из ярких примеров является Единая система государственных информационных ресурсов (ЕСГИР), которая была создана для обеспечения единого доступа к информационным ресурсам всех федеральных органов исполнительной власти.

Благодаря ЕСГИР сократилось время поиска и получения нужной информации. Граждане могут пользоваться различными услугами в электронном виде, не посещая государственные учреждения. Например, подать заявление на получение паспорта или водительского удостоверения можно

через портал Госуслуг. Это позволяет гражданам сэкономить значительное количество времени и сил.

Другим положительным примером цифровизации государственного управления является использование облачных технологий для хранения данных. Такой подход позволяет снизить затраты на инфраструктуру и обеспечить более быстрый и надежный доступ к информации. Например, Министерство финансов Российской Федерации перенесло свои данные в облако и теперь может оперативно предоставлять информацию о бюджете страны [16].

В процессе цифровизации государственного и муниципального управления повсеместно используется системный подход.

Реализация системного подхода позволяет значительно повысить качество стратегического, среднесрочного и текущего планирования, обеспечивая достижение целей национального развития.

Положительным примером реализации такого подхода является цифровое управление национальными проектами в разных отраслях народного хозяйства.

Цифровизация государственного и муниципального управления предполагает использование и других частных подходов.

В соответствии с системным подходом цифровизация государственного и муниципального управления направлена на:

1. Создание единого цифрового пространства на всей территории страны, под которым понимается пространство, интегрирующее:

– цифровые процессы;

– средства цифрового взаимодействия;

– информационные ресурсы;

– совокупность цифровых инфраструктур, на основе норм регулирования, механизмов организации, управления и использования;

2. Оказание государственных и муниципальных услуг населению в цифровой среде на основе цифровых и информационно–коммуникационных технологий;

3. Появление цифровых двойников в деятельности и реализации полномочий государственных органов, государственных гражданских служащих, органов местного самоуправления и муниципальных служащих. «Цифровые двойники» – это виртуальная цифровая модель (структура) существующего в реальности физического объекта или процесса. Модель имеет внутренние процессы, технические характеристики и запланированное поведение реального объекта в условиях взаимодействия рисков и окружающей среды реального государственного и муниципального управления;

4. Возможность подключения к цифровому пространству страны органов власти, коммерческих и некоммерческих организаций;

5. Подключение жителей страны и их объединений к цифровым государственным и муниципальным ресурсам в целях решения вопросов и проблем [60].

В то же время, несмотря на рост расходов на IT–инфраструктуру, именно данная сфера наиболее часто сталкивается с рядом серьезных проблем. В частности, общие проблемы развития цифровой инфраструктуры большинства стран зачастую сводятся к следующим аспектам:

1. Нехватка финансирования (скорость развития и обновления технологий и технологических решений опережает темпы роста расходов на цифровую инфраструктуру);

2. Недостаток квалификации и навыков сотрудников (до 40% организаций госсектора сталкиваются с нехваткой цифровых знаний и навыков у сотрудников);

3. Низкая степень интеграции цифровых систем и платформ внутри и между госорганами;

4. Наличие и необходимость поддержания работы устаревших систем (legacy systems);

5. Низкий уровень доверия граждан (граждане опасаются доверять свои персональные данные госорганам).

Формирование цифрового правительства включает в себя несколько этапов развития от аналогового правительства к технологиям ГосТех. Так, на первом этапе аналоговое правительство выступало в виде закрытой структуры, то есть фокус внимания был сконцентрирован на внутренние процесс. Также государство выступает как единый поставщик услуг, где активно применяются аналоговые системы управления.

Второй эволюционный этап – это переход к электронному правительству. Электронное правительство (E–government) – это использование информационных технологий для автоматизации рабочих процессов, повышения эффективности управления данными, улучшения качества предоставления государственных услуг, развития каналов коммуникаций. В рамках электронного правительства существуют три типа взаимодействия:

- отношения между государственными институтами (G2G);
- отношения по линии «правительство–бизнес» (G2B);
- взаимодействие правительства с гражданами (G2C).

Такой этап характеризуется ориентацией пользователей услуг в зависимости от возможностей государственных органов, частичным внедрением цифровых систем, а также использованием информационно–коммуникационных технологий. При чем следует отметить повышение уровня прозрачности государственного управления, что в свою очередь, повышает уровень доверия граждан.

Так, органы власти ориентированы на онлай–публикации государственной информации, ведение социальных сетей, сайтов организаций и каналов коммуникации с населением. Также органы власти становятся «открытыми» для граждан, то есть предоставляют расширенную информацию о

деятельности госоргана, осуществляют взаимодействие между правительством и гражданами посредством использования загруженных на портал электронных форм. Осуществляется двустороннее интерактивное взаимодействие между правительством и гражданами, постепенное вовлечение граждан в процесс государственного управления при помощи информационных технологий, таких как электронное голосование, заполнение налоговых деклараций, а также заявки на получение лицензий, осуществление финансовых транзакций и др. Следует также отметить координацию процессов не только внутри органа власти, но и в межведомственном взаимодействии. Также граждане имеют возможность полноценного цифрового участия в процессах государственного управления.

Повышение эффективности и прозрачности деятельности государственного сектора стало возможным благодаря внедрению информационных технологий и переводу государственных услуг в электронный формат. Следующий шаг – использовать цифровые технологии для создания более открытых, инклюзивных и сетевых моделей государственного управления, а также формирования культуры принятия решений, основанных на данных.

Третий этап – цифровое правительство. Этот этап развивает концепцию электронного правительства, использует оцифрованные данные для проактивного предоставления социально ориентированных государственных услуг.

Отличительными характеристиками цифрового правительства становятся:

1. Разработка процедур предоставления услуг с учетом цифровизации;

2. Государственные услуги ориентированы на пользователей;

3. Правительство становится цифровой платформой (GaaP);

4. Процесс государственного управления становится еще более открытым;

5. Государственный сектор активно использует данные;

6. Проактивный подход к государственному управлению.

Выделяют шесть основных компонентов цифрового правительства:

1. Цифровая инфраструктура;

2. Цифровая грамотность;

3. Цифровые коммуникации;

4. Активное использование информационных технологий;

5. Нормативное регулирование цифровой среды;

6. Информационная безопасность и цифровые права.

Среди ключевых элементов цифровой архитектуры правительства – единый государственный информационный портал, система совместного управления данными из реестров разных государственных структур; предоставление государственных услуг в формате «одного окна»; открытая база цифровых решений, инновационные системы сбора и анализа данных, обеспечение кибербезопасности и надежной защиты персональной информации.

Согласно методологии Всемирного банка, в качестве критериев оценки эффективности цифровой трансформации выделяют:

1. Время предоставления услуги;

2. Популярность цифровых каналов взаимодействия с государством;

3. Качество перевода государственных услуг в цифровой формат;

4. Количество автоматически обработанных запросов;

5. Уровень цифровой грамотности населения;

6. Сокращение финансовых затрат;

7. Сокращение случаев мошенничества и коррупции.

Приоритетными направлениями повышения цифровой зрелости правительства и государственных органов также являются:

1. Агрегирование и систематизация разрозненных данных в целях повышения эффективности оказания государственных услуг;

2. Создание безопасной и гибкой технологической инфраструктуры;

3. Повышение профессионального потенциала, проведение кадровой политики с акцентом на цифровые компетенции;

4. Взаимодействие с представителями научного и бизнес–сообщества для обмена лучшими практиками в области цифровизации и инноваций;

5. Периодическая оптимизация рабочих процессов, максимальное использование трудового и технологического потенциала;

6. Развитие цифровой экосистемы в соответствии с потребностями пользователей государственных сервисов.

И, четвертый этап – ГосТех (GovTech) – цифровой подход к модернизации государственного сектора, который способен улучшить качество предоставления государственных услуг, упростить взаимодействие с гражданским обществом, повысить эффективность государственного управления. Под понятием ГосТех может подразумеваться целый ряд самых разных направлений деятельности: от формирования «умной» городской среды до применения цифровых инструментов для борьбы с преступностью.

Рисунок 2 – Эволюционный процесс формирования цифрового правительства [51]

На данном этапе государственные услуги, ориентированные на граждан и доступные всем без исключения. Также наблюдается общегосударственный подход к цифровой трансформации, а государственные системы становятся простыми, эффективными и прозрачными.

ГосТех опирается на четыре основных элемента:

1. Внедрение цифровых платформ на основе аналитики больших данных;

2. Развитие общедоступных, клиентоцентричных цифровых сервисов;

3. Прямое мультиканальное взаимодействие государства и граждан;

4. Создание правовых и организационных условий для внедрения инноваций в госсекторе.

В практическом плане ГосТех представляет собой совокупность направлений деятельности, ориентированных на повышение эффективности государственного управления и процессов в четырех основных категориях:

1. Цифровое правительство. Сюда относятся, в частности, платформы для принятия решений, цифровая идентификация, электронное голосование, G2G и G2B–услуги (электронные налоги, банкинг и др.).

2. Умный город: городское планирование, управление отходами, транспортные системы и системы мониторинга, решения по энергосбережению.

3. CrimeTech: системы распознавания личности, решения в области кибербезопасности, электронные суды, цифровые инициативы по противодействию отмыванию денег.

4. Государственное управление: образовательные платформы, системы здравоохранения, решения в области спорта и развлечений, агротехнологии.

ГосТех обладает огромным потенциалом, однако превращение цифровых инициатив в осязаемые, измеримые и последовательные результаты в большинстве стран остается сложной задачей. Движение в сторону ГосТеха требует единого общегосударственного подхода к цифровой трансформации, создания прозрачной системы управления и принятия решений, использования потенциала государственно–частного партнерства для привлечения компетенций, инноваций и инвестиций частного сектора.

Для оценки степени «зрелости» ГосТеха эксперты Всемирного банка разработали «Индекс зрелости GovTech: состояние цифровой трансформации

государственного сектора» (GovTech Maturity Index (GTMI): The State of Public Sector Digital Transformation).

Индекс зрелости GovTech измеряет ключевые аспекты по четырем приоритетным направлениям (на основе показателей, отражающих степень внедрения цифровых технологий в сфере госуслуг, налоговой и бюджетной сферах, в образовании и здравоохранении):

1. «Основные государственные системы» – Core Government Systems Index, CGSI;

2. «Предоставление государственных услуг» – Public Service Delivery Index, PSDI;

3. «Вовлеченность населения» – Digital Citizen Engagement Index, DCEI;

4. «Институциональное обеспечение» – GovTech Enablers Index, GTEI.

Индекс основан на оценке результатов цифровой трансформации в 198 странах мира. Кроме того, доклад включает обзор лучших практик использования цифровых инструментов в государственном секторе.

По результатам исследования, в 43–х странах цифровая трансформация занимает важнейшее место в стратегической повестке государства, а также отмечается успешная реализация многочисленных инновационных проектов. Среди лидеров цифровой трансформации – Австралия, Австрия, Индия, ОАЭ, Республика Корея, Сингапур, Швейцария, ЮАР. При этом в 33 странах наблюдается минимальное внимание к инициативам в сфере ГосТех. Цифровой разрыв наиболее заметен в странах Африки к югу от Сахары и Южной Азии.

Несмотря на увеличение инвестиций в цифровую инфраструктуру и активную разработку государственных программных документов в этой области, цифровая зрелость в большинстве стран остается на недостаточном уровне: 47% стран не имеют стратегий по развитию цифровых навыков среди населения.

Основными барьерами остаются:

1. Отсутствие политической воли государственного руководства и соответствующего нормативного регулирования;

2. Неразвитая цифровая инфраструктура;

3. Низкий уровень цифровой грамотности населения, а также государственных служащих;

4. Неэффективное или недостаточное финансирование.

Следует отметить, что в 2022 году по результатам международного рейтинга Всемирного банка «GovTech Maturity Index» (GTMI) Россия вошла в 10 лидеров [49].

По данным на 2022 год, в рамках индекса зрелости GovTech (GTMI) Россия получила следующие показатели по четырём субиндексам:

1. «Основные государственные системы» (17 показателей) – 0,881 балл.

2. «Предоставление государственных услуг» (9 показателей) – 0,960 баллов.

3. «Вовлечённость населения» (6 показателей) – 0,828 баллов.

4. «Институциональное обеспечение» (16 показателей) – 0,919 баллов.

Лидерами GTMI стали Южная Корея (0,991 балл), Бразилия (0,975 баллов), Саудовская Аравия (0,971 балл) [46].

Флагманским продуктом GovTech в России является Единый портал государственных и муниципальных услуг (Госуслуги). С 2019 года число пользователей портала «Госуслуги» выросло в два раза, достигнув на конец 2023 года более 109 млн человек. Прирост за 2023 год составил 10,2 млн человек. Затраты на IT превысили 540 млрд руб. в сравнении с 280 млрд руб. в 2019 году. Только за 2023 год пользователями было подано 468,3 млн заявлений, на 383,2 млн вопросов ответил чат–бот Макс и на 1,7 млн звонков ответили в кол–центре. В 2023 году россияне получили возможность отправлять официальные обращения в органы власти через портал «Госуслуги». До 2025 года к этой площадке подключатся абсолютно все ведомства [46].

В эпоху цифровой экономики современные регионы сталкиваются с беспрецедентными вызовами, которые требуют новых подходов к управлению. Глобализация, стремительное развитие технологий, климатические изменения и растущие потребности населения создают динамичную и непредсказуемую среду, где традиционные модели управления оказываются неэффективными.

Так, авторами Гарифуллиной А.Ф. и Сизоненко З.Л. обоснованы применение различных моделей управления, на примере Республики Башкортостан [13].

1. Динамичная модель управления, предполагает поиск скрытых или неиспользованных ресурсов, направленных на повышение эффективности. Динамичная модель управления – это и концепция, которая отличается гибкостью, адаптивностью и способностью быстро реагировать на изменения в окружающей среде. При такой модели управления решения принимаются на более низких уровнях иерархии, что позволяет быстрее реагировать на изменения и принимать более информированные решения, важную роль играют команды специалистов, которые работают в тесном сотрудничестве и принимают решения совместно и фокус смещается от процессов на результаты, что позволяет оценить эффективность работы и внести необходимые уточнения.

Такую модель управления Республика Башкортостан больше применяет в «стартапах» где конкуренция высока и изменения происходят быстро, или в IT–компаниях, где технологии развиваются с большой скоростью или в производственных компаниях, где важно быстро реагировать на изменения в спросе и предложении. Динамичная модель управления позволяет быстро реагировать на новые требования и внедрять новые технологии.

2. Трехуровневая модель управления развитием предпринимательской среды республики, включает Министерство предпринимательства и туризма Республики Башкортостан, Ассоциация предпринимателей Республики

Башкортостан, а также Фонд развития и поддержки предпринимательства в Республике Башкортостан как «Центр поддержки предпринимательства».

3. Модель «управления качеством жизни в регионе», разработанная С.А. Айвазяном и М. А. Исакиным. Она основывается на индикативном методе управления, где ключевой инструмент является больше мониторинг интегральных индикаторов качества жизни населения, позволяющий выявлять проблемные области и определять приоритеты для социального развития конкретной территории [52].

4. Модель «управления инновационным развитием региона в контексте цифровой трансформации», фокусируется на координации взаимодействия между хозяйствующими субъектами инновационной сферы и определении зон ответственности органов власти, предполагает реализацию целевой инвестиционно–инновационной программы и выбор стратегии управления инновационным развитием региона [35].

Последние две модели отражают современные тенденции в управлении развитием регионов, так как осуществляют учет взаимосвязи социальных и экономических факторов для достижения устойчивого развития, используют различные индикаторы и мониторинг для принятия взвешенных, информированных решений и применяют новых технологии и цифровые решения в процессе управления развитием региона. Применение этих моделей позволяет создать более эффективную систему управления развитием региона, которая учитывает конкретные нужды населения и способствует достижению устойчивого и процветающего будущего.

Современные регионы, в том числе и Республика Башкортостан, сталкиваются с вызовами, требующими переосмысления традиционных моделей управления [28]. Инновационные подходы, основанные на цифровизации, участии граждан, аналитических инструментах и развитии экосистем, становятся ключевыми для обеспечения устойчивого развития и повышения качества жизни населения.

Учитывая специфику Республики Башкортостан, представляется, что инновационным подходом к системе управления регионом является создание централизованной платформы для предоставления региональных услуг, взаимодействия с гражданами, бизнесом и органами власти. Это повысить и прозрачность информации, и ее доступность, упростит процессы аналитической деятельности, ускорит решение проблем. Применение сквозных технологий в предлагаемом платформенном решении, например, Big Data и ИИ позволят анализировать данные о населении, экономике, инфраструктуре и выявить тенденции, риски, разработают более эффективные управленческие решения. Развитие цифровых навыков у населения, предоставление доступа к региональным онлайн–сервисам и информации, повысит уровень вовлеченности граждан в процессы управления республикой. Создание платформ для сбора предложений и инициатив, использование онлайн–платформ для организации онлайн–голосований, петиций, обращений к органам власти, повысит уровень вовлеченности граждан в процессы управления [53].

Цифровая трансформация управления – это не просто цифровизация процессов, а коренная модернизация управленческой деятельности на основе современных сквозных цифровых технологий. Это предполагает разработку и внедрение новых нормативных правовых, организационно–методических и нормативно–технических документов, специально приспособленных для цифровых решений.

Инновационные подходы в региональном управлении – это не просто использование сквозных цифровых технологий, а комплексный подход к развитию региона, основанный на принципах устойчивости, инклюзивности и участия граждан и населения. Такие подходы к системе управления являются необходимым условием для достижения целей устойчивого развития и создания более эффективной и справедливой системы управления в регионе.

Цифровизация, участие граждан и населения, аналитика и развитие инновационных экосистем – ключевые инструменты для создания более прозрачного, ответственного и устойчивого будущего регионов. Республика Башкортостан входит в состав регионов–участников Ассоциации инновационных регионов России, что увеличивает возможности по применению инновационных методов в системе управления [13].

1.2. Стратегические ориентиры развития цифрового государственного управления

Развитие информационных технологий выступало одной из приоритетных задач российского государства на протяжении последних двух десятков лет.

Еще в 1999 году по инициативе Государственного комитета Российской Федерации по связи и информатизации и Комитета Государственной Думы по информационной политике и связи была разработана Концепция формирования информационного общества в России [25].

В Концепции содержались политические, социально–экономические, культурные и технико–технологические предпосылки и условия перехода и обосновывалась специфика российского пути к информационному обществу. В целях развития информационного общества в 2008 году была принята Стратегия развития информационного общества РФ, а в дальнейшем – Государственная программа РФ «Информационное общество (2011–2020 годы)» и Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы.

Развитие электронного правительства в РФ связано с подписанием Окинавской хартии глобального информационного общества и началом административной реформы (2000–2004). Именно тогда были разработаны и приняты к реализации нормативно–правовые документы, определившие

архитектуру и дальнейшее развитие электронного правительства в РФ, в том числе федеральная целевая программа «Электронная Россия (2002–2010 годы)».

Концепция использования информационных технологий в деятельности федеральных органов государственной власти до 2010 года, Концепция региональной информатизации до 2010 года, Концепция формирования в Российской Федерации электронного правительства до 2010 года, Концепция развития механизмов предоставления государственных и муниципальных услуг в электронном виде.

В 2016 году в РФ начался второй этап развития электронного правительства, когда Минкомсвязь России утвердило Системный проект электронного правительства Российской Федерации [54].

Согласно этому документу, развитие электронного правительства предполагает реализацию принципа «4Л» – чтобы любой гражданин и любое ведомство могли взаимодействовать в любом месте и в любое время.

Предпосылкой современного этапа цифровизации в РФ можно считать принятие в 2017 году Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы, целью которой было заявлено создание условий для формирования в Российской Федерации общества знаний. В стратегии были закреплены основные понятия, связанные с развитием информационных технологий, в том числе понятия цифровой экономики и экосистемы цифровой экономики.

Конкретизация реализации стратегии была отражена в Указе Президента РФ от РФ от 07.05.2018 года № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» [38], где говорится о необходимости разработки ряда национальных проектов, в том числе Национальной программы «Цифровая экономика Российской Федерации», реализация которой должна обеспечить в 2024 году достижение следующих целей:

– «увеличение внутренних затрат на развитие цифровой экономики за счет всех источников (по доле в валовом внутреннем продукте страны) не менее чем в три раза по сравнению с 2017 годом;

– создание устойчивой и безопасной информационно–телекоммуникационной инфраструктуры высокоскоростной передачи, обработки и хранения больших объемов данных, доступной для всех организаций и домохозяйств;

– использование преимущественно отечественного программного обеспечения государственными органами, органами местного самоуправления и организациями».

В рамках реализации указов Президента РФ от 07 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» и от 07 мая 2024 г. № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» [38, 39], в том числе с целью решения задачи по обеспечению ускоренного внедрения цифровых технологий в экономике и социальной сфере, Правительством РФ сформирована национальная программа «Цифровая экономика Российской Федерации», утверждённая протоколом заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 04 июня 2019 г. № 7. Национальная программа завершена 31 декабря 2024 г.

Цель программы – внедрение цифровых технологий в экономике и социальной сфере, создание условий для высокотехнологичного бизнеса, повышение конкурентоспособности страны на глобальном рынке, укрепление национальной безопасности и повышение качества жизни граждан.

В состав национальной программы входит девять федеральных проектов. Восемь из них были включены в состав и реализованы в рамках государственной программы Российской Федерации «Информационное общество» [31].

Федеральные проекты национальной программы завершены в 2024 году.

Рассмотрим их более детально.

1. Федеральный проект «Нормативное регулирование цифровой среды».

Ключевая цель проекта – создание норм права, регламентирующих цифровую экономику, а также внедрение в повседневный обиход цифровых технологий.

Проект «Нормативное регулирование цифровой среды» предусматривает разработку и принятие нормативных правовых актов, направленных на снятие препятствующих развитию цифровой экономики барьеров.

Проект затрагивает законодательство в сфере финансовых технологий, интеллектуальной собственности, телекоммуникаций, судопроизводства, стандартизации и иных областях деятельности.

Планируется также урегулировать сквозные для различных отраслей законодательства вопросы, связанные с идентификацией субъектов правоотношений, электронным документооборотом, сбором, хранением и обработкой данных, в том числе персональных.

Таблица 1. – Хронология реализации федерального проекта «Нормативное регулирование цифровой среды»

№	Год	Результаты
1	2	3
1	2018	Утверждён паспорт федерального проекта «Нормативное регулирование цифровой среды» в составе национальной программы «Цифровая экономика Российской Федерации»
2	2019	1. Установлена возможность формирования основной информации о трудовой деятельности и трудовом стаже каждого работника в электронном виде. 2. Введена возможность использования «облачной» электронной подписи. 3. Установлено оформление ряда госуслуг в электронной форме: внесение записи о предоставлении лицензии в реестр лицензий; установление приоритета электронной регистрации оформления результатов работ (услуг) в области обеспечения единства измерений
3	2020	1. Запущен эксперимент по оформлению в ряде компаний

		трудовых договоров и кадровых документов в электронном виде. 2. Введена возможность выдавать патент на изобретение, полезную модель или промышленный образец в форме электронного документа.

Продолжение таблицы 1

1	2	3
		3. Предусмотрена возможность формирования в электронном виде транспортных накладных и других перевозочных документов. 4. Определены основные подходы к нормативному регулированию создания и применения технологий искусственного интеллекта и робототехники в различных сферах экономики
4	2021	1. Созданы условия для ознакомления с материалами судебных дел в электронном виде, а также для дистанционного участия в судебных заседаниях. 2. Установлены особенности обращения программного обеспечения, являющегося самостоятельным медицинским изделием (SaMD), а также используемого совместно с другими медицинскими изделиями. 3. Определены критерии отнесения программного обеспечения к медицинскому
5	2022	1. Установлен экспериментальный правовой режим в целях реализации инициативы «Персональные медицинские помощники» – проекты–маяки. 2. Подготовлен проект программы экспериментального правового режима для реализации инициативы «Беспилотная аэродоставка грузов»
6	2023	1. Уточнены правила отнесения информации, размещаемой государственными органами и органами местного самоуправления, к общедоступной. 2. Обеспечено подключение комплексной информационной системы адвокатуры России (КИС АР) к Единому порталу государственных и муниципальных услуг (ЕПГУ)
7	2024	1. Усовершенствовано регулирование экспериментальных правовых режимов в сфере цифровых инноваций. 2. Усовершенствован порядок обезличивания персональных данных. 3. Адвокатам предоставлено право проводить свидания с подозреваемыми и обвиняемыми с помощью систем видеоконференцсвязи

2. Федеральный проект «Информационная инфраструктура».

Основной задачей федерального проекта «Информационная инфраструктура» является создание конкурентоспособной, устойчивой и безопасной инфраструктуры высокоскоростной передачи данных, доступной для всех граждан, бизнеса и органов власти. Реализация мероприятий проекта не только обеспечит полномасштабное подключение к сети «Интернет» ключевых социально–значимых объектов инфраструктуры, но и позволит населению пользоваться качественными современными цифровыми услугами даже в самых удаленных уголках нашей страны.

Одним из приоритетных направлений в рамках федерального проекта является создание инфраструктуры для подключения к сети «Интернет» социально значимых организаций на всей территории Российской Федерации, а также эффективного и безопасного использования ими онлайн–сервисов.

В рамках проекта проводится активная работа по подключению государственных (муниципальных) образовательных организаций, центральных избирательных комиссий к Единой сети передачи данных (ЕСПД) в целях обеспечения не только защищенного доступа к государственным и муниципальным информационным системам, но и обеспечения безопасного интернет–пространства.

Вместе с тем, в рамках федерального проекта предусмотрено оснащение учебных классов государственных (муниципальных) образовательных организаций внутренней ИТ–инфраструктурой как для обеспечения безопасного доступа к сети Интернет по технологии Wi–Fi, так и для использования защищенного доступа к государственным и муниципальным информационным системам, что, в свою очередь, является гарантом обеспечения базовой безопасности образовательного процесса.

Также важным мероприятием проекта является оказание универсальных услуг связи в малонаселенных пунктах. Они включают установку точек доступа

беспроводного интернета и организацию сотовой связи в населенных пунктах от 100 до 500 человек.

Всем подключенным населённым пунктам с числом жителей от 100 до 500 человек оказываются услуги связи.

Одновременно с этим в рамках проекта заложены мероприятия, направленные на создание условий для поэтапного внедрения современных стандартов связи 5G/IMT–2020. 5G будет работать на базе отечественного оборудования.

Также федеральным проектом предусмотрено создание космических аппаратов для системы «Экспресс–РВ» в период 2022–2024 гг. Система спутниковой связи и вещания с использованием четырех космических аппаратов обеспечит качественное покрытие услугами связи как стационарных, так и подвижных объектов на всей территории страны, в том числе на территориях Арктической зоны и Дальнего Востока, а также на всей протяженности Северного морского пути.

3. Федеральный проект «Кадры для цифровой экономики».

Минцифры России совместно с Минобрнауки России была проведена работа по подготовке ИТ–специалистов в рамках федерального проекта «Кадры для цифровой экономики» национальной программы «Цифровая экономика Российской Федерации».

В рамках этого федерального проекта предусмотрено два проекта:

1. Приём на бюджетные места по ИТ–специальностям
2. Цифровые профессии

В рамках федерального проекта «Кадры для цифровой экономики» национальной программы «Цифровая экономика Российской Федерации» более 598 тыс. человек принято на обучение по образовательным программам высшего образования в сфере информационных технологий за счёт средств федерального бюджета – нарастающим итогом, начиная с 2019 года.

В 2024 году более 128 тыс. человек принято на бюджетные места по ИТ–специальностям в вузы. Приём на ИТ–специальности составляет около 23% от всего приёма на бюджетные места.

В 2021 году в рамках федерального проекта «Кадры для цифровой экономики» национальной программы «Цифровая экономика Российской Федерации» была запущена программа обучения востребованным ИТ–специальностям со скидкой 50% от государства.

В 2022 году скидка от 50 до 100% на получение ИТ–образования предоставлялась льготным категориям граждан. Среди них – безработные граждане, инвалиды, отцы и матери детей до 3 лет.

Для обучения отобраны курсы ведущих компаний и образовательных организаций в ИТ–сфере, например, «Яндекса», «Нетологии», GeekBrains, Университета Иннополис. По итогам 2022 года среди выпускников проекта самыми популярными курсами стали: «Профессиональный разработчик 1С», «Основы тестирования ПО», «Основы Frontend–разработки», «Инженер по тестированию» и «Аналитик данных».

В 2023 году более 78 тыс. граждан успешно завершили обучение востребованным ИТ–специальностям со скидкой от 50% до 100% от государства за все время реализации проекта.

4. Федеральный проект «Информационная безопасность».

Задачи федерального проекта – повышение уровня защищенности государственных информационных систем и ресурсов и создание условий для снижения количества правонарушений с использованием информационных технологий.

В результате реализации направления «Информационная безопасность» будут обеспечены устойчивость и безопасность информационной инфраструктуры, конкурентоспособность отечественных разработок и технологий информационной безопасности и выстроена эффективная система

защиты прав и законных интересов личности, бизнеса и государства от угроз информационной безопасности.

Основными участниками федерального проекта являются ФСБ, ФСТЭК, ФСО, а также Роскомнадзор.

Среди основных результатов реализации этого федерального проекта можно выделить:

1. Повышение информационной безопасности ГИС. Так, проведена независимая оценка защищённости (пентесты) 100 ГИС, в том числе в 2024 году 63 ГИС, выявлены 879 уязвимостей (с учётом информационных), в том числе 13 критических уязвимостей.

2. Противодействие мошенническим действиям, совершаемым с использованием информационно–коммуникационных технологий. К ИС «Антифишинг» подключено 6 Федеральных органов исполнительной власти, в течение 2022 – 2024 годов заблокировано более 356 тыс. противоправных информационных ресурсов, в том числе в 2024 году – 205,2 тыс. ресурсов.

Количество вызовов, по которым ИС «Антифрод» установила отсутствие информации об инициировании соединения абонентом (подмена номера вызывающего абонента) в течение 2023 – 2024 годов, составило более 1 350 млн вызовов, в том числе в 2024 году – более 600 млн вызовов, к ИС «Антифрод» подключены 1 162 из 1 168 операторов связи (99,5 %).

Разработана концепция Платформы противодействия противоправным деяниям, совершаемым с использованием информационно–коммуникационных технологий, определяющая цели, задачи и порядок создания Платформы.

3. Новые разработки в сфере информационной безопасности. На базе отраслевого центра информационной безопасности цифровой экономики в структуре АНО «Национальный технологический центр цифровой криптографии», проведены 19 НИР и ОКР (в 2024 г. – 10 НИР и ОКР), разработано 8 решений по информационной безопасности для перспективных информационных технологий, в том числе наиболее значимые:

– запущена в опытную эксплуатацию Национальная система «Мультисканер» – принципиально новый общедоступный публичный антивирусный сервис, позволяющий гражданам и компаниям проверять бесплатно файлы на вирусы; проверено 100 тыс. файлов пользователей; проводится пилот с ЕПГУ;

– разработан программно–аппаратный комплекс по обезличиванию персональных данных, реализующий 6 методов гарантированного обезличивания, для 3 видов данных.

4. Выдача сертификатов безопасности для российских сайтов. Национальным удостоверяющим центром (НУЦ) с 2022 года российскими сертификатами безопасности обеспечено более 22 тыс. доменов, в том числе в 2024 году – более 5 тыс. доменов.

5. Повышение грамотности по вопросам информационной безопасности (кибергигиена). В течение 2022 – 2024 годов повышена грамотность более 13,1 млн человек по вопросам информационной безопасности, в том числе в 2024 году – 1,8 млн человек.

5. Федеральный проект «Цифровые технологии».

Ключевая цель проекта – обеспечение технологической независимости государства, возможности коммерциализации отечественных исследований и разработок, а также ускорение технологического развития российских компаний и обеспечение конкурентоспособности разрабатываемых ими продуктов и решений на рынке.

Задачи федерального проекта заключаются в создании благоприятных условий для развития стартапов, разрабатывающих решения в сфере информационных технологий, поддержке отечественных компаний – лидеров рынка ИТ и стимулировании спроса на их решения, а также развитии перспективных высокотехнологичных направлений, таких как квантовые коммуникации, квантовые вычисления, мобильные сети связи пятого поколения (5G).

Решение данных задач предусматривало:

– грантовую поддержку проектов малых и крупных компаний, разрабатывающих российские ИТ–решения;

– грантовую поддержку внедрения на предприятиях отечественных ИТ–решений;

– льготное кредитование компаний с целью стимулирования процессов цифровой трансформации бизнеса;

– реализацию программы льготного лизинга для поддержки внедрения цифровых технологий и платформенных решений на основе отечественных программно–аппаратных комплексов;

– методическое сопровождение разработки и реализации компаниями стратегий цифровой трансформации на основе отечественных ИТ–решений и акселерации российских технологических стартапов;

– обеспечение функционирования и наполнения реестра отечественного программного обеспечения.

Данная система мер обеспечивает поддержку проектов на любой стадии технологической готовности – от идеи, разработки прототипа, акселерации стартапов до полноценного внедрения разработок и тиражирования лучших отечественных решений.

Развитие высокотехнологичных направлений, требующих централизованных прикладных исследований, разработок и создания отечественного оборудования, осуществляется с привлечением ресурсов и компетенций крупнейших российских технологических госкомпаний, заключивших соглашения с Правительством Российской Федерации.

6. Федеральный проект «Цифровое государственное управление».

Федеральный проект направлен на достижение национальной цели «Цифровая трансформация», которая определена указом Президента Российской Федерации от 07 мая 2024 г. № 309 «О национальных целях

развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» [39].

Ключевой целевой показатель достижения национальной цели – увеличение доли массовых социально значимых услуг, доступных в электронном виде, до 95% к 2030 году.

Федеральный проект обеспечивает развитие информационных систем инфраструктуры электронного правительства. Это является одной из ключевых задач Минцифры, направленной на совершенствование процесса предоставления государственных услуг в электронном виде.

Инструменты электронного правительства снижают административные барьеры, экономят время граждан, упрощают регистрацию компаний, получение согласований и разрешений путём организации информирования граждан и оказания государственных и муниципальных услуг в электронном виде.

«Единый портал государственных и муниципальных услуг» (ЕПГУ) – наиболее востребованный среди граждан инструмент электронного правительства. ЕПГУ обеспечивает дистанционное взаимодействие граждан и государства, без необходимости очного посещения государственных органов и МФЦ.

В рамках федерального проекта также обеспечивается цифровая трансформация органов власти. Цифровая трансформация позволяет оптимизировать процессы предоставления услуг и сервисов. Прорывным проектом в этом направлении стал перевод функционирования сервисов на единую цифровую платформы «Гостех».

Кроме того, реализовываются инструменты взаимодействия граждан, бизнеса и органов власти, такие как платформа обратной связи (ПОС), подсистема по обеспечению доступа пользователей к информации, размещаемой на официальных сайтах органов и организаций в информационно–телекоммуникационной сети «Интернет» (Госвеб),

электронная подпись с использованием мобильного приложения «Госключ». Хронология результатов проекта представлена в таблице 2.

Таблица 2. – Хронология реализации федерального проекта «Цифровое государственное управление»

№	Год	Результаты
1	2	3
1	2018	Утверждён первый паспорт федерального проекта (протокол президиума Совета при Президенте РФ по стратегическому развитию и национальным проектам от 24 декабря 2018 г. № 16)
2	2019	Старт пилота по внедрению Платформы обратной связи
3	2020	Запущено 10 суперсервисов (цифровое исполнительное производство; трудовые отношения онлайн; оформление европротокола онлайн; моё здоровье; поступление в ВУЗ онлайн; социальная поддержка онлайн; образование в России для иностранцев; онлайн помощь при инвалидности; пенсия онлайн; уведомление и обжалование штрафов за нарушения ПДД онлайн)
4	2021	1. 2 августа 2021 г. запущено мобильное приложение «Госключ». 2. Молодые люди в возрасте от 14 до 22 лет могут оформить «Пушкинскую карту» и используют приложение для того, чтобы покупать билеты и посещать музеи, концерты, выставки, смотреть российское кино
5	2022	1. Запущено 3 новых суперсервиса (рождение ребёнка; безбумажные перевозки пассажиров и грузов; цифровое строительство). 2. Успешно завершился эксперимент по созданию платформы «ГосТех». 3. Обеспечен перевод всех массовых социально значимых услуг в электронный вид. 4. С 4 июля 2022 г. можно оформить Карту болельщика на Госуслугах. 4. КС «АРМ ГС» внедрён в 10 Федеральных органах исполнительной власти
6	2023	1. С помощью портала Госуслуг семьи с детьми до 17 лет и беременные женщины могут оформить выплаты: единое пособие на детей и беременных женщин;

		2. На платформе «Гостех» создано более 30 федеральных и региональных сервисов

Продолжение таблицы 2

1	2	3
7	2024	1. В суперсервисе «Рождение ребенка» реализована подача отцом заявления на регистрацию рождения. 2. На Платформе обратной связи проходит голосование по выбору общественных территорий для благоустройства в 2025 году. Проголосовало более 16,3 млн человек, в том числе 5,1 млн человек проголосовало через ПОС. 3. На Госуслугах появилась возможность заполнения черновиков заявлений для записи учеников в школы на 2024–2025 учебный год. Заранее заполненные заявления можно отправить в школу после открытия приема

7. Федеральный проект «Искусственный интеллект».

Задача федерального проекта – создать для бизнеса и граждан благоприятные условия использования продуктов и услуг, основанных преимущественно на отечественных технологиях искусственного интеллекта (ИИ) и обеспечивающих качественно новый уровень эффективности деятельности.

Основные направления реализации федерального проекта:

1. Поддержка научных исследований и разработок.

2. Разработка и развитие ПО, в том числе за счет поддержки стартапов и пилотных внедрений технологий ИИ.

3. Создание комплексной системы правового регулирования в сфере ИИ.

4. Увеличение доступности и качества данных.

5. Повышение доступности аппаратного обеспечения.

6. Обеспечение российского рынка технологий ИИ квалифицированными кадрами.

7. Информирование населения о возможных сферах использования ИИ.

Искусственный интеллект в Российской Федерации (ИИ) – комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма), получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека.

Современные технологии искусственного интеллекта реализуются по следующим направлениям:

- компьютерное зрение;
- обработка естественного языка;
- распознавание и синтез речи;
- интеллектуальные системы поддержки принятия решений;
- перспективные методы ИИ.

В целях развития искусственного интеллекта в Российской Федерации Указом Президента Российской Федерации от 10 октября 2019 года № 490 утверждена Национальная стратегия развития искусственного интеллекта до 2030 года в Российской Федерации (далее – Стратегия) [48].

Главным инструментом реализации Стратегии является «дорожная карта» развития высокотехнологичного направления «Искусственный интеллект», где ключевыми участниками являются Правительство Российской Федерации, ПАО «Сбербанк», Российский фонд прямых инвестиций (РФПИ) и Консорциум НТИ по ИИ.

«Дорожная карта» содержит мероприятия государства федерального проекта «Искусственный интеллект», а также продуктовую составляющую и мероприятия вышеперечисленных компаний–лидеров.

Кроме того, для решения задач по развитию высокотехнологичной отрасли «Искусственный интеллект» бизнесом сформирован Альянс искусственного интеллекта, включающий основных участников рынка, заинтересованных в развитии отрасли (ПАО «Сбербанк», «Яндекс», VK,

«Газпром нефть» и Российский фонд прямых инвестиций (РФПИ), «Самолет», «Уралхим», «Сибур», «Северсталь».

Федеральный проект «Искусственный интеллект» действует с 2021 по 2024 гг., включает 5 показателей, 19 результатов, обеспеченных бюджетным финансированием – 27,4 млрд рублей и внебюджетным финансированием – 4,1 млрд руб.

Ключевые результатами федерального проекта до 2023 г.:

- Гранты на прохождение акселерации получили 306 проектов (2023 г. – 99 проектов), представлена грантовая поддержка на разработку, развитие и коммерциализацию ИИ–решений 491 проекту (2023 г. – 88 проектов), гранты на внедрение ИИ–решений получил 21 проект (2023 г. – 16 проектов).

- 42 коллектива разработчиков открытых библиотек по ИИ получили гранты (2023 г– 6 коллективов). Утверждено 96 стандартов в сфере ИИ (2023 г. – 43 стандарта).

По статистике ВЦИОМ 83%, граждан считает, что государство должно развивать ИИ: доверие к ИИ выразило 52% граждан (40% не доверяет, 8 % не определились). Также выявлено, что 68% граждан, заинтересованных в развитии таких технологий, удовлетворены условиями работы в Российской Федерации.

С помощью поддержки 6 исследовательских центров в сфере ИИ первой «волны» было привлечено 26 индустриальных партнеров, опубликовано 112 статей на конференциях уровня A* (2023 г. – 63 статьи).

В 2023 г. было отобрано 6 исследовательских центров второй «волны» в 4 отраслях (здравоохранение, строительство, промышленность и транспорт). Таким образом количество исследовательских центров в сфере ИИ составило 12 штук.

Лидирующими ВУЗами по ИИ–образованию было выпущено 17 615 специалистов (2023 г. – 5 951 чел.), а 3 832 человека получило дополнительное профессиональное образование в сфере ИИ (2023 г. – 2 134 чел.).

Для формирования проектов в области ИИ обучение компетенциям прошли 53 602 школьника (2023 г. – 32 719 чел.). Проекты по ИИ сформированы 2 451 командой школьников (2023 г. – 1 846 команд). Во всероссийской олимпиаде по ИИ с привлечением компаний Альянса в сфере искусственного интеллекта приняли участие 29 513 школьников (2023 г. – 15 906 чел.).

Повышение квалификации в сфере ИИ прошли 3 675 преподавателя высшего образования (2023 г. – 1751 чел.), а также 32 002 школьных учителя (2023 г. – 16 300 чел.).

В 56 хакатонах по ИИ по решению бизнес и социальных проблем, в том числе на основе государственных наборов данных, приняли участие 32 330 человек (2023 г. – 11 498 чел.).

Также обозначены меры поддержки для бизнеса (льготы для поставщиков услуг облачных вычислений, гарантированный спрос на вычислительные мощности, гранты на разработку и внедрение ИИ–решений, обеспечение инвестиций, сертификация ИИ–решений, пилотные зоны для апробации разработок); для учёных (увеличение финансирования научных исследований в области ИИ, льготный доступ к вычислительным мощностям, запуск профильных лабораторий); для школьников и студентов (новые отраслевые образовательные программы, гранты для привлечения ученых и сотрудников крупных компаний к преподаванию, специальные стипендии, всероссийские конкурсы, олимпиады и летние школы).

В начале 2024 года указом Президента Российской Федерации в национальную стратегию развития ИИ внесены существенные изменения. В новый документ добавлены, в частности, такие основные понятия, как большие генеративные модели, большие фундаментальные модели, исходные данные, модель ИИ, отказоустойчивость, параметры модели ИИ, промышленные данные, решение в области ИИ, сильный ИИ, доверенные технологии ИИ. Отдельно отмечено, что технологии ИИ являются областью международной

конкуренции. Технологическое лидерство в области ИИ может позволить государствам достичь значимых результатов по основным направлениям социально–экономического развития.

8. Федеральный проект «Развитие кадрового потенциала ИТ–отрасли».

Федеральный проект национальной программы «Цифровая экономика Российской Федерации» формирует у молодёжи цифровые компетенции со старших классов. В перспективе он поможет уменьшить разрыв между требованиями работодателей и уровнем кандидатов в области ИТ.

Федеральный проект реализуется в рамках перечня инициатив социально–экономического развития Российской Федерации до 2030 года [44].

Цель федерального проекта – создание возможностей для формирования востребованных рынком труда цифровых компетенций.

Какие результаты обеспечены к 2025 году.

Более 231 тыс. студентов получили дополнительную квалификацию по ИТ–профилю на «цифровых кафедрах» – участниках программы стратегического академического лидерства «Приоритет–2030».

Более 250 тыс. талантливых школьников 8–11 классов и студентов колледжей завершили обучение на бесплатном дополнительном курсе обучения современным языкам программирования.

Проект направлен на достижение «цифровой зрелости» ключевыми отраслями экономики и социальной сферы, в том числе здравоохранением и образованием, а также государственного управления в рамках национальной цели «Цифровая трансформация». Для этого увеличат количество квалифицированных ИТ–кадров и будут поддерживать баланс спроса и предложения на рынке труда в ИТ–отрасли.

Проект «Цифровые кафедры» запущен в 2022 году. Благодаря ему студенты вузов–участников программы «Приоритет–2030» как ИТ, так и не ИТ–специальностей смогут получить вторую «цифровую» квалификацию

ИТ–профиля в соответствии с текущими потребностями приоритетных отраслей экономики.

Для его запуска разработали требования и Матрицу (модель) цифровых компетенций – по ним вузы–участники разрабатывали свои дополнительные профессиональные программы ИТ–профиля. Длительность программ составляет от 9 до 15 месяцев, а трудоёмкость – не менее 250 часов.

В соответствии с Матрицей оценивается уровень сформированности цифровых компетенций студентов, составляется их цифровой профиль с рекомендациями по развитию ИТ–навыков.

Для оценки соответствия разработанных программ запросам ведущих ИТ–компаний и приоритетных отраслей экономики дополнительные программы ИТ–профиля вузов проходят экспертизу.

В 2022 стартовал проект «Код будущего» – курсы обучения современным языкам программирования для школьников 8–11 классов и студентов колледжей. Чтобы стать участником проекта, необходимо подать заявление на Госуслугах.

При подаче заявления можно выбрать один из языков программирования – Python, JavaScript, C++, 1C, C# и другие. Также выбирается формат обучения – онлайн или офлайн. В 2023–2024 учебном году для обучения в формате офлайн во всех субъектах Российской Федерации и г. Байконуре было открыто более 6 тыс. образовательных площадок

В 2023–2024 учебном году на портале Госуслуг было размещено более 200 курсов от 28 образовательных организаций – провайдеров.

9. Федеральный проект «Обеспечение доступа в интернет за счёт развития спутниковой связи».

Федеральный проект «Обеспечение доступа в Интернет за счёт развития спутниковой связи» национальной программы «Цифровая экономика Российской Федерации» реализуется в рамках перечня инициатив социально–экономического развития Российской Федерации до 2030 года,

утверждённых распоряжением Правительства Российской Федерации от 6 октября 2021 года № 2816–р [44].

Цель федерального проекта – создать равные возможности доступа к современным телекоммуникационным сервисам всем жителям и компаниям в нашей стране.

Реализация инициативы «Доступ в Интернет» обеспечит россиян возможностью воспользоваться современными телекоммуникационными сервисами, в том числе в удалённых и труднодоступных местностях, где строительство волоконно–оптических линий связи высокозатратно или невозможно. Для этих целей в рамках федерального проекта создаются спутниковые системы связи «Экспресс» на геостационарной орбите.

В 2030 году территория РФ будет покрыта спутниковой связью с применением космических аппаратов на геостационарной орбите.

Федеральный проект «Обеспечение доступа в Интернет за счет развития спутниковой связи» направлен на достижение показателя «Рост доли домохозяйств, которым обеспечена возможность широкополосного доступа к информационно–телекоммуникационной сети «Интернет» до 97%» национальной цели развития Российской Федерации «Цифровая трансформация».

В рамках показателя 97% домашних хозяйств к концу 2030 года будут обеспечены возможностью широкополосного доступа к сети «Интернет».

Таким образом, Национальная программа ««Цифровая экономика Российской Федерации» получила свою «вторую» жизнь путем трансформации в Национальный проект ««Экономика данных и цифровая трансформация государства».

В 2025 году началась реализация проекта, рассчитанного до 2030–го года [33].

В разработке проекта приняли участие более 50 федеральных органов власти и служб, а также более 600 экспертов: представители бизнеса, науки и

образования, институтов развития, региональные органы исполнительной власти и местного самоуправления.

Приняли участие в опросах общественного мнения о приоритетности развития ИТ–направлений более 4 000 человек.

Цель проекта – цифровая трансформация государственного и муниципального управления, экономики и социальной сферы.

Национальный проект «Экономика данных и цифровая трансформация государства» (НЭД) является комплексным и затрагивает все ключевые отрасли экономики.

Мероприятия НЭД направлены на:

– обеспечение информационной безопасности и предоставления комфортного комплекса госуслуг для граждан, охватывающего наиболее востребованные жизненные ситуации;

– решение задач госуправления и регионального развития;

– обеспечение «цифровой зрелости» государственного и муниципального управления, отраслей соцсферы и ключевых отраслей экономики [39].

В национальный проект входят 9 федеральных проектов (таблица 3).

Таблица 3. – Федеральные проекты Национального проекта «Экономика данных и цифровая трансформация государства»

№	Название федерального проекта	О проекте
1	2	3
1	Инфраструктура доступа к информационно–телекоммуникационной сети «Интернет»	Планируется создать низкоорбитальную спутниковую группировку из 292 космических аппаратов для быстрого и дешёвого доступа к сети «Интернет» на территории всей страны
2	Цифровые платформы в отраслях социальной сферы	Направлен на создание универсальных цифровых платформ в отдельных социально–экономических сферах. Это необходимо для обеспечения эффективного

		электронного взаимодействия и исключения административных барьеров при оказании государственных услуг и предоставлении социальных гарантий населению. Также проект направлен на достижение «цифровой зрелости» отраслей социальной сферы

Продолжение таблицы 3

1	2	3
3	Искусственный интеллект	Направлен на ускоренное развитие технологий искусственного интеллекта (ИИ) в РФ. Ожидаемый результат – стимулирование научных исследований в области искусственного интеллекта, развитие ИИ–решений в государственном управлении, совершенствование системы подготовки кадров и поддержки разработчиков
4	Цифровое государственное управление	Направлен на развитие инфраструктуры услуг и сервисов в цифровом виде для их предоставления при непосредственном обращении заявителя или в проактивном режиме, а также на достижение «цифровой зрелости» в ключевых отраслях экономики и сферы государственного управления
5	Отечественные решения	Направлен на обеспечение перехода российских организаций ключевых отраслей экономики на использование отечественных разработок и оборудования для повышения эффективности их деятельности и снижения зависимости от иностранных решений
6	Прикладные исследования и перспективные разработки	Направлен на предотвращение технологического отставания в сфере информационных технологий за счет развития перспективных квантовых и телекоммуникационных технологий. В рамках проекта планируется проведение научных исследований и разработок в сферах: – разработка отечественного квантового процессора и создание прототипов квантовых сенсоров; – проведение научных исследований и

		разработок в сфере квантового шифрования и коммуникаций; – создание перспективных технологий (6G) в сфере телекоммуникаций – критические технологии создания оборудования для сетей связи 5G Advanced и 6G.
7	Инфраструктура кибербезопасности	Направлен на снижение ущерба от кибератак и повышение уровня информационной безопасности.

Продолжение таблицы 3

1	2	3
		В рамках проекта планируется реализация мероприятий, направленных на создание системы эффективного противодействия преступлениям, совершаемым с использованием ИКТ, а также на снижение ущерба от их совершения, обеспечение сетевого суверенитета и ИБ в сети «Интернет».
8	Кадры для цифровой трансформации	Направлен на сокращение дефицита высококвалифицированных специалистов в сфере информационных технологий. Школьники и студенты колледжей могут бесплатно обучаться на ИТ–курсах, а студенты вузов – пройти обучение по основным образовательным программам для разработчиков ИТ решений продвинутого уровня. В подготовке будущих ИТ–специалистов будут принимать активное участие аккредитованные ИТ–компании
9	Государственная статистика	Направлен на повышение качества, достоверности и защищенности статистических данных, сокращение сроков их формирования. Так, планируется: – переход к новой технологической основе формирования официальной статистической информации (включая технологии обработки данных); – разработка статистических методологий расчета показателей и стандартов качества статистических данных с использованием административных и больших данных;

		– замена новыми технологиями взаимодействия с респондентами устаревших и трудозатратных технологий; – повышение удовлетворенности респодентов и пользователей официальной статистической информации

Следует отметить основные планируемые показатели реализации Национального проекта к 2030 году:

– доля домохозяйств, которым обеспечена возможность качественного высокоскоростного широкополосного доступа к информационно–телекоммуникационной сети Интернет – 97%;

– доля российских организаций ключевых отраслей экономики, перешедших на использование базового и прикладного российского ПО в системах, обеспечивающих основные производственные и управленческие процессы – 80%;

– доля российского ПО, используемого в деятельности государственных органов, государственных корпораций, государственных компаний и хозяйственных обществ, в уставном капитале которых доля участия Российской Федерации в совокупности превышает 50%, а также в их аффилированных юридических лицах – 95%;

– доля предотвращённых попыток мошеннических действий, совершённых с использованием информационно–телекоммуникационных технологий (по отношению к 2024 году) – 150%;

– доля трафика российского сегмента информационно–телекоммуникационной сети Интернет, ежегодно обрабатываемого автоматизированной системой обеспечения безопасности (АСБИ), с учётом его ежегодного роста – 98%;

– доля государственных услуг и сервисов, по которым средняя оценка удовлетворённости качеством работы госслужащих и работников организаций

социальной сферы по их оказанию в электронном виде с использованием ЕПГУ и (или) РПГУ выше 4,5 – 75%;

– достижение «цифровой зрелости» государственного и муниципального управления и ключевых отраслей социальной сферы, предполагающей автоматизацию большей части транзакций в рамках единых отраслевых цифровых платформ и модели управления на основе данных с учётом ускоренного внедрения технологий обработки больших объёмов данных, машинного обучения и искусственного интеллекта – 46,7%;

– доля массовых социально значимых государственных и муниципальных услуг, предоставляемых в электронной форме – 99%;

– доля органов государственной власти и органов местного самоуправления, подключённых к единой цифровой платформе подбора, развития и ротации кадров – 60%;

– количество массовых социально значимых государственных и муниципальных услуг в электронной форме, доступных с использованием единого портала госуслуг, процесс оказания которых обеспечен ведомствами в проактивном режиме либо в момент обращения заявителя – 100 ед. [33].

Также необходимо отметить, что одним из важнейших изменение в связи с цифровизацией – это создание в каждом субъекте РФ так называемого центра управления регионом – ЦУРа. Центр управления регионом – это формируемый в субъекте РФ проектный офис, создание и деятельность которого регламентируется нормативным правовым актом субъекта РФ.

ЦУР осуществляет:

– «координацию работ по мониторингу и обработке всех видов обращений и сообщений физических и юридических лиц, поступающих в органы и организации, в том числе с использованием федеральных, региональных, муниципальных систем обратной связи и обработки сообщений, а также публикуемых гражданами и юридическими лицами в общедоступном

виде в социальных сетях, мессенджерах, иных средствах электронной массовой коммуникации;

– взаимодействие с гражданами через социальные сети, мессенджеры и иные средства электронной коммуникации по направлениям и тематикам деятельности центра управления региона;

– оперативное реагирование по направлениям и тематикам деятельности ЦУР через взаимодействие с органами и организациями; предоставление дополнительной информации в целях территориального и стратегического планирования развития субъектов РФ» [60]

Центр управления Республикой Башкортостан (ЦУР) – постоянно действующий орган при главе Республики Башкортостан и правительстве региона [41].

Среди основных задач ЦУРа следует выделить:

- выработка предложений по стратегическим целям и механизмам их достижения;

- обеспечение немедленного реагирования и оперативного разрешения инцидентов;

- содействие в реализации и управление реализацией отдельных значимых проектов правительства;

- мониторинг и анализ складывающейся в Республике Башкортостан ситуационной обстановки, а также прогнозирование её изменения;

- организация сбора и обработки необходимой достоверной информации.

В 2024 году Башкортостан стал пилотным регионом для реализации платформы обратной связи для бизнеса «ЦУР.Бизнес». Новый сервис внедрен на базе федеральной государственной информационной системы «Единый портал государственных и муниципальных услуг». Главное условие для направления обращения посредством Платформы обратной связи – авторизация предпринимателей или юридического лица на Едином портале Госуслуг.

Сообщения направляются через электронные формы (виджеты), размещенные на официальных сайтах органов.

Внедрение специального сервиса рассмотрения обращений от предпринимателей и инвесторов помогает оперативно рассматривать и реагировать на запросы бизнеса. Если бизнесу требуется консультация, он получит ее в течение пяти дней. В случае необходимости помощи или решения проблемы, ответ будет предоставлен в течение 10 календарных дней для первого варианта и в течение 30 календарных дней для второго. Это позволит принимать системные решения по направлениям инвестиционной деятельности и развития предпринимательства [8]. Также на Инвестиционном портале Республики Башкортостан размещено 24 электронных сервиса для предпринимателей и инвесторов, среди которых популярными являются «Меры поддержки», «Инвестиционная карта Республики Башкортостан», «Предпринимательский час», «Витрина проектов», «Имущество РБ».

1.3. Информационная безопасность в государственном управлении

Информационное пространство становится одним из важнейших элементов современной жизни общества и государства. В настоящее время информация приобретает особую значимость, так как она влияет на принятие управленческих решений, функционирование экономических систем и безопасность граждан. В этой связи проблема информационной безопасности выходит на первый план, в том числе и в государственном управлении, где сохранность и целостность конфиденциальных данных имеет решающее значение для устойчивого функционирования государства.

Государственная система управления проходит всеобъемлющую цифровую трансформацию, внедряются электронные сервисы, значительно повышается зависимость государственных органов от информационных технологий. В связи с этим обстоятельством, возрастает необходимость

надёжного обеспечения информационной безопасности и защиты данных от возможных внешних и внутренних угроз, злоупотреблений.

Государственные управленческие решения в сфере обеспечения информационной безопасности принимаются на основе соответствующей нормативно–правовой и институциональной базы.

Нормативно–правовая база в сфере информационной безопасности представляет собой совокупность законодательных и подзаконных актов, которые регулируют отношения в области защиты информации, кибербезопасности, защиты персональных данных. Она играет ключевую роль в формировании правовых основ для управления информационной безопасностью, защиты интересов государства и всех граждан. Основными элементами нормативно–правовой базы являются законы, подзаконные акты, международные соглашения.

Правовое содержание информационной безопасности государства допустимо представлять, как установленный законом правовой порядок обеспечения национальной безопасности в информационной сфере, интегрирующий множество информационных процессов, относящихся к различным областям жизнедеятельности общества. Основной целью обеспечения информационного правопорядка в условиях цифровой экономики является правовая суверенизация, которая выражается в разработке нормативно–правовой базы, регламентирующей функционирование информационных ресурсов на территории государства в интересах национальной безопасности государства [63].

Законы, касающиеся информационной безопасности, обеспечивают правовую основу для принятия управленческих решений по защите конфиденциальной информации государственного, ведомственного и персонального уровня. Они могут включать законодательства о персональных данных, о кибербезопасности, о государственной тайне. Законодательство о персональных данных регулирует сбор, обработку и хранение персональной

информации граждан. Примером является Федеральный закон «О персональных данных» в России, который устанавливает права субъектов данных и обязанности операторов.

Законодательство о кибербезопасности определяет меры по защите информационных систем и сетей от киберугроз. В России таким законом является Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» [36]. Законодательство о государственной тайне регулирует защиту информации, составляющей государственную тайну, и определяет порядок доступа к такой информации и порядок её распространения.

Подзаконные акты уточняют и конкретизируют положения законов, устанавливая детализированные требования и процедуры. К ним относятся постановления правительства, регулирующие порядок осуществления контроля за соблюдением норм в области информационной безопасности; приказы министерств и ведомств, касающиеся технических стандартов, требований к системам защиты информации.

Международные соглашения регулируют участие государства в международных договорах, касающихся кибербезопасности, играют важную роль в формировании правовой базы для принятия управленческих решений. Примером является Будапештская конвенция о киберпреступности, которая устанавливает общие подходы к борьбе с киберпреступностью и сотрудничеству между государствами.

Центры информационной безопасности играют ключевую роль в обеспечении киберзащиты, анализа угроз и разработки новых технологий для защиты информации. Эти центры широко представлены в сети Интернет и охватывают различные направления деятельности, каждое из которых имеет свои уникальные функции и цели [2].

Информационно–аналитические центры занимаются сбором, обработкой и анализом данных о текущих угрозах и уязвимостях в области

информационной безопасности. Они предоставляют экспертные оценки и рекомендации по улучшению защиты информации. Такие центры часто публикуют отчеты, исследования и прогнозы, которые помогают организациям понимать риски и принимать обоснованные решения.

Например, Российская компания Positive Technologies 20 марта 2025 года опубликовала аналитический отчёт «Актуальные киберугрозы: IV квартал 2024 года – I квартал 2025 года». Отчет содержит информацию об общемировых актуальных угрозах информационной безопасности, основанную на экспертизе компании Positive Technologies, результатах расследований, проводимых PT Expert Security Center, а также на данных авторитетных источников. По мнению компании, большинство кибератак в мире не предаются огласке из–за репутационных рисков [2].

Согласно отчёту, в IV кв. 2024 г. количество зарегистрированных инцидентов увеличилось на 5% по сравнению с предыдущим кварталом, и на 13% в сравнении с аналогичным периодом прошлого года. Вредоносный код остается основным инструментом: применялся в 66% успешных атак на организации и 51% на частных лиц. Против организаций, чаще всего, использовались шифровальщики (42%) и программы для удаленного управления (38%), против частных лиц – шпионские программы (48%). За рассматриваемый период в результате 53% успешных атак на организации была раскрыта конфиденциальная информация, а нарушение основной деятельности компаний наблюдалось в 32% инцидентов.

Центры оперативного реагирования (CSIRT) специализируются на быстром реагировании на инциденты информационной безопасности. Они работают в режиме 24/7 и обеспечивают поддержку организациям в случае кибератак или утечек данных. Основные функции таких центров включают: обнаружение и анализ инцидентов, устранение последствий атак, консультирование по вопросам защиты и предотвращения будущих

инцидентов. Такие центры есть в США, в Великобритании и других странах. Например, Security Operation Centre от Сбербанка.

Научно–исследовательские центры занимаются разработкой новых технологий и методов в области информационной безопасности. Они проводят исследования по вопросам криптографии, защиты данных, сетевой безопасности и других аспектов. Эти центры сотрудничают с университетами и промышленностью для внедрения новых решений. Примеры: Федеральный научный технический центр защиты информации ФСТЭК России.

Центры сертификации занимаются проверкой и подтверждением соответствия продуктов и услуг стандартам безопасности. Они обеспечивают доверие к технологиям и решениям в разных отраслях. Сертификация может касаться как программного обеспечения, так и аппаратных решений. В России центром сертификации организаций по стандартам управления информационной безопасностью выступает Федеральная служба по техническому и экспортному контролю (ФСТЭК России).

Центры информационной безопасности являются важными игроками в глобальной экосистеме киберзащиты. Их разнообразные направления деятельности позволяют эффективно противостоять угрозам, обеспечивать защиту данных и развивать новые технологии. Эти центры не только помогают организациям справляться с текущими угрозами, но и способствуют формированию безопасной цифровой среды в целом.

Однако, в области государственного нормативно–правового регулирования информационной безопасности в России немало проблем и вызовов. Быстрое развитие технологий и изменение характера киберугроз требуют оперативного обновления законов, что на практике, зачастую происходит медленно. Учитывая международные обязательства, государству необходимо гармонизовать национальное законодательство с международными стандартами, что может быть сложно из–за различий в правовых системах.

Значимой проблемой являются ограниченность ресурсов, выделяемых для реализации законов, а также недостаток квалифицированных кадров. Это может сказаться на эффективности мер по защите информации. Государственные органы играют ключевую роль в реализации нормативно–правовой базы, они разрабатывают и внедряют стратегии и программы по информационной безопасности, обеспечивают мониторинг соблюдения законодательства и оценку его эффективности, сотрудничают с предприятиями и научными учреждениями для обмена опытом и технологиями.

Таким образом, нормативно–правовая база является основой для формирования эффективной системы управления информационной безопасностью. Она обеспечивает правовые рамки для защиты информации и создания безопасной информационной среды. Важно, чтобы эта база была гибкой и адаптивной к изменениям в технологической среде и к новым вызовам, что требует постоянного анализа и обновления законодательства.

Институциональная база в контексте обеспечения информационной безопасности включает в себя совокупность государственных органов, организаций и учреждений, а также их взаимодействие и функции, направленные на защиту информации и кибербезопасность. Важность этой базы заключается в том, что она определяет структуру и механизмы, через которые осуществляется реализация государственной политики в области информационной безопасности.

Основными элементами институциональной базы являются государственные органы (президент РФ, совет безопасности РФ, ФСБ, МВД, СВР, министерство цифрового развития, связи и массовых коммуникаций), регуляторы и надзорные органы (Роскомнадзор, ФСТЭК), научные и образовательные учреждения (научные институты и университеты, образовательные программы и курсы).

Президент Российской Федерации является главным гарантом безопасности государства, определяет основные направления государственной

политики в области информационной безопасности и утверждает ключевые документы, такие как Доктрина информационной безопасности. Совет безопасности Российской Федерации – это консультативный орган, который обеспечивает координацию действий различных государственных структур в сфере безопасности, включая информационную безопасность.

Федеральная служба безопасности (ФСБ) – это основной орган, отвечающий за защиту государственной тайны, борьбу с киберпреступностью и защиту критической информационной инфраструктуры. Министерство цифрового развития, связи и массовых коммуникаций отвечает за развитие цифровых технологий и внедрение стандартов безопасности в информационных системах.

Министерство внутренних дел (МВД) занимается расследованием киберпреступлений и обеспечением общественной безопасности в сети. Служба внешней разведки (СВР) участвует в обеспечении безопасности информации на международном уровне и противодействует внешним угрозам. Роскомнадзор – это федеральная служба, ответственная за контроль и надзор в сфере связи, информационных технологий и массовых коммуникаций, включая защиту персональных данных. Федеральная служба по техническому и экспортному контролю (ФСТЭК) занимается вопросами защиты информации в государственных и коммерческих организациях, а также сертификацией средств защиты информации.

Научные институты и университеты участвуют в подготовке специалистов в области информационной безопасности. Образовательные программы и курсы обеспечивают подготовку кадров, необходимых для работы в сфере информационной безопасности, включая аспекты правового регулирования и технической защиты.

Институциональная база требует эффективного взаимодействия и координации между различными государственными органами и учреждениями. Межведомственные комиссии и рабочие группы создаются для решения

конкретных задач в области информационной безопасности, таких как разработка новых стандартов или реагирование на инциденты. Совместные учения и тренировки проводятся для повышения готовности государственных структур к реагированию на киберугрозы и инциденты. Высокотехнологичный обмен электронной информацией между различными органами власти позволяет им своевременно реагировать на угрозы.

Несмотря на наличие институциональной базы, в сфере обеспечения информационной безопасности существуют определенные проблемы. В частности, фрагментация: разные органы могут действовать независимо друг от друга, что затрудняет координацию и эффективное реагирование на угрозы; недостаток ресурсов: ограниченные финансовые и человеческие ресурсы могут сказываться на способности органов выполнять свои функции; быстрое развитие технологий: постоянно меняющаяся технологическая среда требует от государственных органов адаптации и обновления подходов к безопасности.

Для повышения эффективности институциональной базы в сфере информационной безопасности необходимо создание действенных механизмов взаимодействия между государственными органами, предприятиями и научными учреждениями (усиление координации); обеспечение финансирования для разработки и внедрения современных технологий защиты информации (инвестиции в технологии); разработка программ для повышения квалификации специалистов в области информационной безопасности (обучение и повышение квалификации); участие в международных инициативах и соглашениях, направленных на борьбу с киберпреступностью (международное сотрудничество).

Институциональная база государственных управленческих решений в сфере обеспечения информационной безопасности является важным компонентом системы национальной безопасности. Эффективная работа этой базы требует постоянного анализа, обновления и адаптации к новым вызовам, связанным с развитием технологий и изменением угроз в киберпространстве.

Создание устойчивой и эффективной институциональной структуры позволит не только защитить информацию на национальном уровне, но и повысить общую безопасность общества, обеспечивая защиту критической инфраструктуры и личных данных граждан.

Таким образом, для успешного противодействия киберугрозам необходимо развивать механизмы координации, улучшать взаимодействие между государственными и частными структурами, а также готовить квалифицированные кадры, способные эффективно реагировать на современные вызовы в области информационной безопасности. Важно, чтобы все участники процесса управления информационной безопасностью в государственных учреждениях имели единое понимание проблемы и работали по единой стратегии, что обеспечит комплексный подход к защите важной государственной, ведомственной, персональной информации и создаст более безопасную цифровую среду для граждан и предприятий.

Информационная безопасность в государственном управлении в политическом ключе представляет собой многогранную тему, затрагивающую как внутренние аспекты функционирования государственных органов, так и международные отношения. Информационная безопасность становится важным элементом национальной безопасности. В условиях глобализации и цифровой трансформации государственного управления – угрозы, исходящие из киберпространства, могут оказывать значительное влияние на политическую стабильность, общественное доверие к государственным институтам и способность правительства эффективно выполнять свои функции. Утечки информации, кибератаки и манипуляции с данными могут подрывать легитимность власти и вызывать общественные протесты.

Трансформационные процессы в обществе усилили роль информации в обеспечении стабильного функционирования государства. Обеспечение информационной безопасности стало одной из ключевых целей национальной политики. Информационное противоборство вышло в стадию когнитивной

войны, в которой информационное воздействие направлено в первую очередь на дестабилизацию социально–политических и экономических процессов [47].

Современные государства активно используют информационные технологии для проведения информационных войн. Это включает в себя не только защиту собственных информационных ресурсов, но и активные действия по дезинформации противников. В условиях глобальной конкуренции за влияние на международной арене, государства могут прибегать к кибератакам на критическую инфраструктуру других стран или к манипуляциям с общественным мнением через социальные сети.

Политические силы могут использовать вопросы информационной безопасности для продвижения своих интересов, что может привести к принятию законов, которые ограничивают свободу слова и доступ к информации под предлогом защиты от киберугроз. Это создает напряженность между необходимостью обеспечения безопасности и защитой прав граждан. Государственные органы часто сотрудничают с частными компаниями в области информационной безопасности. Это сотрудничество может быть использовано для укрепления позиций власти и контроля над информационными потоками. Однако такие отношения могут вызвать опасения по поводу приватизации безопасности и недостатка прозрачности в действиях государственных структур.

Информационная безопасность влияет на уровень доверия граждан к государственным институтам. Успешные кибератаки или утечки данных могут подорвать доверие к власти и вызвать недовольство среди населения. Важно, чтобы государственные органы эффективно информировали общество о мерах, принимаемых для защиты информации, и обеспечивали прозрачность своих действий.

Анализ информационной безопасности в государственном управлении требует комплексного подхода. Политические интересы, внутренние и международные угрозы, а также общественное мнение должны быть учтены

при разработке стратегий и политик в этой области. Эффективное управление информационной безопасностью может способствовать защите государственных интересов, укреплению доверия граждан к власти.

Современные *угрозы информационной безопасности* в сфере государственного управления обладают рядом специфических особенностей, которые делают их особенно актуальными и сложными для предотвращения и реагирования. Рассмотрим некоторые особенности угроз.

Киберугрозы постоянно эволюционируют, и злоумышленники используют новые технологии и методы для обхода существующих систем защиты (адаптивность и эволюция угроз). Угрозы часто имеют конкретные цели, такие как государственные учреждения, критическая инфраструктура или важные данные, что делает их более опасными и сложными для обнаружения (целевые атаки). Злоумышленники применяют современные технологии, такие как искусственный интеллект и машинное обучение, для автоматизации атак и повышения их эффективности (использование сложных технологий). Атаки могут включать несколько этапов, начиная с фишинга для получения доступа к системе и заканчивая установкой вредоносного программного обеспечения для кражи данных или разрушения инфраструктуры (многоуровневые атаки).

Угрозы часто используют методы социальной инженерии, чтобы манипулировать пользователями и заставить их раскрывать конфиденциальную информацию или выполнять действия, которые могут привести к компрометации систем (социальная инженерия). Угрозы могут исходить как от отдельных злоумышленников, так и от организованных преступных групп или даже государств, что усложняет их идентификацию и реагирование (сложность и разнообразие источников угроз). Кибератаки могут происходить из любой точки мира, что затрудняет правоприменение и координацию действий между различными странами (глобальный характер).

Атаки на государственные структуры могут иметь серьезные последствия для общественного доверия к государственным институтам и их способности

защищать граждан (влияние на общественное мнение и доверие). Современные угрозы могут использовать уязвимости в цепочке поставок, что делает их более сложными для обнаружения и предотвращения, особенно если речь идет о сторонних поставщиках и сервисах (уязвимости в цепочке поставок). С увеличением объема доступной информации в открытых источниках злоумышленники могут легче собирать данные для планирования атак и создания более точных профилей целей (доступность и распространенность информации).

Эти особенности угроз информационной безопасности в сфере государственного и муниципального управления требуют от государственных органов и организаций постоянного мониторинга угроз, адаптации стратегий защиты и внедрения современных технологий для обеспечения безопасности информационных систем. Многое зависит от аппаратной, технологической и кадровой обеспеченности государственных органов.

Рассмотрим основные понятия информационной безопасности в самом общем виде. Это важно с точки зрения правильного понимания государственным служащим практических проблем информационной безопасности в целом, и в государственном управлении – в частности [12].

Информационная безопасность: состояние защищенности информации от несанкционированного доступа, использования, раскрытия, разрушения, изменения или уничтожения. Конфиденциальность: свойство информации, при котором доступ к ней ограничен и разрешен только определенным лицам или системам. Целостность: свойство информации, при котором она остается неизменной и точной, а также защищена от несанкционированных изменений.

Доступность: свойство системы и информации быть доступными и используемыми авторизованными пользователями в любое время. Аутентификация: процесс проверки подлинности пользователя или системы, который подтверждает их идентичность. Авторизация: процесс предоставления

разрешений пользователю или системе на доступ к определенным ресурсам или информации после успешной аутентификации.

Учетные данные: информация, используемая для аутентификации пользователя, например, пароли, PIN–коды или биометрические данные. Шифрование: процесс преобразования данных в код, который может быть прочитан только с помощью специального ключа, обеспечивая конфиденциальность информации. Уязвимость: слабое место в системе или приложении, которое может быть использовано злоумышленником для нарушения безопасности.

Атака: намеренное действие, направленное на нарушение безопасности системы или получение несанкционированного доступа к информации. Инцидент безопасности: событие, которое нарушает нормальную работу системы безопасности или приводит к утечке информации. Политика безопасности: набор правил и процедур, определяющих, как организация защищает свою информацию и системы.

Эти понятия являются основой для понимания информационной безопасности и помогают в разработке эффективных мер по защите информации. Анализ стратегий защиты информации в государственных органах, в части касающейся сведений ограниченного доступа, требует комплексного подхода.

Стратегии защиты информации включают в себя политики и процедуры (разработка и внедрение политик безопасности, регулярные аудиты и оценки рисков), технические меры (шифрование данных, системы контроля доступа, мониторинг и обнаружение вторжений), обучение и осведомлённость (обучение сотрудников, культура безопасности), инцидентное реагирование (план реагирования на инциденты).

Разработка и внедрение политик безопасности заключается в установлении чётких правил доступа к информации, включая классификацию данных и определение уровней доступа. Регулярные аудиты и оценки рисков

заключается в проведении периодических проверок для выявления уязвимостей и оценки эффективности существующих мер безопасности. Важно использовать современные алгоритмы шифрования для защиты данных как в состоянии покоя, так и при передаче, внедрить многофакторную аутентификацию и ролевое управление доступом к информации. Мониторинг и обнаружение вторжений наиболее эффективны при использовании систем IDS/IPS для выявления и предотвращения несанкционированного доступа.

Необходимы также меры следующего характера: регулярное обучение по вопросам информационной безопасности, включая методы социальной инженерии и безопасного обращения с данными; формирование культуры, в которой безопасность информации является приоритетом для всех сотрудников; разработка и тестирование плана действий в случае нарушения безопасности, включая процедуры уведомления и восстановления.

Несанкционированный доступ – это доступ к информации без соответствующих прав, что может привести к утечке или повреждению данных. Утечка информации – это неправомерная передача или раскрытие сведений ограниченного доступа. Кибератаки включают фишинг, вредоносный код, атаки нулевого дня, DDoS–атаки, направленные на получение доступа к защищенным данным. Сотрудники могут случайно или намеренно разглашать информацию, используя недостаточно защищенные системы или не соблюдая политики безопасности.

Основные нарушения информационной безопасности, возникающие при этом угрозы безопасности и их причины приведены на рисунке (рисунок 3).

Рисунок 3 – Защита информации в государственных органах

Объектом защиты информации в государственных органах являются информационные ресурсы, содержащие сведения ограниченного доступа. Целью защиты является исключение нанесения материального, морального или иного ущерба собственникам информации в результате нарушения прав доступа. Наиболее распространённые нарушения: конфиденциальности (хищение, утрата), доступности (блокирование, уничтожение), целостности (модификация, отрицание, навязывание ложной) информации.

Причины возникновения угроз безопасности могут быть умышленными и не умышленными. Не умышленным относят ошибочные действия лояльных сотрудников, ошибки аппаратных и программных средств, умышленным – незаконное проникновение под видом легального пользователя, разрушение системы с помощью программ–вирусов, нелегальные действия легального пользователя, подслушивание внутрисетевого трафика. Для эффективной защиты информации в государственных органах необходимо реализовать комплексный подход, который включает в себя как технические, так и организационные меры. Регулярный мониторинг, обучение сотрудников и

адаптация к новым угрозам помогут минимизировать риски и защитить сведения ограниченного доступа от нарушений и утечек.

Административная составляющая информационной безопасности охватывает организационные меры и управленческие решения, направленные на защиту информационных ресурсов организации от угроз. Она включает создание политики безопасности, программы защиты, управление рисками и другие мероприятия. Основные понятия административного уровня: политика безопасности – это документально закрепленные правила и процедуры, определяющие порядок обращения с информацией внутри организации; программа безопасности – это комплекс мероприятий, направленных на реализацию требований политики безопасности; управление рисками – это процесс выявления, оценки и минимизации рисков, связанных с обработкой и хранением конфиденциальной информации, с использованием программ.

Политика безопасности представляет собой совокупность правил и процедур, регламентирующих обращение с важной информацией. Её цель – обеспечение целостности, доступности и конфиденциальности данных. Основными элементами являются: определение ответственности сотрудников за соблюдение норм информационной безопасности; регламентация порядка доступа к информации и ресурсам; правила обработки персональных данных и другой информации; меры реагирования на инциденты безопасности.

Политика безопасности включает: организационные меры (назначение ответственных лиц, инструктаж персонала), технические средства защиты (антивирусная защита, шифрование данных), порядок доступа к информации (права пользователей, управление учетными записями), контроль исполнения (внутренний аудит, мониторинг соблюдения политики).

Программа безопасности реализуется на основании утвержденной политики и направлена на выполнение конкретных действий для обеспечения требуемого уровня защищённости информации. Основные элементы программы включают: разработка инструкций и регламентов; организация

обучения сотрудников правилам безопасного использования служебной информации; создание системы мониторинга и контроля за соблюдением мер информационной безопасности; проведение регулярных проверок состояния информационной инфраструктуры. Цель программы: снизить вероятность возникновения инцидентов информационной безопасности путём внедрения превентивных мер и повышения осведомлённости сотрудников.

Процесс управления рисками является важным элементом административной составляющей информационной безопасности. Управление рисками информационной безопасности предполагает: идентификацию рисков, т.е. выявление возможных угроз и уязвимостей; оценку рисков – определение вероятности наступления угрозы и последствий для государства, граждан и бизнеса; выбор методов снижения риска, разработка и внедрение защитных мер; контроль эффективности, мониторинг результатов реализации выбранных решений. Методы управления рисками могут включать технические, организационные и правовые меры, такие как шифрование данных, их резервное копирование, обучение сотрудников, заключение договоров с поставщиками услуг.

Таким образом, административный уровень информационной безопасности обеспечивает координацию усилий всех подразделений организации по защите информации, обеспечивая целостный подход к управлению рисками и поддерживая высокий уровень информационной безопасности в государственном и муниципальном управлении.

Процедурный уровень информационной безопасности включает организационно–технические меры, направленные на повышение устойчивости информационных процессов и снижение рисков утечки данных. Этот уровень тесно взаимосвязан с административным уровнем и дополняет его конкретные мероприятия по обеспечению информационной безопасности. Основные аспекты процедурного уровня информационной безопасности следующие: классы мер процедурного уровня (организационные, технические, физические,

кадровые меры), управление персоналом, физическая защита, поддержание работоспособности, реагирование на нарушения режима безопасности, планирование восстановительных работ.

Организационные меры – это инструкции, правила внутреннего распорядка, требования к работе с секретной информацией. Технические меры – это использование антивирусов, межсетевых экранов, систем обнаружения вторжений. Физические меры – это охрана помещений, ограничение физического доступа к серверам и оборудованию. Кадровые меры – это контроль подбора и подготовки персонала, проверка лояльности сотрудников.

Эффективность мер информационной безопасности существенно зависит от квалификации и дисциплины сотрудников. Ключевыми аспектами управления персоналом являются: подбор компетентного персонала; периодическое проведение тренингов и семинаров по информационной безопасности; установление чётких обязанностей сотрудников в области информационной безопасности; регулярная оценка деятельности сотрудников, связанной с обеспечением безопасности.

Защита физической среды размещения ИТ инфраструктуры важна для предотвращения несанкционированного доступа и повреждений оборудования. Основные компоненты физической защиты: ограничение доступа посторонних лиц к помещениям, содержащим серверы и рабочие станции; установка охранных систем видеонаблюдения и сигнализации; применение специальных замков и дверей повышенной прочности; соблюдение условий эксплуатации аппаратуры (температура, влажность).

Для поддержания непрерывности бизнес–процессов необходимо регулярно проводить профилактику технических сбоев и отказов оборудования. Мероприятия по поддержке работоспособности включают: резервное копирование важных данных; тестирование и обновление программ; ремонтные работы и обслуживание оборудования; планирование замены устаревших компонентов и модернизация инфраструктуры.

Быстрое и адекватное реагирование на выявленные случаи нарушений позволяет минимизировать последствия атак и утечек информации. Важнейшие шаги при нарушении режима безопасности: незамедлительное уведомление соответствующих служб и руководства; локализация инцидента и предотвращение распространения ущерба; анализ события и подготовка отчета; принятие необходимых мер для устранения причины происшествия.

План восстановления после кибератак помогает быстро вернуть инфраструктуру в рабочее состояние. Составляющие плана восстановления: определение критически важных информационных ресурсов и сервисов; подготовка копий ключевых данных и приложений; разработка сценария быстрого развёртывания резервных мощностей; обучение персонала оперативному восстановлению данных и приложений.

Таким образом, процедурный уровень информационной безопасности направлен на практическое исполнение нормативных документов и стандартов, применяемых на административном уровне, обеспечивая устойчивость функционирования государственных органов, организаций перед внешними и внутренними угрозами информационной безопасности.

Программно–технический уровень информационной безопасности подразумевает применение специализированных технологий и инструментов для защиты информации. Эти меры реализуются посредством различных видов программного обеспечения и аппаратных устройств, нацеленных на обнаружение, предупреждение и ликвидацию потенциальных угроз.

Основные направления программно–технического обеспечения информационной безопасности: средства аутентификации и авторизации; межсетевые экраны (firewalls); средства анализа сетевого трафика; антивирусные программы и средства борьбы с вредоносным кодом; системы шифрования; система обнаружения и предотвращения вторжений (IDS/IPS); брандмауэры прикладного уровня (Web Application Firewall, WAF);

DLP–системы (Data Loss Prevention); VPN туннелирование; патч–менеджмент и обновления программного обеспечения.

Средства аутентификации и авторизации обеспечивают надежную идентификацию пользователей и контролируют доступ к данным и сервисам. Примеры: одноразовые пароли, биометрические системы идентификации (сканеры отпечатков пальцев, лица, сетчатки глаза), многофакторная аутентификация (использование нескольких факторов одновременно, например, пароль + токен), межсетевые экраны (firewalls).

Фирмы используют межсетевые экраны для фильтрации входящего и исходящего трафика сети, блокируя потенциально опасные подключения и запрещённые запросы. Существуют различные типы межсетевых экранов: пакетные фильтры (stateless firewalls), фильтры с отслеживанием состояний соединений (stateful inspection), приложения с глубоким инспектированием пакетов (application–level gateways).

Средства анализа сетевого трафика. Инструменты сетевого мониторинга позволяют анализировать трафик в режиме реального времени, выявляя подозрительные активности и аномалии. Типичные технологии: IDS/IPS (Intrusion Detection Systems / Intrusion Prevention Systems), Deep Packet Inspection (DPI), NetFlow анализаторы.

Антивирусные программы и средства борьбы с вредоносным кодом. Антивирусные решения защищают устройства от вирусов, троянов, шпионских программ и другого вредоносного кода. Современные продукты включают эвристический анализ и облачные базы сигнатур: классические антивирусные сканнеры, Sandbox–технологии (изоляция подозрительного кода), поведенческий анализ (HIPS).

Системы шифрования. Шифрование используется для защиты данных при хранении и передаче, делая их нечитаемыми для злоумышленников. Наиболее распространённые методы шифрования: симметричное шифрование (AES, DES), асимметричное шифрование (RSA, DSA), протоколы SSL/TLS для

зашифрованной передачи данных. Система обнаружения и предотвращения вторжений (IDS/IPS). IDS и IPS предназначены для автоматического выявления и предупреждения попыток проникновения в сеть и атаки на систему. Они способны реагировать на известные угрозы автоматически либо сигнализировать администраторам для принятия мер вручную.

Брандмауэры прикладного уровня (Web Application Firewall, WAF). WAF защищают веб–приложения от специфичных атак типа SQL–инъекции, XSS–вторжений и других типов угроз, характерных именно для веб–сервисов. DLP–системы (Data Loss Prevention). DLP–системы используются для предотвращения случайной или намеренной утечки конфиденциальных данных. Они контролируют передачу файлов, сообщений электронной почты и даже распечатанных документов.

VPN–туннелирование. VPN создает защищённый канал связи между удалёнными пользователями и корпоративной сетью, позволяя передавать данные безопасным способом вне зависимости от места нахождения пользователя. Патч–менеджмент и обновления ПО. Регулярные обновления операционных систем и программного обеспечения помогают устранять найденные уязвимости и защищать инфраструктуру от новых угроз.

Таким образом, комплексное использование указанных мер позволяет обеспечить многоуровневую защиту информационных активов предприятия. Эффективность каждой отдельной меры возрастает при сочетании с другими средствами, создавая многослойную защиту, способную противостоять современным киберугрозам.

Типовые удалённые атаки в глобальных компьютерных сетях включают различные методы несанкционированного проникновения и воздействия на информационные системы. Некоторые наиболее распространённые типы атак: DDoS–атаки, фишинг, SQL–инъекции, атаки XSS (Cross–Site Scripting), Man–in–the–Middle (MitM), Brute Force (подбор пароля), эксплойты нулевого дня (zero–day exploits), ransomware (шифровальщики), DNS–спуфинг (DNS

spoofing). Механизмы реализации удаленных атак в глобальных компьютерных сетях представляют собой комплекс методов и технологий, используемых злоумышленниками для достижения своих целей.

DDoS (Distributed Denial of Service) – распределённая атака типа «отказ в обслуживании». Атака направлена на перегрузку ресурсов сервера путём отправки большого количества запросов от множества источников одновременно, что делает сервер недоступным для легитимных пользователей. Механизмы реализации: амплификация, синхронизация TCP–запросов, UDP–флуд. Амплификация – использование отражающих сервисов (например, DNS–серверов), которые отправляют увеличенный объем трафика. Синхронизация TCP–запросов – отправка огромного числа SYN–пакетов на сервер, вызывая состояние полуоткрытых соединений и исчерпывая ресурсы. UDP–флуд – это генерация большого количества UDP–пакетов, направленных на случайные порты, заставляя сервер обрабатывать каждый пакет.

Фишинг подразумевает обман пользователей с целью кражи конфиденциальной информации (логинов, паролей, банковских реквизитов). Обычно осуществляется путем рассылки поддельных электронных писем, сообщений или ссылок, ведущих на фальшивые веб–сайты. Механизм реализации: создание фишинговых страниц, имитирующих известные сервисы (банковские сайты, социальные сети); рассылка массовых спам–сообщений со ссылкой на фейковый сайт; использование социальной инженерии для убеждения пользователя ввести личные данные.

SQL–инъекция позволяет внедрить вредоносные команды SQL в запросы базы данных приложения. Это даёт возможность украсть данные, изменить или удалить записи, либо даже захватить контроль над базой данных целиком. Механизм реализации: подготовка специально сформированных SQL–запросов, вводимых в поля ввода формы; используются специальные символы для изменения синтаксиса оригинального запроса, автоматические инструменты сканирования и эксплуатации SQL–уязвимостей (sqlmap).

Атаки XSS (Cross–Site Scripting) используют уязвимости веб–приложений для внедрения вредоносного JavaScript–кода на страницы сайта. Код выполняется в браузере жертвы, позволяя перехватывать куки, сессионные данные и другие чувствительные сведения. Механизм реализации: инъекция JavaScript–кода в страницу через небезопасные формы ввода или комментарии; распространение через встроенные скрипты на сторонних ресурсах. Типы атак: отражение (Reflected), хранение (Stored), DOM–based.

Man–in–the–Middle (MitM) «человек посередине» – это вид атаки, при которой злоумышленник вставляется между двумя сторонами коммуникации, незаметно прослушивая или изменяя передаваемые данные. Чаще всего используется в открытых Wi–Fi сетях. Механизм реализации: захват пакетов через ARP–spoofing (изменение MAC–адресов устройств); перехват HTTP–трафика, отсутствие шифрования SSL/TLS; установка снифферов (sniffers) для анализа сетевого трафика.

Brute force предполагает автоматический перебор возможных комбинаций паролей для взлома учётных записей. Используются списки часто используемых паролей или алгоритмы автоматического подбора. Механизм реализации: массированный подбор паролей с использованием специальных инструментов (hydra, medusa); применение списков популярных паролей (password, 123456); использование графического процессора (GPU) для ускорения процесса подбора.

Эксплойты нулевого дня нацелены на ранее неизвестные уязвимости программного обеспечения, на исправление которых разработчики ещё не выпустили патчи безопасности. Механизм реализации: поиск и эксплуатация недавно обнаруженных, но пока не закрытых разработчиками уязвимостей; специализированные хакерские форумы и рынки для обмена эксплойтами.

Ransomware представляет собой вирус–шифровальщик, который блокирует доступ к файлам и данным на компьютере пользователя, требуя выкуп за восстановление доступа. Механизм реализации: заражение

компьютера через вредоносные вложения электронной почты или уязвимые программы; шифрование файлов на зараженном устройстве; требование выкупа за расшифровку данных.

DNS–спуфинг позволяет злоумышленникам перенаправлять трафик пользователей на поддельные IP–адреса вместо реальных адресов целевых сайтов, приводя к утечке личных данных. Механизм реализации: изменение таблицы DNS–кэша клиента или сервера, чтобы перенаправлять запросы на ложные адреса; умышленное отравление DNS–кэшей (cache poisoning).

Для защиты от этих атак необходимы современные средства информационной безопасности, такие как межсетевые экраны, антивирусные решения, регулярные обновления ПО, обучение сотрудников основам кибербезопасности и использование двухфакторной аутентификации. Эти виды атак являются основными угрозами для современных корпоративных сетей и индивидуальных пользователей, и защита от них требует постоянного мониторинга и обновления защитных механизмов.

Операционная система *Windows предлагает целый ряд эффективных средств и механизмов для управления безопасностью*, необходимых для защиты инфраструктуры организаций и частных пользователей от широкого спектра потенциальных угроз. Рассмотрим основные решения и подходы, применяемые в архитектуре Windows для повышения уровня безопасности.

Групповые политики (Group Policy) обеспечивают централизованное управление политиками безопасности и конфигурации для всех устройств и пользователей внутри корпоративной среды, использующей инфраструктуру Active Directory. Администратор может задать единые правила и параметры безопасности, касающиеся учетных записей, паролей, разрешений, криптографии и многого другого. Основные элементы: управление параметрами безопасности учётных записей (минимальная длина пароля, срок действия, сложность); настройка аудита событий безопасности; ограничение установки и запуска нежелательных приложений; централизованная настройка

правил шифрования, VPN–подключений и параметров межсетевого экрана. Преимущества: единая политика безопасности для всей организации; возможность быстрой реакции на инциденты безопасности; повышение общей устойчивости инфраструктуры перед внешними угрозами.

Контроль учётных записей (User Account Control) – механизм, позволяющий предотвратить запуск критически важных операций без одобрения администратора. Когда программа пытается выполнить какое–то опасное действие (например, внести изменения в реестр или установить новую программу), UAC запрашивает подтверждение у пользователя. Принцип работы: запуск приложений и установка драйверов требуют повышенного уровня полномочий; блокировка потенциально вредных действий и сохранение системы в стабильном состоянии. Преимущества: предупреждение случайных установок вредоносного кода; минимизация риска нарушения целостности операционной системы.

Windows Defender (антивирусная система) является интегрированным решением для защиты от вирусов, троянов, руткитов и прочих форм вредоносного кода. Обеспечивает мониторинг активности на уровне файловой системы, реестра и оперативной памяти. Компоненты: сигнатурный анализ – выявление известных образцов вредоносного кода; эвристическое распознавание – обнаружение подозрительных поведений программ; анализ поведения – отслеживание попыток несанкционированного доступа к важным компонентам системы; облачные технологии – проверка файлов и поведенческих шаблонов через облачную базу данных. Преимущества: высокая степень интеграции с системой и быстродействие; бесплатное решение, поддерживаемое корпорацией Microsoft.

Защитник Windows Firewall (Межсетевой экран) – это встроенная в систему служба фильтрации сетевого трафика, контролирующая входящие и исходящие соединения. Позволяет гибко настраивать правила фильтрации и повышает уровень защиты устройства от внешних атак. Возможности: блокада

несанкционированных подключений; построение профиля безопасности на основании уровня доверия к сетям (домашняя сеть, рабочая сеть, публичная сеть); поддержка фильтрации трафика на основе портов, протоколов и служб. Преимущества: простота настройки и поддержка широкой функциональности; совместимость с современными технологиями сетевой безопасности.

Центр безопасности Windows Security Center объединяет всю информацию о защите устройства в одном месте, отображая состояние антивирусной защиты, статуса брандмауэра, настроек приватности и многих других аспектов безопасности. Функционал: отображение текущего состояния системы защиты; генерация предупреждений и рекомендаций по улучшению защиты; регулярное обновление сведений о статусе антивирусного программного обеспечения и сертификатов. Преимущества: удобство централизованного мониторинга и управления безопасностью; предоставляет понятную картину общего состояния защиты устройства.

BitLocker Disk Encryption реализует полный аппаратный метод шифрования дисков, исключающий чтение данных посторонними лицами при краже оборудования или попытке физического доступа к хранилищу данных. Особенности: полное шифрование диска, включая загрузочные области; интеграция с доверенным платформенным модулем TPM для безопасной загрузки; возможность восстановления данных при потере ключа шифрования. Преимущества: надежная защита персональных и коммерческих данных; защита от потери или хищения устройства.

Безопасность процессов (Process Integrity Protection) определяет иерархию уровней допуска процессов в операционной системе. Например, низкоуровневые процессы не могут вмешиваться в высокоуровневые. Механизм: каждому процессу присваивается определенный уровень целостности; высоко привилегированные процессы защищены от вмешательства менее значимых процессов. Преимущества: значительное

снижение рисков заражения вредоносным кодом; увеличение надежности системы в целом.

Журналы событий и аудит (Event Logs & Auditing). Эта подсистема регистрирует события, происходящие в системе, включая события безопасности, ошибки приложений и прочие значимые операции. Она позволяет проводить глубокий анализ происшествий и выявлять возможные угрозы задолго до серьезных последствий. Примеры: аудит неудачных попыток входа в систему; логирование действий с файлами и регистрацией ключей; мониторинг нарушений целостности системы. Преимущества: быстрое реагирование на угрозы благодаря подробному протоколированию; постоянный мониторинг деятельности пользователей и приложений.

Сертификаты и инфраструктура открытого ключа (PKI) основана на использовании цифровых сертификатов для идентификации субъектов и проверки подлинности транзакций. Сертификат подтверждает принадлежность определённого лица владельцу сертификата. Применение: электронная подпись документов; безопасный обмен информацией посредством зашифрованных каналов связи; проверка подлинности веб–ресурсов и клиентов. Преимущества: улучшенная идентификация пользователей и устройств; надёжная защита коммуникаций.

Управление правами на доступ к документам (Rights Management Services, RMS) позволяет устанавливать политику ограничений на доступ к электронным документам, таким как файлы Word, Excel и PDF. После активации документа владелец устанавливает правила, кто имеет право читать, редактировать или печатать документ. Используется для предотвращения несанкционированного копирования и распространения важной информации; установления сроков жизни файла и запретов на дальнейшую передачу третьим лицам. Преимущества: эффективная защита интеллектуальной собственности; минимизация потерь данных вследствие злоупотреблений.

Гипервизоры и изоляция процессов (Hyper–V) позволяет создавать отдельные виртуальные машины, каждая из которых функционирует автономно и независимо от основной системы. Даже если одна виртуальная среда подвергается нападению, остальные остаются незатронутыми. Принципы работы: изоляция каждой виртуальной машины от остальных; защищенность ядра гипервизора, отделённого от пользовательского пространства. Преимущества: возможность тестирования нового программного обеспечения без ущерба для основной системы; устойчивость к сбоям и повышение отказоустойчивости.

Архитектура безопасности Windows включает разнообразные меры, позволяющие организациям и частным пользователям существенно повысить устойчивость своей IT–инфраструктуры к внешним и внутренним угрозам. Правильная настройка и эффективное применение указанных средств создают надежную защитную оболочку вокруг информационных активов предприятия и личной информации конечного пользователя.

Проблемы информационной безопасности требуют постоянного внимания и серьезного отношения со стороны государства. Сегодняшняя ситуация характеризуется высоким уровнем риска и низкой степенью готовности многих государственных структур к возможным атакам. Необходима целенаправленная политика, направленная на усиление информационной безопасности, поддержку отечественных производителей сетевого оборудования и снижение зависимости от иностранных поставщиков.

Ситуационная задача

Министерство цифрового развития Российской Федерации совместно с Правительством Москвы реализует новый национальный проект «Экономика данных и цифровая трансформация государства». Одной из ключевых инициатив проекта является внедрение технологий искусственного интеллекта (ИИ) в деятельность органов государственной власти всех уровней для

повышения эффективности управления и качества предоставляемых услуг населению.

Вы – аналитик отдела внедрения цифровых решений Правительства Республики Башкортостан. Вам поручено разработать концепцию пилотного проекта по внедрению технологии ИИ в один из департаментов городского хозяйства Уфы. Ваша цель – выбрать конкретный департамент, определить направления применения ИИ–технологий и обосновать целесообразность выбранного решения, основываясь на реальных потребностях жителей города и приоритетах национального проекта.

Задание:

Анализ потребностей: Выберите один из городских департаментов, наиболее нуждающихся в цифровизации процессов с использованием ИИ (например, транспорт, ЖКХ, здравоохранение). Обоснуйте выбор, выделив конкретные проблемы, существующие в деятельности департамента.

Разработка концепции: Предложите решение на базе современных технологий ИИ, которое позволит повысить эффективность работы выбранного вами департамента. Опишите предполагаемые выгоды от внедрения вашей инициативы.

Обоснование целесообразности: Оцените потенциальную экономию бюджетных средств, повышение удовлетворенности населения качеством государственных услуг, сокращение сроков обработки запросов и другие возможные эффекты от реализации вашего проекта.

Практическое применение нового национального проекта: Укажите, каким образом ваш проект соответствует целям и задачам национального проекта «Экономика данных и цифровая трансформация государства», приведите аргументы, почему именно ваше предложение целесообразно реализовать в рамках данной программы.

Этап тестирования: Определите этапы тестирования предложенного решения, включая методы оценки результатов пилота и критерии успешности внедрения ИИ–решения.

Критерии оценивания задания:

1. Четкость постановки целей проекта и обоснование выбора конкретного департамента.

2. Глубина анализа существующих проблем и четкое определение направлений применения ИИ.

3. Практическая значимость предлагаемого решения и обоснованная оценка его экономической эффективности.

4. Соответствие цели национального проекта и аргументация важности своего предложения.

5. Структурированность изложения материала и логика построения отчета.

Задания для самостоятельного выполнения

1. Составьте терминологический словарь по проблеме государственного управления в сфере информационной безопасности. Включите в словарь основные термины, касающиеся информационной безопасности в целом, и в государственном управлении, в частности. Приведите соответствующие дефиниции и дайте краткую характеристику терминов.

2. Выполните обзор нормативно–правовой базы информационной безопасности в России. Определите степень достаточности законодательного регулирования в сфере информационной безопасности для осуществления деятельности государственных органов, банковской сферы, промышленности, образования, медицины, частного бизнеса.

3. Выполните обзор институциональной базы информационной безопасности в России. Определите степень охвата информационных угроз,

характер взаимного подчинения, координации и возможного дублирования функциональных обязанностей соответствующих ведомств и министерств по вопросам информационной безопасности.

4. Проведите анализ основных угроз информационной безопасности на основе информации из различных аналитических центров, научных публикаций. Определите пути устранения угроз информационной безопасности в государственном и муниципальном управлении. Приведите пример распространённой информационной угрозы в регионе.

5. Обоснуйте необходимость внедрения цифровых технологий в интересующей вас сфере. Опишите (составьте перечень) проблемы развития этой сферы в РФ, для решения которых необходимо применение цифровых технологий.

Преимущества и ожидаемые результаты от цифровизации этой сферы.

6. Приведите краткое описание текущей практики применения цифровых технологий в интересующей вас сфере (приведите примеры реализованных проектов по цифровизации в этой сфере, оцените уровень применения в этих проектах цифровых технологий. Опишите проблемы, препятствующие цифровизации этой сферы в России.

7. Определите наиболее важные направления развития цифровых технологий в интересующей вас сфере. Сформируйте портфель возможных и реальных цифровых технологий, и решений для этой сферы.

ГЛАВА 2. ПРАКТИЧЕСКИЕ АСПЕКТЫ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

2.1. Цифровые платформы, экосистемы и клиентоцентричность

За последнее время в наиболее доступные и привлекательные рыночные ниши уже проникли и стали там играть главные роли цифровые платформы. Развернулся процесс постепенного прихода цифровой экономики в рынки и индустрии трудоемкие для автоматизации и оцифровки. Эксперты и аналитики сформировали первоначальный корпус знаний по проблемам и вопросам цифровой трансформации, но столкнулись с неминуемостью дополнительно объяснять сосуществование и взаимодействие цифровых платформ, эффекты их технологической и экономической интеграции [57].

Цифровые платформы появляются не только как инструменты продвижения услуг населению (B2C), они возникают и в качестве цифровых площадок между бизнесами (B2B). Так цифровые инвестиционные площадки позволяют инвесторам найти проекты для инвестиций, а производителям услуг привлечь средства для развития бизнеса. Цифровые платформы позволяют легко организовывать сделки с участием трех и более контрагентов, формируя таким образом новые измерения для рыночных отношений. Крупные национальные и транснациональные игроки понимают возможности и перспективы цифровых платформ, и поэтому создают цифровые экосистемы, объединяющие различные цифровые платформы, получая синергию от объединения и обмена разработчиками, технологиями, исследованиями, стартапами.

Перевод предоставления государственных услуг (и деятельности правительств в целом) в цифровой формат традиционно отстает от бизнеса. Чиновники управлению рисками предпочитают безрисковое управление, которое в бизнесе всегда ведет к проигрышу.

Внедрение цифровых технологий – не только высокорискованное занятие, оно требует особых гибких подходов к реализации: ведение проектов с использованием идеологии Agile, венчурное бюджетирование, управление по целям и результатам. А гибкие подходы очень плохо интегрируются с жесткой практикой контроля, финансирования, отчетности. Но, с другой стороны, цифровизация государственной деятельности имеет гораздо большие масштабы, чем у самых крупных корпораций, и в случае успешности проектов способно радикально реформировать экономику, создать существенное преимущество для национального бизнеса [62].

Так, внедрение цифровых платформ в государстве, как отмечено в работе [62] способно решить многие проблемы рынка и стать своего рода информационным инструментом регулирования экономики, подобным советскому Госплану, но не директивному, а рекомендательному. Не случайно аналитики компании Gartner считают задачу создания государственных цифровых платформ, или как они их называют – технологических платформ цифрового правительства (Digital Government Technology Platform, DGTP), основной задачей руководителей, ответственных за цифровизацию правительственных органов. Согласно исследованию Gartner, к 2023 году более 80% внедрений информационных технологий в деятельность правительств, которые не будут основаны на технологической платформе, не смогут решить поставленные задачи.

Согласно концепции Gartner, технологическая платформа цифрового правительства должна интегрировать пять цифровых платформ: платформу опыта граждан (Citizen Experience), экосистемную платформу (интерфейсы и технологии, политики и процедуры взаимодействия граждан и бизнеса с государством), платформу Интернета вещей (собирающую данные), платформу информационной системы (классические корпоративные системы и приложения) и интеллектуальную платформу, обеспечивающую аналитику, роботизированную автоматизацию процессов (RPA) и использование

искусственного интеллекта (ИИ) для обработки данных, включая данные из геоинформационных систем.

Цифровая экосистема – это работающие совместно цифровые платформы. Причем потребитель конкретного блага обращается обычно к одной цифровой платформе, которая запрашивает информацию, функционал или решение задач у других цифровых платформ, выступая неким виртуальным посредником. Клиенту предоставляется единое платформенное решение его запроса на основе нескольких сочлененных специальных информационных систем. Цепочки интеграции различны: комбинированные, множественные, конкурентные. За короткий период, разобравшись с условиями кооперации нового типа, бизнес пришел к автоматизированному контролю издержек и управлению совокупной ценой и ценностью предоставляемого блага. Модели монетизации цифровых платформ прогрессируют и открывают новые, обновляют сложившиеся совмещаемые и альтернативные варианты взаимовыгодных торговых и сервисных сделок для участников [57].

Сам термин «экосистемы» буквально получил второе дыхание, когда стал применяться к сфере цифрового развития экономики. Крупные информационные субъекты некоторых отраслей экономики, в первую очередь оказывающие массовые информационные и финансовые услуги, стали называть себя «цифровыми экосистемами». В первую очередь цифровые экосистемы стали возникать в частном секторе как новая технология рыночного существования, обеспечивающая необходимый уровень масштабирования бизнеса (продуктового, клиентских аудиторий и географического),его оптимизации с точки зрения всех видов издержек, удержания клиентов и обеспечения необходимого уровня конкурентной инновационности товаров и услуг. Цифровую экосистему сегодня определяют также по–разному, подчеркивая различные стороны новой продуктивности функциональной цифровой инфраструктуры с точки зрения задач и целей деятельности организации. Иногда цифровую экосистему определяют как цифровую

платформу, имеющую «некоторые расширения» в иные сферы (отрасли). Иногда говорят о «платформенной экосистеме» как некой «совокупности» (сети) связных платформ (платформенных технологических решений). Сегодня в экономической публицистике под цифровой экосистемой подразумевают консолидацию в единой среде цифровых сервисов и продуктов (производимых традиционно в разных экономических отраслях) в некий «связный» для клиента формат, укладывающийся или в устоявшуюся логику (модель потребления, потребительского поведения, цепочки потребления) и стили жизни (жизненные ситуации).

Экосистема воплощает принципы экономики замкнутого цикла, что является признаком «четвертой промышленной революции, связанного с повышением интегрированности социально–экономического пространства». Экосистемы – это «экономика будущего». Следуя этой же логике, можно предположить, что экосистемная парадигма может быть основой для фактического «расширения» государства при видимом (формальном) сужении его присутствия. При этом «расширение» государства совсем не означает «нового огосударствления» всего и вся, а лишь то, что государство в лице своих институтов и ресурсов находит более «сбалансированную и эффективную позицию» в системе общественных отношений, обеспечивая динамическую устойчивость общественно–экономической конструкции (информационной конструкции общества) в целом. Г. Клейнер предлагает в качестве структуры социально–экономической экосистемы выделить такие внутренние составляющие, как организационная (кластерные системы), инфраструктурная(платформы), бизнес–процессные (сеть), инновационная (бизнес–инкубаторы) или «проектов развития» (которые есть тоже инновации). Внешние составляющие экосистемы: ареал (сектор рыночного пространства) и жизненный цикл. По мнению Г. Клейнера, ключевым моментом экономических экосистем является «не управление ресурсами, а управление правом доступа». Это замечание имеет весьма важное значение для понимания

отличия экосистемы от традиционных форм системной организации экономического и социального пространства. Управление не ресурсами, а правами – это переход на новый уровень философии управления, где оператор экосистемы (экосистемной отрасли) в наименьшей степени ориентирован не на «экосистемное администрирование», но поддержку режимов, которые «автоматически исполняются» при общей согласованности участников экосистемы.

Экосистема очень хорошо вписывается в формат информационной экономики (экономики знания), поскольку она есть «естественная форма (технология) аккумуляции, распространения и приращения знания». Автор работы [62] выделяет следующие интегральные параметры экосистемной парадигмы устройства пространства экономических взаимодействий:

1. Устойчивая локализация экосистемы, что означает наличие отраслевых, географических или технологических границ.

2. Связность пространства экосистемы, в том числе прозрачность и наблюдаемость процессов движение «энергии» (цепочек создания и потребления «ценностей» экосистемы).

3. Некоторая «размытость» границ ареала экосистемы и наличие «переходной полосы» («мембраны»), посредством которой происходит «обмен» с другими системами (экосистемами).

4. Внутренняя уравновешенность (сбалансированность, устойчивость) экосистемы. Преобладание длительных ламинарных процессов над краткосрочными турбулентными состояниями.

5. Коэволюция участников экосистемы как возможность и способность участников экосистемы совместно (синхронно) развиваться (видоизменяться) в процессе создании ценности, поиск сотрудничества с теми, кто выступал ранее в качестве конкурента с целью восполнения недостатка дефицитных для экосистемы (или ее подсистем) «пространственно–временных» и «энергетических» ресурсов.

6. В основе экосистемы всегда лежит ценностное предложение – для всех и для конечного бенефициара (как интегральная ценность, ценностная сублимация). Ценности экосистемы могут иметь различную природу: от материальных и виртуальных объектов до условий, режима, атмосферы, которые ведут к оптимизации затрат участников, инновационных идей и сигналов и пр.

7. Наличие в экономической экосистеме «ключевой (фокальной) фирмы» (ключевой организации), которая выступает в качестве «оператора» экосистемы, отвечает за поддержания ее «правил» и «алгоритмов».

8. Экосистемы имеют «точки», через которые можно оказывать системное воздействие на ее поведение и достигать динамическое равновесие: объем запасов в системе (информации, знаний в том числе), сбалансированность входящего и исходящего объемов вещества, структура запасов и структура потоков (топология каналов), запаздывание в рамках системы, балансирующие циклы(балансирующие контуры) обратной связи (отрицательной и положительной), целевая модель экосистемы, мировоззрение и ее семантическое (смысловое ядро).

9. Экосистемы имеют несколько «горизонтов» воплощения: от семантического и целевого уровня к системно–организационному и далее на уровень технологической инфраструктуры (формы материальной реализации экосистемы).

10. Экосистема выступает в качестве «агрегатора» (ценностного, «продуктового агрегатора»). «Продукт» экосистемы может быть значительно «шире», чем продукты его участников, и быть результатом «динамической сборки» из разных «компонент» и ориентируется на «кластеры потребностей» конечных бенефициаров.

11. Экосистема (экосистемная модель сборки субъектов взаимодействия) есть отражение кибернетической модели системы, в которой гомеостаз при взаимодействии с внешней средой поддерживается за счет управления

балансом «положительных и отрицательных обратных связей». Управление в экосистеме (или управление экосистемой) имеет весьма условные (специфические) параметры, которые не совпадают, в полной мере, с классическими управляющими моделями и технологии в государственном (общественном) секторе. Управление в экосистеме максимально децентрализовано – оно как бы «размыто» в среде «экосистемных» свойств саморегуляциии самоорганизации, которые тем не менее целенаправленно поддерживаются (воспроизводятся) «управляющим оператором» экосистемы. Управление в экосистеме в значительной степени следует понимать в «экономической» коннотации, то есть управление – это взаимовлияние и взаимовыгодное взаимодействие через обмен ценностями, партнерство и коллаборация в формировании и поддержке цепочек (потоков) движение «энергии» в экосистеме. В масштабе всей экосистемы управление – это управление ее состояниями как «динамическими сборками» параметров состояния устойчивости и сбалансированности по всему «объему» размерностей экосистемы (по всем горизонтам) и во взаимосвязи между ними. Управление в экосистеме – это постоянное «вычисление» «уравнения» сбалансированности – гомеостаза. При этом само «управление» с плавающим набором переменных и постоянно меняющимися коэффициентами. Целевая функция экосистемы при этом остается неизменной. Экосистема в своем естественном состоянии всегда выходит на режим «саморегулирования» и «самоуправления», таким образом как бы все время самовоспроизводит себя, аналогично «социально–экономическому генотипу».

Модель управления в экосистеме предполагает наличие «управляющего ядра» (управляющего оператора), которое по своей природе скорее можно определить как «операционное ядро», содержащее (по аналогии с программным кодом) в себе «инструкции» для всех участников по пребыванию и активностям в экосистеме. Управление в экосистеме – это поддержание ее связности, другими словами недопущение (или оперативное устранение) «разрывов»

(divide). Управление в экосистемах это набор правил, описывающих, кто может входить в экосистему, как поделить ценность, как решать конфликты. Управление в экосистеме – это постоянное выравнивание «паттернов» состояний участников экосистемы, потоков и ресурсов, экосистемных цепочек движения «энергии». Ключевой фактор в управлении экосистемы – наличие «центральной фирмы» (в государственном секторе – оператора (регулятора) отрасли), роль которой (особенно на этапе создания экосистемы: ее структуры и «производственных процессов») заключается в налаживании и регулировании связей (коммуникаций), предоставлении набора общих активов, а также проведении политики так называемого выравнивания – политики достижения согласия между членами относительно их позиций в системе и потоков между ними (и доступа к ресурсам и ценностям конечно). В экосистеме на базе общих активов участники могут создавать новые ценности (инновационные продукты – ценности). Но центральная фирма минимизирует риски процесса создания инновационных ценностей. Создание ценностей в экосистеме осуществляется путем проектирования структуры экосистемы, реинжиниринга, реорганизации, реформирования с целью восполнения недостатка дефицитных для экосистем ресурсов.

Цифровая аналитическая платформа будет обрабатывать массивы данных по всему «входящему потоку» и иметь возможность обращаться к связанным данным, расположенным в государственных и негосударственных информационных системах. Основу цифровой аналитической платформы составляет модель данных, которая разрабатывается на основе единой методологии Национальной системы управления данными, что обеспечивает эффективную интеграцию (на уровне данных и процессов) в государственную цифровую среду посредством Единой информационной платформы национальной системы управления данными (ЕИП НСУД) [62].

На единой информационной платформе зарегистрированным представителям органов власти доступен каталог унифицированных и

структурированных описаний государственных данных из разных ведомств. Поиск и предоставление данных для информационного взаимодействия стали проще. Это позволило предоставлять сведения для государственных услуг в режиме реального времени.

Федеральная государственная информационная система «Единая информационная платформа национальной системы управления данными» (ФГИС «ЕИП НСУД») – важный элемент инфраструктуры электронного правительства. Она была создана для систематизации, описания данных и требований к их качеству, а также упрощения информационного обмена между ведомствами.

С помощью ФГИС «ЕИП НСУД» государственные информационные системы получают возможность работать с доступными данными различных ведомств как с единым актуальным и достоверным массивом информации. При этом качество данных автоматически контролируется, а их формат соответствует унифицированным требованиям.

Использование ФГИС «ЕИП НСУД» предусмотрено программами цифровой трансформации и способствует повышению качества управления данными в органах власти.

Создание и развитие ФГИС «ЕИП НСУД» упростило разработку электронных государственных услуг. Благодаря использованию ведомственных витрин данных и СМЭВ 4 необходимые классификаторы, справочники и выписки можно получать в режиме реального времени. Комплексные госуслуги, такие как «Запись на приём к врачу» или «Регистрация транспортного средства», предоставляются быстрее.

В 2024 году произошло ряд изменений в работе ФГИС «ЕИП НСУД», а именно:

- добавлена возможность мониторинга доступности витрин данных;

- обеспечена возможность наблюдения за переводом витрины в промышленную эксплуатацию;

- проведена ревизия каталога данных: сохранены только доступные и актуальные форматы обменов сведениями, удалено более 1500 устаревших объектов;

- переработана и обновлена база знаний [18].

Создание витрин данных – одно из ключевых направлений цифровизации государственных услуг. На витринах размещаются проверенные государственные данные, подготовленные для осуществления межведомственного взаимодействия. Использование органами власти типового программного обеспечения и специализированного сервиса платформы «ГосТех» способствует увеличению доли массовых социально значимых услуг, доступных в электронном виде.

Витрина представляет собой подготовленную онлайн–площадку, где ведомства размещают только те данные, которые необходимы для взаимодействия. При этом нет необходимости предоставлять потребителям данных доступ ко всей информационной системе.

Минцифры разработано специальное программное обеспечение, которое предоставляется участникам взаимодействия бесплатно. С его помощью ведомства создают витрины данных, отвечающие требованиям безопасности и стандартам информационного взаимодействия.

ПО «Витрина данных» поставляется в трёх основных конфигурациях:

1. Лайт – для тестов и работы с простыми регламентированными запросами;

2. Медиум – подходит для большинства сценариев использования, содержит полный комплект модулей ПО;

3. Стандарт – позволяет реализовать максимально возможное количество сценариев использования, подходит для построения сложных архитектурных решений.

Использование этого программного обеспечения позволило запустить популярные государственные услуги с возможностью получения документов в

режиме реального времени. К примеру, стало гораздо проще получить выписку из ЕГРН или записаться к врачу.

Также с 2023 года появилась возможность использовать для создания и размещения витрин данных базовый сервис платформы «ГосТех». Это позволило повысить скорость информационного обмена, поскольку данные и системы, расположенные в рамках единой платформы, стали ближе друг к другу. Использование сервиса «ГосТех» позволяет отказаться от закупки и постоянной загрузки собственных вычислительных мощностей. Теперь витрины данных сразу размещаются в защищённой инфраструктуре, отвечающей всем требованиям.

Далее рассмотрим особенности клиенториентированности и платформенных решений.

Платформенные решения ориентируют на клиента бизнес–модель, воплощенную в цифровых платформах.

Несколько связанных и персонализированных платформенных решений упаковываются в отдельное клиентское предложение в формате цифрового продукта или цифрового сервиса. Это один из вариантов воплотить принцип клиентоориентированности в цифровой экономике.

Базовые свойства цифровых платформ позволяют изучать пользователя и подстраиваться под его нужны. В основе подобной аналитики интенсивный сбор метрик, накапливающий большие объемы данных о клиентах и их поведении. Настолько большие, что потребовалось выделить в отдельный класс технологии для обработки таких объемов. На собираемой о клиентах информации реализуется широкий функционал, предусматривающий автоматизацию. Не только вручную вносятся изменения в настройки платформенного решения. Автоматическая подстройка и конфигурирование осуществляются по результатам сбора и обработки операционных данных о состояниях и поведении пользователя. Не говоря уже об автоматической персонализации или автоматизированной кастомизации цифровых продуктов и

цифровых сервисов, расширяющих существенным образом круг заинтересованных потребителей платформенного решения.

На практике повышение ценности для клиентов благодаря постоянному мониторингу и анализу их профилей и поведения привело к возникновению множества соответствующих подходов, принципов, стандартов, инструментов и технологий.

Среди них, например:

– скоринг – агрегированный учет значимых действий пользователей, выраженный конечным упорядоченным набором специальных расчетных предметных показателей;

– рейтинг – ранжирование пользователей по заданным признакам с применением избранных расчетных показателей, контекста вычислений и решаемой предметной задачи;

– арбитраж – устранение проблем с транзакциями пользователей или спорных ситуаций с использованием контрольных расчетных показателей транзакционного взаимодействия участников;

– геймификация – использование игровых элементов и механик для неигровых действий.

Количество цифровых продуктов и сервисов, продвигающих разнообразные платформенные решения на рынках, постоянно увеличивается по числу и вариантам потребления.

Причем каждое платформенное решение имеет свои особенности и настройки, воплощает принципы и подходы к эффективным коммуникациям с клиентами. Образуется переизбыток предложений на разных рынках, имеющий отчасти негативные последствия. И если среди конкурирующих платформенных решений клиент выбирает какое–либо одно, то среди дополняющих, сопутствующих или совместимых, клиенту не просто предстоит сделать разумный выбор, но и использовать их совместно для решения тех или иных задач и проблем в удобных сценариях.

Переход от осознания того, что платформенное решение должно быть максимально полезным и удобным конечному клиенту к тому, что платформенное решение следует сделать органичной частью полезного, удобного и рационального цифрового пространства клиента – это переход от клиентоориентированности к клиентоцентричности.

Клиентоцентричность, в отличие от клиентоориентированности, предполагает формирование ценностного предложения с учетом той цифровой среды, в которой клиент решает свои задачи и проблемы системно и последовательно. А это означает, что обеспечивается высокое качество собственных цифровых платформ и их интеграции с другими информационными системами разного уровня, обращая внимание на совокупный пользовательский опыт. Тем самым инициируется переход от обособленных цифровых платформ к цифровым экосистемам.

Экосистемы цифровых платформ (экосистемы платформенных решений) – это эффективный ответ на запрос пользователя в части формирования для него удобной и рациональной цифровой среды без дополнительных трудностей при использовании множества цифровых продуктов и цифровых сервисов.

Для пользователя платформенных решений переключение между продуктами и сервисами это новые транзакционные издержки времени и внимания. Поэтому он наверняка предпочтет, если на него не просто будут сориентированы все используемые платформенные решения, а ему предоставят экосистему, в которой со своими потребностями клиент будет в центре общего функционала тесно связанных продуктов и сервисов.

В России цифровые экосистемы только зарождаются. В настоящее время одновременно формируется несколько экосистем и платформ на основе различных отраслей. Для России развитие цифровых рынков, национальных экосистем и платформ может стать не только драйвером экономического роста, но и основой для сохранения экономического и технологического суверенитета.

Рассмотрим некоторые преимущества цифровых экосистем и платформ:

Для гражданина это, прежде всего, бесшовный клиентский путь, широта выбора, привлекательные условия, а также снижение территориальных барьеров

Для бизнеса – доступ к новой клиентской базе по всей территории РФ, удобные бизнес–сервисы (логистика, маркетинг, др.)

Для экономики преимущества заключаются в:

- росте эффективности и прозрачности – исключение неэффективных посредников, рост конкуренции на всех уровнях, снижение уровня асимметрии информации, «обеление» экономики;

- развитии малого и среднего предпринимательства – прибыльность, срок жизни за счет расширения спроса и снижения издержек;

- создании новых и высококвалифицированных рабочих мест;

- привлечении инвестиций в российскую экономику;

- развитие национального венчурного рынка.

Ну и конечно для государства это, прежде всего, обеспечение национальной безопасности – независимость от иностранных экосистем/платформ, предотвращение накопления иностранными экосистемами/платформами важной экономической и иной информации, а также технологическая независимость – инвестиции в наукоемкие отрасли, кросс–отраслевой трансфер технологий.

Однако, следует также и выделить группу рисков, которые возникают в результате развития экосистем/платформ схожи с аналогичными рисками классического бизнеса, но могут иметь свои особенности.

Так, основными группами риска для гражданина является, прежде всего, злоупотребление отношениями с клиентами, навязывание товаров и услуг, недостаток ответственности платформ за конечные продукты и услуги, а также ущемление прав потребителей.

Что касается бизнес–структур, то здесь следует выделить практику недобросовестной конкуренции, которую предстоит уточнить в контексте развития экосистем/платформ.

Для экономики и государства – это кибер–риски, технологические риски и риски безопасности данных клиентов, а также риск снижения конкурентоспособности национальной экономики с учетом трансграничной специфики развития экоситем/платформ.

По данным на начало 2025 года, в России есть несколько крупных экосистем, которые присутствуют в разных вертикалях:

- «Сбер». Есть сервисы в категориях финансов, здоровья и недвижимости.

- «Яндекс». Лидирует в сегменте мобильности («Яндекс Такси»), информации («Яндекс Карты») и голосовых ассистентов («Алиса»).

- VK. Включает социальные сети, почту, облачные технологии, образовательные платформы.

- МТС. Предлагает телекоммуникации, финансовые услуги, медиаконтент, облачные решения.

- Ozon. Включает электронную коммерцию, финтех–услуги, логистику, медиаплатформу.

Таким образом, экосистемы для государственного и муниципального управления – это единое цифровое пространство, которое объединяет модульные информационные системы и сервисы, используемые различными органами власти. Такие экосистемы аккумулируют информацию о разных отраслях экономики, включая строительство, промышленность, транспорт, экологию, образование, здравоохранение и другие.

Вот некоторые элементы экосистем для государственного управления:

1. Конструктор жизненных ситуаций. Цифровой сервис, с помощью которого пользователь может в зависимости от жизненной ситуации самостоятельно определить перечень документов и ведомство, в которое ему необходимо обращаться для получения услуги. Конструктор жизненных

ситуаций позволяет обеспечить снятие административных барьеров и сокращение срока получения государственных и муниципальных услуг в различных сферах: образование, здравоохранение, транспорт и др., путем создания системы приема заявлений на получение государственных и муниципальных услуг с функцией единого окна, оснащенной инструкциями с подробными алгоритмами, методическими указания, содержащими разъяснения о государственных и муниципальных услугах, а также сроках и способах их получения.

2. Цифровая вертикаль строительной отрасли. Она объединяет информационные системы и цифровые сервисы, которые взаимодействуют друг с другом. Это позволяет переводить и хранить все строительные и градостроительные документы в цифровом виде. В таких ИС размещаются различные сведения, документы и материалы об объектах строительства, градостроительном потенциале территорий, развитии территорий, об их застройке и иные необходимые для осуществления градостроительной деятельности сведения.

С помощью ИС осуществляется учет объектов строительства и обмен необходимой строительной и градостроительной информацией как между участниками строительства, так и между органами власти и иными интересантами, а также рассмотрение, согласование, подписание указанной информации.

К строительной и градостроительной информации относятся: схемы территориального планирования, генеральные планы, правила землепользования и застройки, проекты планировок территорий и проекты межевания территорий, результаты инженерных изысканий, проектная, исполнительная и рабочая документация для строительства и реконструкции, разрешение на строительство, уведомление о планируемом строительстве, акты проверок, уведомление об окончании строительства и многое другое [59].

3. Портал государственных услуг. Справочно–информационный портал, который позволяет гражданам и организациям получать информацию о государственных и муниципальных услугах, а также получать их в электронной форме.

Один из примеров экосистемы для государственного управления – платформа «ГосТех». Это облачное платформенное решение для федеральных и региональных органов власти. В основе платформы – домены, которые представляют собой приоритетные направления деятельности государственных органов и юридических лиц. Как отмечено в работе Зуденко С.А. «…Домены можно рассматривать как приоритетные направления, т.е. наиболее широко представленные в региональной практике и значимые для каждой территории. Не случайно набор приоритетных доменов «Здравоохранение», «Наука и образование», «Общественный транспорт», «Строительство и ЖКХ», «Госуправление» согласуется с приоритетными направлениями, указанными в стратегиях цифровой трансформации субъектов Российской Федерации.

Наряду с указанными приоритетными, развитие получат и другие домены, что создает реальные возможности для использования готовых кластеров решений в практической деятельности органов власти в регионах. Использование доменов означает изменение подхода к управлению информационными системами как активами, изменение порядка принятия решений по вопросам развития цифровой инфраструктуры. Более полное раскрытие преимуществ доменного подхода связано с расширением регионального и муниципального участия в вопросах реализации электронного взаимодействия с гражданами и бизнесом путем использования цифровых платформ…» [20].

Также автором выделены основные преимущества использования платформы «ГосТех»:

- снижение времени на разработку и развертывание информационных систем в результате использования общих методологических подходов, типовых решений. Так, оценочно на разработку государственных информационных систем затрачивается от 1,5 до 2 лет, использование возможностей «ГосТех» позволит сократить срок до 3–5 месяцев или нескольких недель применительно к новым сервисам.

- применение отечественных инструментов, методов и технологий для работы с информацией, необходимой органам государственной власти, в том числе решение проблемы безопасности программного обеспечения, и организации взаимодействия между органами власти и обществом [20].

2.2. Практика применения искусственного интеллекта в государственном управлении

Для начала следует определить, что именно относится к искусственному интеллекту (ИИ). Как определено в нормативных документах – «Национальной стратегии развития искусственного интеллекта на период до 2030 года», утверждённой указом Президента Российской Федерации от 10 октября 2019 г. № 490, и в федеральном законе от 24.04.2020 N 123–ФЗ. технологии искусственного интеллекта – «совокупность технологий, включающая в себя компьютерное зрение, обработку естественного языка, распознавание и синтез речи, интеллектуальную поддержку принятия решений и перспективные методы искусственного интеллекта» [40, 42].

Искусственный интеллект (Artificial Intelligence, AI) – комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека [40]. Комплекс технологических решений включает в себя

информационно–коммуникационную инфраструктуру, программное обеспечение (в том числе то, в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений.

В этом определении понимаются следующие свойственные человеку когнитивные функции – это умение рассуждать, обучаться и совершенствоваться на основе предыдущего опыта, решать определенные задачи, взаимодействовать с окружающей средой.

С ИИ тесно связаны следующие понятия.

Машинное обучение (англ. machine learning, ML) – класс методов искусственного интеллекта, характерной чертой которых является не прямое решение задачи, а обучение за счёт применения решений множества сходных задач [19].

Нейронная сеть (Artificial Neural Network – математическая модель (а также её программное или аппаратное воплощение), состоящая из слоев «нейронов», передающих друг другу данные, и построенная по принципу организации и функционирования биологических нейронных сетей [14].

Как видно из определений, ИИ является областью компьютерных наук, которая занимается созданием интеллектуальных систем, способных выполнять задачи, традиционно требующие человеческого интеллекта. Т.е. искусственный интеллект – это название всей области; машинное обучение – это один из разделов ИИ; а нейросети – это один из популярных видов машинного обучения. Для нейросетей используются различные подходы к их построению (архитектура нейросети) и процессу обучения, например, глубокое обучение, обучение с учителем, без учителя. Использование той или иной архитектуры, принципа связано с типами решаемых задач, с возможностью получения первоначальных данных для обучения [58].

Как в других сферах, в последние годы искусственный интеллект находит всё более широкое применение в госуправлении.

Отметим, что искусственный интеллект в госсекторе распространяется не стихийно. Государственная регуляторная и методологическая политика в сфере разработки, внедрения и использования ИИ в нашей стране имеет четкую структуру и определенную гибкость. Ведутся работы над развитием тематики в федеральном проекте «Искусственный интеллект». Он начинался как подчинённый проект национальный программы «Цифровая экономика» (2019–2024). Сейчас федеральный проект получил расширение и развитие в рамках национальной программы «Экономика данных» (2025–2030) [21].

Важный ряд особых требований со стороны органов власти – размещение систем ИИ внутри собственной инфраструктуры, повышенное внимание к требованиям информационной безопасности, расширенный список оснований для применения новых технологий (не только финансовых). В документах и практике госсектора можно увидеть такие параметры:

- ART (Average Resolution Time) – среднее время обслуживания клиента
- CES (Customer Effort Score) – индекс клиентских усилий
- NPS (Net Promoter Score – индекс определения приверженности / готовности рекомендовать сервис)
- CSI (Customer Satisfaction Index) – уровень удовлетворенности пользователей, включая доступность формы, среднее время заполнения формы на ЕПГУ, удобство оказания услуги
- Доля незаконченных заявлений
- Среднее время заполнения формы на ЕПГУ
- Учет личных обстоятельств (для предоставления индивидуального пакета сервисов)
- Комплексность предоставления услуг в зависимости от жизненной (бизнес–) ситуации клиента.

Также органы власти обращают внимание на нахождение решения в реестре российского ПО.

Заметен искренний интерес к теме со стороны сотрудников органов власти – как функциональных заказчиков, так и «цифровиков». Кажется, что тема ИИ позволяет проявлять творческое начало, создавать что–то совсем новое. Это желание подкрепляется крайне высокой квалификацией «цифровиков» госсектора.

Важно также отметить, что сам по себе ИИ зачастую является добавкой к большим приложениям. Поэтому идеи по внедрению ИИ в госсекторе часто возникают после анализа существующих систем, углубления в конкретную предметную область, с одной стороны, и знания возможностей новых технологий с другой.

Технологии ИИ в конкретных приложениях для госсектора применяются уже несколько лет: например, компьютерное зрение или обработка естественного языка. Поэтому существуют готовые приложения или решения, которые заняли свои ниши. Повышенный интерес к ИИ позволяет сейчас вендорам обращать внимание на свои предложения.

В 2024 году на рынке были очень заметны специализированные ИИ–вендоры. Иногда им трудновато мыслить в категориях государственных систем даже при наличии великолепных кейсов в госсекторе. Зато у них есть широкая палитра собственных приложений, накоплен опыт в коммерческом секторе.

Становится очевидно, что ИИ для госсектора – это не про увольнение сотрудников, а про кардинальное повышение качества и увеличение объёма выполняемой работы. Лучше всего это видно при формулировании полезных ответов на обращения граждан [21].

В современном информационном обществе в ускоренном темпе проявляет себя «экономика данных», а потенциальная ценность ИИ заключается в обработке огромного массива информации для подготовки соответствующих документов или принятия управленческих решений. С позиции органов государственной власти проблематика внедрения

искусственного интеллекта в основные процессы остается актуальной. В связи с ростом информационного потока из внешней среды требуется увеличение количества штатной численности персонала с соответствующими компетенциями для обработки такой информации или, как альтернатива – внедрение автоматизации процессов на основе ИИ для повышения качества государственного управления.

Внедрение ИИ в основные процессы государственного управления имеет двойственную составляющую. С одной стороны ИИ может обеспечить производительность, оперативность и, самое главное, прозрачность государственных органов власти. С другой стороны, необходимо учесть и потенциальные риски, связанные с безопасностью граждан в случае появления нестандартных алгоритмов и решений, которые в последующем могут принести вред государству в целом. Так, опираясь на основные положения механистической философии, которая была популярна в XVI – XVII веках Рене Декарт в своих трудах отметил, что «…если живой организм функционирует подобно сложному механизму, следовательно, должна быть возможность создать рукотворную копию такого организма…» [7]. Таким образом формируется серьезная научная проблема, которая заключается в определении того какую же роль органы государственной власти должны играть в частности как разработчики, пользователи или регулирующие органы. Противоречие явно проявляется в том, что ИИ способен улучшить систему управления процессами в широком спектре предоставления государственных услуг и в данном случае органы власти становятся пользователями ИИ, но, в то же время органы власти осознают необходимость управления ИИ в государственном секторе для предотвращения злоупотреблений и снижения рисков некорректного использования данных.

Относительно внешнего вызова по внедрению ИИ в основные процессы органов государственной власти в современной России существенную роль играет Министерство цифрового развития, связи и массовых коммуникаций.

В рамках проведения круглого стола по проблемам цифровой трансформации в органах власти [22] были определены ключевые барьеры, а также предложены направления внедрения решений на базе ИИ. Среди барьеров можно выделить: дефицит финансирования, отсутствие развитой инфраструктуры, а также недостаток профессиональных компетенций государственных служащих, которые способны выполнять задачи с позиции постановщиков задач, подбора данных, использования сервисов ИИ и реализация функций контроля обозначенной системы.

Относительно решения задачи по кадровому обеспечению Министерство цифрового развития, связи и массовых коммуникаций считает необходимым предоставить доступ всем субъектам РФ, которые активно работают в направлении внедрения ИИ, с целью использования цифровой платформы «Гостеха» [1], которая позволяет проводить оценку привлекаемых разработчиков и пользователей ИИ в основных процессах органа государственной власти.

Существенную проблему в процессах внедрения ИИ в органах государственной власти следует рассматривать в контексте открытия доступа для информации (больших данных). Такая информация становится основой для обучающих алгоритмов и моделей ИИ. В большинстве случаев отдельные данные не имеют цифровой формы или хранятся не системно, разрозненно. В данном случае уходит очень много времени на поиск достоверной информации, необходимой для обучения модели ИИ. Поэтому важно с подачи федерального центра от профильных министерств создавать совместно наборы данных и, в последующем, передавать данные разработчикам на уровне регионов, что значительно снизит потери времени на обработку данных и их полноценное использование ИИ.

Если проанализировать практический аспект внедрения ИИ, то он происходит фрагментарно на федеральном уровне, не говоря уже о муниципальном. Так, например, Сахалинская область внедряет ИИ в процессы

развития территорий данного региона. В данном случае Министерство архитектуры и градостроительства Сахалинской области заключило соглашение о сотрудничестве с Rocket Group. Эта компания является одной из ведущих российских разработчиков rTIM на базе генерированного искусственного интеллекта [50]. Это сотрудничество только стартует, но по прогнозам самих государственных служащих это позволит региону более чем в 3 раза ускорить процессы мастер–планирования с учетом того, что имеется дефицит кадров в данной сфере. «…Региональное правительство с помощью платформы rTIM получит возможность очень быстро генерировать десятки концепций мастер–планов, проверять гипотезы наиболее эффективного экономического развития территорий, проводить экономическую оценку участков и мгновенно реагировать на изменения, не теряя драгоценное время. Это позволит региону быстро и эффективно готовить необходимую документацию для подготовки новых инвестиционных проектов…» [50].

Для г. Москва перспективным стал проект внедрения ИИ–системы для проверки ошибок при перечислении средств из бюджета. В данном случае Департамент финансов г. Москвы стал первым в России, кто внедрил ИИ для автоматизированной проверки платежных документов, связанных с перечислением средств из городского бюджета. Новая система позволяет значительно сократить время обработки данных и повысить точность выявления ошибок, что способствует повышению эффективности работы городских финансовых структур [30].

Рассматривая тенденции, которые реализует правительство Ямало–Ненецкого автономного округа (ЯНАО) в сфере внедрения ИИ, следует выделить проекты, основанные на сотрудничестве с профильными крупными организациями, которые уже имеют существенный опыт внедрения ИИ на данной территории. Так, совместно с Ассоциацией разработчиков и пользователей искусственного интеллекта в медицине «Национальная база

медицинских знаний» (НБМЗ) реализуют проект «Внедрение систем искусственного интеллекта для медицины» [10].

Предпосылки сотрудничества со Сбербанком в части внедрения ИИ в органы государственной власти были заложены Президентом Российской Федерации на конференции «Путешествие в мир искусственного интеллекта» [24], где было озвучено поручение относительно проведения Сбербанком стратегических сессий с каждым субъектом РФ по возможностям применения ИИ. В результате в 2024 году Сбербанком были отобраны 55 проектов применения искусственного интеллекта в органах государственной власти. Такие проекты позволят снизить часть издержек, и, рассматривая перспективы, позволят, без привлечения сторонних специалистов, «закрыть» ряд ИТ–решений, необходимых для внедрения ИИ.

Важно понимать, что для внедрения проектов развития ИИ необходима и соответствующая кадровая составляющая. С целью решения этой задачи Сбербанком были проведены обучающие курсы по ИИ для представителей правительства ЯНАО, имеющих отношение к принятию решений о необходимости технологии в том или ином сегменте.

Такой подход к процессам внедрения становится наиболее приемлемым и становится основой формирующегося механизма внедрения ИИ в основные процессы государственных органов власти.

Еще одним удачным примером внедрения ИИ в ЯНАО – это проект «Осторожно медведь». Такой проект очень актуален для ряда населенных пунктов, учитывая специфику региона, где наблюдается высокая активность диких животных. Суть проекта заключается в том, что с помощью видеокамер, подключенных к ИИ с функцией распознавания нужных объектов (компьютерное зрение), органы власти и соответствующие службы оперативно получают информацию о приближении к населенному пункту медведей, что позволяет вовремя принять соответствующие меры и оповестить жителей.

Основной сложностью для реализации этого проекта является ведение базы данных медведей для обучения модели ИИ.

Использование «компьютерного зрения» также помогает оценивать уровень загруженности разных объектов (объектов спортивной инфраструктуры, магистральных дорог, дорог общественного пользования и т.д.). По состоянию на апрель 2024 года в ЯНАО установлено более 4 тысяч камер видеонаблюдения. Внедрение ИИ позволило оценить эффективность работы видеокамер. Так, например, установленная видеокамера, по разным причинам, могла быть направлена не на объекты фиксации (массовое скопление людей), а в другую сторону. В результате внедрения корректировок ИИ, настроенный под различные сценарии, отслеживает «правильность» компьютерного зрения, то есть получение «нужной картинки».

Данный опыт был заимствован у г. Москвы, то есть наблюдается преемственность использования данной технологии.

Также, на наш взгляд, интересен опыт ЯНАО в части внедрения ИИ в процессы, связанные с обращениями граждан. Так, получив обращение, ИИ анализирует текст и сразу «подсвечивает» ключевой смысл обращения. При чем, изучается и полный текст обращения, и его краткое содержание. Отмечается, что «попадание» ИИ очень высокое, что в дальнейшем даст возможность экономить время госслужащих.

Еще одним интересным примером стало использование технологий GPT (generative pre–trained transformer) с российской языковой моделью на портале «Госуслуги», а также оказание государственных услуг с помощью голосовых колонок «Алиса» и «Маруся».

Еще одним направлением внедрения ИИ можно выделить сферу культуры. Так, на основании Распоряжения Правительства РФ №3550–р от 11.12.2023 внедрение ИИ предусмотрено по шести проектам: «Сервис ГОСБилет», «Единый читательский билет», «Цифровой культурный профиль»,

«Культурный регион, типовое облачное решение», «Интерактивные культурные помощники», «Домен «Культура» [55].

В экономику Республики Башкортостан также активно внедряют технологии искусственного интеллекта, которые используются в различных сферах и в разнообразных формах в соответствии с задачами национального проекта «Цифровая экономика».

Согласно аналитическому докладу Национального центра развития искусственного интеллекта при Правительстве России по итогам прошлого года республика находится на 5–м месте по обеспеченности кадрами для развития и использования этой технологии. Также 5–ую позицию Башкортостан занимает по использованию искусственного интеллекта в региональных системах государственного сектора. При этом практически все решения – отечественные.

«…Искусственный интеллект имеет огромный потенциал для улучшения многих аспектов государственного управления и может стать важным инструментом для повышения эффективности госсектора и качества услуг, предоставляемых нашим гражданам…», – отметил исполняющий обязанности Премьер–министра Правительства Башкортостана Андрей Назаров [23].

Наряду с внедрением традиционных систем искусственного интеллекта открылись новые направления, позволяющие существенно увеличить производительность труда и повысить эффективность деятельности госорганов, добиться положительных социальных эффектов. В Башкортостане искусственный интеллект активно используется в разнообразных формах, включая голосовых помощников, камеры видеонаблюдения и компьютерное зрение.

С конца 2023 года внедрен голосовой помощник на едином номере «122» контакт–центра Министерства здравоохранения республики с 9 различными сценариями. За 10 месяцев текущего года по данной линии поступило почти три миллиона звонков из них 25% обработал робот.

«…Искусственный интеллект активно применяется на дорогах республики для обеспечения транспортной безопасности. Запущенная в 2020 году комплексная система интеллектуального видеонаблюдения насчитывает 1000 камер, которая включает в себя функцию распознавания лиц, детектора дыма и огня, определение скопления людей, заезда и парковки автомобилей на газоны, оставленных предметов…», – прокомментировал и.о. министра цифрового развития государственного управления Республики Башкортостан Геннадий Разумикин [23].

Реализации проектов внедрения ИИ способствует такая мера поддержки как гранты. Благодаря этому уфимская IT–компания смогла запустить пилотный проект программно–аппаратного комплекса интеллектуальной системы контроля эффективного потребления корма для крупного рогатого скота в сельхозпредприятии Аургазинского района. Решение продемонстрировало снижение потерь корма более чем в полтора раза.

С 2025 года начнется реализация национального проекта «Экономика данных», в том числе проекта «Искусственный интеллект». Одним из ключевых мероприятий проекта «Искусственный интеллект» станет создание, наполнение и обеспечение возможности доступа к централизованной государственной инфраструктуре данных.

Также следует отметить, что в 2025 году продолжится реализация развития инфраструктуры связи в Башкортостане, запущен новый инструмент – Инвестиционный налоговый вычет. Правительством Республики Башкортостан уже заключено соглашение с ПАО «Мобильные ТелеСистемы», которым ведутся работы по созданию инфраструктуры связи на участке автодороги Архангельское – Инзер. Связь обеспечена в деревнях Тереклы и Усаклы Архангельского района Республики. Всего в 2024 году введены в эксплуатацию 6 базовых станций на участке от с. Архангельское до с. Кулмас Белорецкого района. В 2025 году будет запущено 5 базовых станций до с. Инзер. Второй

этап – это создание инфраструктуры связи на участке автодороги «Инзер – Белорецк» в период с 2026 по 2027 годы.

Не остаются без внимания сервисы для граждан. В планах – реализация и наполнение единого электронного реестра граждан республики, в котором будут содержаться данные о разных категориях граждан, что позволит оказывать услуги онлайн в проактивном режиме.

Министерство цифры планирует создать витрину данных по льготным категориям граждан, имеющих право на бесплатный проезд по карте АЛГА, разработать 25 региональных услуг на федеральном портале госуслуг и завершить пилот по разработке социальных услуг на платформе ГОСТЕХ. Важная задача на 2025 год – повышение доли граждан, обращающихся за услугами в электронном виде с 95,3% до 97%.

В помощь ИТ–отрасли внесены поправки в законодательство республики о получении налоговых мер поддержки для эффективного ведения деятельности. Также появилась возможность включать компании в республиканский реестр, выписка из которого позволяет существенно упростить процедуру получения госаккредитации. Для удобства запущена соответствующая услуга на региональном портале госуслуг. В Республике Башкортостан созданы условия для оказания комплексной поддержки предприятиям региона. Общий объем привлеченных средств из федеральных источников за несколько лет составил порядка 6,4 млрд рублей [9].

Отметим, что для разработки единого механизма внедрения ИИ в органы государственной власти через государственные компании стимулирует такое внедрение в контексте соответствующей стратегии цифровой трансформации по таким приоритетам как:

1. Реализация государственных услуг, которые позволяют любому пользователю получить приемлемый ответ на конкретные вопросы.

2. Проектирование территориального развития с ориентиром на развитие социальной среды, то есть обоснование строительства новых,

дошкольных учреждений, школ и учреждений здравоохранения с учетом плотности населения и инфраструктурного обеспечения.

3. Внедрение в процессы диагностики алгоритмов распознавания заболеваний.

4. Мониторинг спутниковых снимков для выявления мест незаконной вырубки леса, не эффективного использования сельскохозяйственных земель, фиксация незарегистрированных объектов недвижимости и пр. Также ключевым моментом является анализ видеонаблюдения для фиксации возгорания в лесах, сельскохозяйственных землях, а также мониторинг и выявление передвижения диких животных в близи населенных пунктов.

5. Наблюдение за погодой и ее прогнозирование развития.

Однако, одним из барьеров, препятствующих внедрению ИИ в основные процессы является политический контекст. Так, большинство руководящего состава органов государственной власти скептически относятся к принятию решений полностью системой ИИ. Так, в г.Москва сложилась «традиционная система управления», которая основана на потребностях жителей. Она нацелена на то, чтобы человек в городе чувствовал себя комфортно, безопасно, получал услуги высокого качества. Для этого «…не нужно ни искусственного интеллекта, ни каких–то больших теорий…» [22], отмечают в своих выступлениях высший руководящий сосав органов государственной власти. При этом в городе действует множество элементов электронного правительства, информационных потоков, обработки данных, но это вспомогательные механизмы, которые позволяют госслужащему более эффективно принимать решения. Так, целеполагание в государственном управлении является политическим процессом: высшее руководство страны ставит ключевые цели. А дальше начинается процесс достижения этих целей – того, чем у нас в стране занимается правительство, и это более технологичный процесс.

Однако сторонники внедрения ИИ и передачи ему возможности принимать решение утверждают о том, что важно правильно поставить цель перед ИИ. Например, если поставить задачу справедливого распределения средств, то лучше искусственного интеллекта этого никто не сделает, потому что там будет честный подход и не будет человеческого влияния и предпочтений.

В соответствии с распоряжением Правительства РФ [37] определена дорожная карта «Развитие высокотехнологичного направления «Искусственный интеллект» на период до 2030 года», в рамках которой на проверку ИИ–зрелости ведомств планируется выделить более 45 млн рублей до конца 2024 года. Это еще один из системных решений, способствующих оценить ситуацию в регионах и выработать последовательное внедрение ИИ в основные процессы государственного управления с учетом развития соответствующего инфраструктурного обеспечения на местах.

Одним из рациональных решений Правительства РФ стало передача контроля над внедрением ИИ в госсектор и в отрасли экономики Высшей школе экономики (НИУ ВШЭ). На базе этого вуза функционирует Национальный центр развития искусственного интеллекта [34]. По сути это площадка для отбора ИИ–решений для бизнеса, науки и государства, заняться экспертизой документов о регулировании этой сферы, а также экспертным сопровождением внедрения ИИ в госуправлении и в секторах экономики.

Также следует рассматривать следующий этап внедрения ИИ на основе повышения квалификации соответствующих специалистов, способных обеспечивать модели ИИ соответствующими базами данных и обеспечивать безопасность функционирования системы.

Таким образом, исходя из анализа процессов внедрения, ответственное использование искусственного интеллекта может улучшить функционирование государственных органов несколькими способами.

Во–первых, использование ИИ в государственном секторе может помочь правительствам повысить производительность за счет более эффективных внутренних операций и государственной политики.

Во–вторых, ИИ может помочь сделать разработку и реализацию государственной политики и услуг более инклюзивными и отвечающими меняющимся потребностям граждан и конкретных сообществ.

В–третьих, искусственный интеллект может усилить подотчетность правительств за счет расширения их возможностей в области надзора и поддержки независимых надзорных институтов.

Несмотря на потенциальные преимущества ИИ, растет обеспокоенность по поводу рисков, связанных с фрагментарным и неконтролируемым внедрением ИИ в государственном секторе. К таким рискам относятся усиление предвзятости, отсутствие прозрачности в разработке системы и нарушения конфиденциальности и безопасности данных – все это может привести к несправедливым и дискриминационным результатам с серьезными последствиями для общества.

Еще одним из барьеров для внедрения ИИ в условиях цифровой трансформации экономики РФ становится дефицит квалифицированных кадров, второй барьер – это неразвитость инфраструктуры (техническая оснащенность, настройка программного комплекса и прочие аспекты, связанные с функционированием больших данных). Следовательно, ожидать одинакового подхода к внедрению ИИ в регионах в ближайшее время не стоит. Следует выбрать индивидуальный подход и масштабировать практики, которые уникальны для отдельных регионов, а отдельные практики применять системно на государственном уровне с привлечением крупных предприятий, заинтересованных в совместном развитии, такие как Сбербанк, Национальный центр развития искусственного интеллекта при Правительстве Российской Федерации, Rocket Group.

Поэтому на современном этапе, на государственном уровне важно определиться в какие процессы внедрять новую технологию. И в данной статье эти направления, в принципе, определены исходя из опыта внедрения ИИ в различных регионах и сферах: предоставление госуслуг, планирование территориального развития, медицинская диагностика, анализ спутниковых снимков, наблюдение за погодой, анализ данных видеонаблюдения. Специалистам мало обучиться генерировать картинки и тексты, но применять новейшие разработки в своих бизнес–процессах бывает чрезвычайно сложно. Для чего важно системно подходить к вопросам подготовки таких специалистов в рамках высшего образования и системы ДПО.

2.3. Цифровой маркетинг и аналитика в государственном управлении

Современный этап эволюции государства и государственного управления характеризуется переходом к электронному правительству, развитием механизмов оказания государственных услуг в режиме онлайн, использованием больших объемов данных для выработки стратегических решений. Необходимость интеграции новых подходов в государственном маркетинге обусловлена стремительным ростом роли информационных технологий в жизни общества, что ставит перед органами власти серьезные вызовы и открывает значительные перспективы.

Государственный цифровой маркетинг отличается рядом специфических черт по сравнению с традиционным бизнес–подходом. Во–первых, основными действующими лицами выступают учреждения публичной власти, преследующие социально ориентированные цели, а не стремление максимизировать прибыль. Во–вторых, целевая аудитория состоит преимущественно из граждан, представителей малого и среднего бизнеса, общественных объединений и иных субъектов гражданского общества, имеющих право требовать прозрачности и доступности информации.

Есть примеры успешной реализации государственного цифрового маркетинга. Министерство здравоохранения Российской Федерации активно ведёт официальные страницы в популярных социальных сетях («ВКонтакте», Telegram), оперативно публикует важную информацию, доступную широким слоям населения. Новости регулярно обновляются, модераторы оперативно реагируют на события, публикуются разъяснительные статьи. Ведётся оперативное консультирование граждан по вопросам здоровья, работают интерактивные сервисы по информированию и профилактике заболеваний.

Федеральная налоговая служба России предлагает гражданам удобные цифровые инструменты, среди которых выделяются следующие инновационные решения: личный кабинет налогоплательщика, позволяющий отслеживать налоги и оплачивать счета онлайн; чат–боты, обеспечивающие круглосуточную консультацию по вопросам налогообложения; сервис обратной связи, облегчающий взаимодействие граждан с налоговой службой.

Официальный сайт социального фонда Российской Федерации отличается высокой степенью удобства и простоты пользования: персонализированные уведомления о состоянии пенсионных накоплений; возможность подачи заявлений и документов через портал госуслуг; высокий уровень прозрачности процедур начисления пенсий и выплат пособий.

Наиболее эффективными инструментами цифрового маркетинга оказались социальные сети и мобильные приложения. Они позволяют быстро доставлять актуальную информацию широкой аудитории, формировать доверие и повышать лояльность граждан. Внедрение голосовых помощников и чат–ботов позволяет повысить скорость обработки запросов и уменьшить нагрузку на операторов контакт–центров. Привлекательный дизайн и удобство интерфейсов повышает удовлетворенность пользователей и способствует лучшему восприятию информации. Российские государственные органы демонстрируют значительные успехи в области цифровой трансформации и

организации эффективной маркетинговой деятельности, ориентированной на повышение уровня комфорта и удобства жизни граждан.

Государственный маркетинг охватывает деятельность органов власти по продвижению своей политики, программ и услуг среди граждан, организаций и международных партнёров с целью формирования позитивного имиджа страны и укрепления общественного доверия к власти и государству. Применение инструментов цифрового маркетинга помогает государству стать ближе к населению, делает процессы управления более открытыми и понятными. Когда граждане видят открытость и готовность власти к диалогу, уровень доверия населения к власти повышается, что способствует улучшению общей атмосферы сотрудничества общества и государства.

Цифровое управление и государственный маркетинг тесно переплетены между собой благодаря общему подходу к использованию технологий и методов привлечения внимания граждан, повышению уровня вовлеченности и удовлетворённости населения от взаимодействий с государством. Под цифровым государственным управлением понимают использование информационных и коммуникационных технологий для повышения эффективности предоставления государственных услуг, совершенствования управленческих процессов и усиления обратной связи с обществом. Успешность перехода к цифровому управлению зависит от ряда факторов, включая наличие квалифицированных кадров, технологической инфраструктуры, правовых норм и культурной готовности граждан (общества) к новым формам общения с властью.

Важную роль в государственном управлении играет также стратегическое планирование, направленное на создание целостной экосистемы цифровых услуг, охватывающих все важные сферы жизнедеятельности общества, бизнеса и государства. Эффективность мероприятий по государственному маркетингу, по работе с целевой аудиторией (гражданами) в нужное время и в нужном месте, измеряется: уровнем вовлеченности граждан; повышением уровня

лояльности к государственной власти всех уровней; улучшением общего позитивного восприятия органов власти, правительства; повышением значимости государственных цифровых услуг для граждан.

Цифровой маркетинг открывает широкие перспективы для любого бизнеса или услуги, независимо от размера и сферы деятельности. Умение управленцев грамотно применять современные инструменты и данные аналитики поможет вывести компанию (ведомство) на новый качественный уровень, повысив её экономическую (бюджетную) эффективность.

Госсектор является одним из наиболее развитых в цифровом отношении сфер России. В управлении страной задействованы информационно–аналитические системы, благодаря которым процессы государственного управления становятся более быстрыми, безопасными и контролируемыми. Множество услуг для бизнеса и граждан оказываются в электронном виде. Аналитика данных, которыми оперируют госструктуры, позволяет объективно оценивать деятельность ведомств, эффективность реализуемых проектов и качество оказываемых услуг, оперативно выявлять проблемы и находить оптимальные способы их устранения, заниматься прогнозированием [4].

Таким образом, государственное управление и цифровой маркетинг тесно взаимосвязаны, хотя, на первый взгляд, кажутся совершенно разными и далёкими друг от друга областями деятельности. У них имеются общие элементы – цифровые технологии, которые сегодня активно внедряются в государственное управление для повышения эффективности взаимодействия государства с гражданами (обществом). Например, портал «госуслуги» позволяет получать государственные услуги онлайн, такие как оформление документов, запись на приём к врачу, уплата налогов и штрафов. Это пример цифрового маркетинга через привлечение пользователей удобством, доступностью цифровых государственных услуг. В нынешнее время, государство широко применяет инструменты цифрового маркетинга для

информирования населения о важных инициативах, законах, мероприятиях. И, это всё работает весьма эффективно, является перспективным и значимым.

Социальные сети используются министерствами и ведомствами для распространения важных новостей, продвижения кампаний вакцинации, экологической осведомленности и другие общественно значимые темы. Оба оговоренных направления используют большие данные для анализа поведения целевой аудитории и оптимизации процессов. Государство собирает и обрабатывает большие объемы данных о гражданах для улучшения качества услуг, принятия решений в области здравоохранения, образования, транспорта и безопасности. Таким же образом цифровой маркетинг изучает поведение потребителей, чтобы предложить наиболее релевантные продукты и услуги.

На сегодняшний день цифровая среда становится ключевым каналом профессионального взаимодействия между сотрудниками предприятий и организаций, между компаниями и их потребителями, между гражданами и государством. Современные цифровые технологии предоставляют бизнесу и власти новые возможности для взаимодействия с населением. Однако использование инструментов цифрового маркетинга требует от заинтересованных лиц глубоких знаний и понимания особенностей виртуального пространства. В этой связи становятся актуальными систематизированные знания о принципах и инструментах современного цифрового маркетинга, о потенциале веб–аналитики, о возможностях оптимизации маркетинговых усилий для достижения целей управления.

Цифровой маркетинг, являясь инструментом бизнеса, предназначенным для продвижения товаров и услуг в цифровой среде, сегодня успешно применяется в государственном управлении. Цифровой маркетинг представляет собой совокупность способов коммуникации бренда (услуг) с целевой аудиторией посредством цифровых платформ и каналов. Ключевыми инструментами являются социальные сети, поисковая оптимизация, контент–маркетинг, email–маркетинг, таргетированная реклама.

Каждый из инструментов позволяет эффективно взаимодействовать с потенциальными клиентами, создавать узнаваемость бренда (услуг) и повышать продвижение среди потребителей (граждан). Преимущества цифрового маркетинга состоят в следующем: масштабируемость и глобальность охвата аудитории; возможность персонализации предложений товаров и услуг; точное измерение результатов кампаний по продвижению и быстрая обратная связь от клиентов; оптимальное соотношение затрат на продвижение товаров и услуг, полученного экономического эффекта.

Контент–маркетинг направлен на привлечение потребителей путём предоставления полезного и интересного контента интернет сайтов. Форматы контента разнообразны: статьи, блоги, видеоролики, инфографика, кейсы и другое. Правильно организованный и адресно представленный контент привлекает внимание потребителей, повышает доверие к бренду (услуге) и улучшает позиции соответствующего сайта в поисковых системах.

Поисковая оптимизация (SEO) направлена на повышение позиций сайта в результатах выдачи поисковых систем. Грамотная SEO–стратегия включает внутреннюю оптимизацию сайта, построение ссылок, улучшение поведенческих факторов и своевременное востребованное обновление контента. Чем выше позиция сайта в поиске, тем больше посетителей и потенциальных клиентов получает бренд (услуга).

Таргетированная реклама направлена исключительно на определенную аудиторию. Платформы социальных сетей, поисковиков и видео ресурсов предлагают инструменты для точной настройки рекламных объявлений по интересам, демографическим признакам, поведению и другим параметрам. Такая точность позволяет повысить эффективность инвестиций в рекламу.

Email–маркетинг основан на отправке электронных писем подписчикам. Этот канал эффективен для постоянных пользователей услуг, для повторных кампаний, информирования об изменениях в номенклатуре, укрепления

лояльности клиентов. Важно также учесть качество контента электронного письма и соблюдение правил анти–спама.

Социальные платформы становятся действенным инструментом формирования репутации бренда (услуги) и непосредственного общения с пользователями. Публикация интересных постов, ведение страниц брендов (услуг), проведение конкурсов и акций помогает привлечь внимание и стимулировать лояльность среди подписчиков.

Веб–аналитика является основой для принятия решений в цифровом маркетинге. Для успешного ведения цифрового маркетинга важно уметь анализировать поведение пользователей на сайте и оценивать эффективность проведенных кампаний. Основные цели веб–аналитики состоят в следующем: определение источников трафика; изучение характеристик посетителей (демография, интересы, устройства); анализ пути покупателя и выявление барьеров; выявление наиболее эффективных каналов привлечения клиентов; повышение коэффициента конверсии.

Коэффициент конверсии – это процент посетителей, которые выполняют желаемое действие на веб–сайте, например, получают ту или иную государственную услугу. Высокий коэффициент конверсии указывает на то, что веб–сайт эффективен. Чтобы улучшить коэффициенты конверсии, компании могут оптимизировать дизайн и содержание веб–сайта, упростить процесс навигации и использовать целевые маркетинговые кампании.

В аспекте государственного цифрового маркетинга понимание поведения и предпочтений граждан имеет первостепенное значение. В заданном контексте, веб–аналитика становится важнейшим инструментом.

Современные инструменты веб–аналитики, такие как Google Analytics, Яндекс Метрика, Adobe Analytics и другие, позволяют собирать большое количество данных и превращать их в полезные метрики и отчёты. Благодаря таким данным компания (ведомство) сможет принять обоснованные решения

относительно стратегии дальнейшего развития своего присутствия в интернете в виде цифровых услуг или электронной коммерции.

Хорошим примером комплексного использования аналитики в государственном секторе являются ситуационные центры, куда поступают и где обрабатываются показатели из различных государственных информационных систем, а также от операторов связи, из социальных сетей и других источников. Так контролирующие органы получают оперативную информацию об экономическом и социальном развитии страны, региона или конкретного муниципалитета. Широкое распространение в государственном управлении получила концепция витрин данных – масштабных аналитических хранилищ, которые содержат структурированные выборки данных из той или иной области и способны предоставлять соответствующую информацию по запросам пользователей. Такие витрины внедрены на уровне региональных органов исполнительной власти, а также отдельных ведомств – Росреестра, Федерального казначейства и других [3].

Большие данные (Big Data) представляют собой гигантские объёмы оцифрованной, многообразной и непрерывно увеличивающейся информации с различной степенью структурированности, для работы с которой необходимы специальные инструменты и технологии, а также вычислительные мощности и хранилища. Однако данные сами по себе не являются конечной целью, они требуют обработки и анализа. Аналитика больших данных (Big Data Analytics) – процесс, включающий в себя сбор, очистку, преобразование некоторого набора данных в полезные знания в целях выявления скрытых тенденций. На основе всестороннего анализа данных можно сформулировать выводы, прогнозировать развитие событий, принимать более взвешенные управленческие решения, предлагать стратегии, снижать риски и повышать конкурентоспособность [4].

Государство – один из крупнейших владельцев данных, который не только собирает их сам, но ещё и аккумулирует полученную информацию от

других поставщиков. Однако эти данные в госсегменте используются далеко не всегда, а если применяются, то зачастую недостаточно эффективно. Между тем, бизнесом накоплен значительный опыт использования данных, есть наработанные методики и практики, которые можно использовать и для пользы государства. К тому же при помощи бизнеса представители госсектора могут те данные, которые у них есть, превращать в интересный продукт, который затем может быть полезен и предприятиям страны [6].

Кроме государственных органов, можно выделить три самых крупных владельца больших данных – это телеком–операторы, банки и социальные сети. У сотовых операторов есть обезличенные данные о перемещениях абонентских устройств, они могут анализировать территорию по социально–демографическим характеристикам, по динамике этих характеристик во времени. Это полезно для решения задач, связанных с определением благосостояния населения, миграцией, туризмом, безопасностью. Банки могут составить более точную картину расходов населения и оборотов юридических лиц. Социальные сети владеют анкетной информацией пользователей, у них есть возможность наблюдения детального трафика: они могут видеть, что конкретно человек загружал и смотрел, что вводил в поисковых полях [6].

Главной проблемой получаемых данных из альтернативных источников, особенно телеком–операторов и социальных сетей, является то, что они не всегда достоверны, содержат ошибки и не полные записи, что может привести к искажению аналитических выводов. Поэтому, в отличие от бизнеса, государственные органы чаще используют свои специализированные порталы, такие как «Единая система нормативно–справочной информации», «Национальная система пространственных данных» и другие.

Государство предпринимает дополнительные меры по цифровой трансформации государственного управления. Например, созданная Росреестром федеральная государственная информационная система «Единая

цифровая платформа – Национальная система пространственных данных» запущена в пилотном режиме ещё в 2022 году. На ней содержатся открытые данные о территории, в том числе сведения о земле и недвижимости, а также базовые сервисы, ориентированные на людей и профессиональных участников рынка. Полностью завершить формирование единой цифровой платформы пространственных данных и единой электронной картографической основы, объединив разрозненные сведения о земле и иных объектах недвижимости на территории всей страны, планируется к 2030 году [32].

Однако, подобные порталы, будучи весьма полезными, специализируются несколько в другом, и не дают всей оперативной информации для осуществления цифрового маркетинга в государственном управлении. Следовательно, управленцу, в своей работе, в связи с должностными обязанностями, полезно использовать все имеющиеся альтернативные источники данных для оперативного контроля ситуации в области, подлежащей государственному регулированию. Конечно же, при этом нужно понимать все возможные издержки использования альтернативных источников и уметь вносить обоснованную коррекцию в полученные аналитические данные во избежание ошибочных выводов.

Из–за большого объема данных государственные ведомства и современные компании всё чаще обращаются к BI–системам. Это помогает принимать обоснованные решения, строить прогнозы, гипотезы и выявлять скрытые закономерности в данных. BI–системы – это автоматизированные аналитические решения, предназначенные для сбора, обработки и визуализации больших объемов данных из разных источников. Главная задача таких платформ – помочь выявлять закономерности, находить точки роста, оптимизировать внутренние процессы и принимать более точные управленческие решения на основе фактических данных. С помощью BI–систем можно: объединять разрозненные данные из множества систем (CRM, ERP, Excel, базы данных и др.); анализировать ключевые показатели

эффективности (KPI); строить прогнозы и выявлять риски; оперативно получать актуальные отчеты в понятной визуальной форме [56].

Управление и аналитика в государственном секторе с помощью BI–инструментов – это возможность руководителей предприятий и ведомств разных уровней не только отслеживать актуальные метрики эффективности в режиме онлайн, но и прогнозировать различные социальные и экономические изменения, оценивать риски, принимать грамотные стратегические и оперативные решения в бизнесе и государственном управлении.

Рассмотрим один из примеров BI систем. PolyAnalyst – это российская платформа визуальной разработки сценариев анализа данных и текстовых документов, а также построения интерактивных отчётов, не требующая навыков программирования. Программный продукт PolyAnalyst предназначен для анализа структурированных и неструктурированных данных на высокопрофессиональном промышленном уровне. Система включает: набор инструментов для загрузки данных из множества источников, объединение, агрегация, очистка и преобразование этих данных; набор алгоритмов машинного обучения и статистических методов анализа; технологии обработки данных на естественном языке.

Работать в системе PolyAnalyst могут бизнес–пользователи и отраслевые специалисты без навыков программирования, в том числе финансисты, аудиторы, юристы. Они могут быстро, без привлечения ИТ–специалистов, решать локальные аналитические задачи, проводить исследования своих данных и самостоятельно проверять идеи. PolyAnalyst предлагает простой и интуитивно–понятный пользовательский интерфейс, где все этапы создания аналитического сценария реализованы в единой среде. Сценарии строятся путём перетаскивания функциональных блоков и их соединения друг с другом на поле разработки решения. Пользователь формирует наглядную, последовательную, легко модифицируемую и расширяемую модель анализа. Построенные аналитические сценарии могут быть динамически привязаны к

ключевым бизнес–процессам компании, и автоматически выполняться по расписанию или при наступлении определенного события. Сценарии анализа также могут интегрироваться в текущие ИТ–системы компании путём обмена данными через программный интерфейс. ИТ рынок программных средств также предлагает более простые BI системы. Например, Microsoft Power BI.

Технологии бизнес–аналитики и многофункциональные решения с возможностью прогнозирования и мониторинга становятся востребованными для контроля эффективности использования государственных инвестиций, работу структурных подразделений различных министерств и ведомств, а также их взаимодействие с соответствующими государственными органами. Эти инструменты выявляют скрытые связи между показателями социально–экономического развития, позволяют обоснованно оценивать эффективность принятых управленческих решений [5].

Государственные органы и ведомства также могут использовать в своей работе Hr аналитику, которая сосредоточена на исследовании, совершенствовании и использовании элементов человеческого капитала, таких как предыдущий опыт или образование, а также на применении аналитических методов в сочетании с данными о людях для информирования об организационной стратегии и повышения производительности. Значительный рост доступа к Hr технологиям в последние годы, включая информационные системы управления персоналом, облачные платформы и приложения, предоставил возможность собирать и анализировать большие объёмы данных о сотрудниках по сравнению с более ранними ИТ системами [11].

На основе анализа научной литературы можно выделить следующие ключевые выводы. Взаимосвязь цифрового маркетинга и государственного управления заключается в том, что цифровой маркетинг активно используется в государственном управлении для укрепления доверия граждан к власти, повышения открытости и улучшения взаимодействия между государством и обществом. Применение информационных и коммуникационных технологий

позволяет улучшить эффективность предоставления государственных услуг, оптимизировать управленческие процессы и усилить обратную связь с населением. Эффективное государственное управление требует создания целостной экосистемы цифровых услуг, охватывающей важные сферы жизни общества и бизнеса. Использование аналитики данных в государственном секторе способствует объективной оценке деятельности ведомств, выявлению проблем и поиску оптимальных решений.

Эти выводы подчеркивают важность интеграции цифровых технологий и аналитики в процессы государственного управления для повышения его эффективности и качества обслуживания граждан. Несмотря на очевидные преимущества цифровой трансформации, существует ряд серьезных рисков, связанных с возможностью утечки конфиденциальной информации, нарушением приватности граждан и недостаточной защищенностью инфраструктурных объектов. Поэтому важным направлением работы должно стать формирование культуры безопасного обращения с персональными данными и внедрение надежных технических решений защиты информации.

Ситуационная задача

«Использование искусственного интеллекта и аналитики данных в органах власти»

Контекст:

В небольшом городе, население которого составляет около 100,000 человек, местные органы власти сталкиваются с рядом проблем, связанных с предоставлением услуг гражданам. Городская администрация получает множество обращений от жителей по вопросам, связанным с благоустройством, транспортом, здравоохранением и другими сферами. Однако, из-за большого объема запросов и ограниченных ресурсов, многие обращения остаются без ответа или решаются с задержкой.

Задача:

Городская администрация решила внедрить систему на основе искусственного интеллекта (ИИ) и аналитики данных для оптимизации работы с обращениями граждан и повышения качества предоставляемых услуг. Ваша задача как консультанта по цифровой трансформации состоит в том, чтобы разработать стратегию внедрения этой системы.

Этапы решения задачи:

1. Анализ текущей ситуации:

Определите основные проблемы, с которыми сталкивается городская администрация при обработке обращений граждан.

Проанализируйте существующие процессы и выявите узкие места, которые можно улучшить с помощью ИИ и аналитики данных.

2. Разработка модели ИИ:

Определите, какие данные необходимо собрать для обучения модели ИИ (например, типы обращений, время обработки, удовлетворенность граждан и т.д.).

Разработайте алгоритм, который будет классифицировать обращения по категориям и приоритизировать их в зависимости от срочности.

3. Создание аналитической платформы:

Предложите решения для визуализации данных, которые помогут руководству города отслеживать эффективность работы системы и выявлять тенденции в обращениях граждан.

Разработайте дашборд для анализа данных по обращениям, который позволит принимать обоснованные решения на основе собранной информации.

4. Обучение сотрудников:

Подготовьте программу обучения для сотрудников городской администрации по использованию новой системы и интерпретации данных.

Обсудите важность взаимодействия между ИИ и человеком, акцентируя внимание на том, что ИИ должен служить помощником, а не заменой.

5. Оценка результатов:

Определите ключевые показатели эффективности (KPI), которые будут использоваться для оценки успешности внедрения системы (например, время обработки обращений, уровень удовлетворенности граждан).

Разработайте план мониторинга и регулярной оценки результатов работы системы.

Вопросы для обсуждения:

1. Какие вызовы могут возникнуть при внедрении системы ИИ в органы власти?

2. Как обеспечить защиту данных граждан при использовании аналитики данных?

3. Какие методы можно использовать для повышения доверия граждан к системе на основе ИИ?

4. Какова роль граждан в процессе цифровой трансформации государственного управления?

Задания для самостоятельного выполнения

1. Составьте терминологический словарь по проблеме цифрового маркетинга и аналитики в государственном управлении. Включите в словарь основные термины, касающиеся цифрового маркетинга в целом, и в государственном управлении, в частности. Приведите соответствующие дефиниции и дайте краткую характеристику терминов.

2. Проведите анализ основных угроз информационной безопасности при осуществлении цифрового маркетинга на основе информации из различных аналитических центров, научных публикаций. Определите пути устранения угроз информационной безопасности.

3. Проанализируйте работу искусственного интеллекта «Алиса» по следующим критериям:

– распознавание;

– осмысление:

– действие.

Подготовьте письменное заключение о преимуществах и недостатках работы искусственного интеллекта «Алиса».

4. Произвести анализ потребностей определенной категории людей в соцсети (на выбор):

Примеры социальных групп для анализа:

1. Подростки от 12 до 15 лет (основные увлечения, интересы, стремления, девиации)

2. Юноши от 16 до 18 лет (основные увлечения, профессиональные интересы, склонности, девиации)

3. Молодые люди от 20 до 35 лет (хобби, тип выбираемой профессии, основные жизненные проблемы, способы решения жизненных проблем)

4. Зрелые люди от 35 до 50 лет (основные интересы, профессиональные деформации, семейные проблемы)

5. Престарелые люди от 60 до 70 (основные запросы в соцсетях, интересы, жизненные сложности).

5. Приведите по 3 примера Telegram ботов: чат, информаторы, игровые, ассистенты. Проведите их сравнительный анализ.

6. Проанализируйте работу чат–бота сервиса Госуслуг «Макс» по следующим критериям:

– понимание запроса;

– алгоритм взаимодействия;

– корректность вывода результатов запроса.

Подготовьте письменное заключение о преимуществах и недостатках работы чат–бота сервиса Госуслуг «Макс».

6. На примере одного из возможных проектов по цифровизации интересующей вас сферы необходимо:

– показать роль Big data (больших данных) для обоснования и принятия решения о реализации данного проекта (перечень больших данных, которые

необходимо собрать, цели сбора этих данных (какие тенденции или закономерности можно выяснить), источники сбора данных, методы анализа данных, использование данных социальных сетей и др.);

– опишите (представьте в схематичной форме) цифровую платформу данного проекта;

– определите ожидаемые результаты реализации проекта.

ЗАКЛЮЧЕНИЕ

В условиях стремительного технологического прогресса и глобальных изменений, происходящих в обществе, изучение проблем цифровизации государственного управления становится не просто актуальным, а жизненно необходимым. Цифровизация государственных процессов и внедрение современных технологий, таких как искусственный интеллект, цифровые экосистемы и аналитика данных, открывают новые горизонты для повышения эффективности управления, улучшения качества предоставляемых услуг и формирования более прозрачного и доступного государственного аппарата.

Искусственный интеллект, в частности, представляет собой мощный инструмент, способный трансформировать подходы к решению общественных проблем. Он позволяет обрабатывать огромные объемы данных, выявлять тенденции и предсказывать потребности граждан, что способствует более оперативному реагированию со стороны органов власти. Внедрение ИИ в процессы государственного управления не только оптимизирует работу государственных учреждений, но и значительно повышает уровень удовлетворенности населения.

Развитие цифровых экосистем также играет ключевую роль в формировании современного цифрового государства. Эти экосистемы объединяют различные государственные и частные сервисы, создавая единое

информационное пространство, где граждане могут легко получать доступ к необходимым услугам. Такой подход способствует интеграции различных сфер государственной деятельности и обеспечивает более комплексный подход к решению проблем общества.

Цифровой маркетинг и аналитика данных становятся важными инструментами для взаимодействия органов власти с гражданами. Они позволяют не только информировать население о доступных услугах и инициативах, но и активно вовлекать граждан в процесс принятия решений. Анализ данных о поведении и предпочтениях граждан помогает государственным органам адаптировать свои стратегии и предлагать более персонализированные решения, что в свою очередь укрепляет доверие населения к власти.

Таким образом, изучение цифрового государственного управления является важным шагом к созданию эффективной, прозрачной и ориентированной на граждан государственной системы. Будущее государственных структур напрямую зависит от способности адаптироваться к новым вызовам и использовать возможности, предоставляемые цифровыми технологиями. Мы живем в эпоху, когда знание о цифровом управлении становится ключевым для формирования активных и ответственных граждан, готовых участвовать в развитии своего общества.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. Академия Ростеха расширила возможности Диагностической платформы [Электронный ресурс]. – Режим доступа: https://rostec.academy/media–center/news/tpost/ae2rrp5lf1–akademiya–rosteha–rasshirila–vozmozhnost – Дата обращения: 13.05.2025.

2. Актуальные киберугрозы: IV квартал 2024 года – I квартал 2025 года // Positive Technologies. – 2025. – [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru–ru/research/analytics/aktualnye–kiberugrozy–iv–kvartal–2024–goda–i–kvartal–2025–goda/ – Дата обращения: 11.05.2025.

3. Аналитика данных для эффективного госуправления: главные тенденции BI в госсекторе // N3.Аналитика. – [Электронный ресурс]. – Режим доступа: https://analytics.netrika.ru/publikatsii/stati/analitika–dannykh–dlya–effektivnogo–gosupravleniya–glavnye–tendentsii–bi–v–gossektore/ – Дата обращения: 25.05.2025.

4. Боднарук, Т. Р. Аналитика больших данных в государственном управлении: от проблем к решениям / Т. Р. Боднарук, М. Р. Боднарук // Экономика и бизнес: теория и практика. – 2024. – № 10–1(116). – С. 83–86. – DOI 10.24412/2411–0450–2024–10–1–83–86. – EDN LLJSMF.

5. Большие данные и бизнес–аналитика в государственном и муниципальном управлении: состояние и тенденции развития / М. В. Перова, А. А. Егорихина, Е. К. Головкина [и др.] // Наука, инновации, образование: актуальные вопросы и современные аспекты: монография. – Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2023. – С. 41–55. – EDN TXCTLU.

6. Большие данные: новые горизонты для госсектора // РБК. – [Электронный ресурс]. – Режим доступа: https://spb.plus.rbc.ru/news/63a957dc7a8aa9419deb3728 – Дата обращения: 25.05.2025.

7. Брекоткина И.П. Рационализм нового времени и гносеологические представления Рене Декарта / И.П. Брекоткина // Вестник Удмуртского университета. Серия «Философия. Психология. Педагогика». 2020. №3. – С. 237–243. [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/ratsionalizm–novogo–vremeni–i–gnoseologicheskie–predstavleniya–rene–dekarta – Дата обращения: 13.04.2025.

8. В Башкортостане запустили платформу обратной связи для бизнеса [Электронный ресурс]. – Режим доступа: https://pravitelstvorb.ru/news/24871/ – Дата обращения: 11.05.2025.

9. В Башкортостане озвучили планы цифрового развития на 2025 год [Электронный ресурс]. – Режим доступа: **https://it.bashkortostan.ru/presscenter/news/689358/** – Дата обращения: 15.05.2025.

10. Внедрение в Ямало–Ненецком автономном округе [Электронный ресурс]. – Режим доступа: https://webiomed.ru/nashi–proekty/yanao/. – Дата обращения: 03.05.2025.

11. Волкова, Н. В. Hr–аналитика. Аналитика данных в управлении персоналом: учебник для вузов / Н. В. Волкова, С. А. Евсеева. – Москва: Издательство Юрайт, 2025. – 104 с. – (Высшее образование). – ISBN 978–5–534–19568–2. – Текст: электронный // Образовательная платформа Юрайт [сайт]. – [Электронный ресурс]. – Режим доступа: https://urait.ru/bcode/569183 – Дата обращения: 25.05.2025.

12. Вострецова, Е. В. Основы информационной безопасности: учебное пособие для студентов вузов / Е. В. Вострецова. – Екатеринбург: Изд–во Урал. Ун–та, 2019. – 204 с.

13. Гарифуллина, А.Ф. Инновационные подходы к системе управления на региональном уровне: от цифровизации к устойчивому развитию / А.Ф. Гарифуллина, З.Л. Сизоненко // Экономика и управление: научно–практический журнал. 2024. № 5. С. 68–74. DOI: 10.34773/EU.2024.5.11.

14. Глоссарий предпринимателя [Электронный ресурс]. – Режим доступа: Https://e–glossary.rghpu.ru/ai_21 – Дата обращения: 12.05.2025

15. Годовые расходы на облачную ИТ–инфраструктуру по всему миру с 2013 по 2025 год [Электронный ресурс]. – Режим доступа: https://www.statista.com/statistics/503686/worldwide–cloud–it–infrastructuremarket–spending – Дата обращения: 10.05.2025

16. Двоеглазова, Е. А. Цифровизация государственного управления / Е.А. Двоеглазова, Ч.М. Куракова // Актуальные исследования. 2024. №5 (187). Ч.I. С. 70–74. [Электронный ресурс]. – Режим доступа: https://apni.ru/article/8347–tsifrovizatsiya–gosudarstvennogo–upravleniya – Дата обращения 12.05.2025

17. Дружба О.В., Дружба К.Г. и др. Поколение Z в сетях виртуальности / Дружба О.В., Дружба К.Г., Каирова И.А., Кошман М.В., Левицкий С.С., Лепилова Л.А., Мерзлякова И.Л., Морозова О.М., Орехова Л.Г., Пивоварова И.А., Сурков В.В. // Монография. Ростов–на–Дону, 2021.

18. Единая информационная платформа национальной системы управления данными [Электронный ресурс]. – Режим доступа: **https://digital.gov.ru/en/activity/czifrovizacziya–gosudarstva/infrastruktura–elektronnogo–pravitelstva/federalnaya–gosudarstvennaya–informaczionnaya–sistema–edinaya–informaczionnaya–platforma–naczionalnoj–sistemy–upravleniya–dannymi** – Дата обращения 14.05.2025

19. Записки преподавателя Какими бывают ML и DL [Электронный ресурс]. – Режим доступа: https://waksoft.susu.ru/2018/06/07/kakimi–byivayut–ml–i–dl/ – Дата обращения: 15.03.2025

20. Зуденкова, С. А. Гостех: от платформы к экосистеме / С. А. Зуденкова // Вопросы российского и международного права. – 2024. – Т. 14, № 1–1. – С. 292–298. – DOI 10.34670/AR.2024.97.92.040. – EDN PAHSPS.

21. **ИИ в госсекторе: Перспективные сценарии и план для начала использования** [Электронный ресурс]. – Режим доступа: **https://www.tadviser.ru/index.php/** – Дата обращения: 11.05.2025.

22. Искусственный интеллект в государственном управлении [Электронный ресурс]. – Режим доступа: https://www.tadviser.ru/index.php/Статья:Искусственный_интеллект_в_государственном_управлении. – Дата обращения 12.10.2024

23. Использование искусственного интеллекта обсудили в правительстве Башкирии [Электронный ресурс]. – Режим доступа: **https://национальныепроекты.рф/news/ispolzovanie–iskusstvennogo–intellekta–obsudili–v–pravitelstve–bashkirii/** – Дата обращения: 27.05.2025

24. Конференция «Путешествие в мир искусственного интеллекта» [Электронный ресурс]. – Режим доступа: http://www.kremlin.ru/events/president/transcripts/72811 – Дата обращения: 03.05.2025

25. Концепция формирования информационного общества в России : одобрено Решением Государственной комиссии по информатизации при Государственном комитете Российской Федерации по связи и информатизации от 28 мая 1999 года № 32. [Электронный ресурс]. – Режим доступа: http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/37cd5e6756dce634c32568c000474a8a (дата обращения: 01.10.2025)

26. Кострова, Ю.Б. Особенности использования информационно–коммуникационных технологий в государственном управлении / Ю.Б.Кострова // Научные труды Московского университета имени С.Ю. Витте. Том Выпуск 7. – Москва: Московский университет им. С.Ю. Витте, 2020. – С. 41–52

27. Кострова, Ю.Б. Тенденции развития маркетинга и менеджмента в условиях цифровой экономики / Ю.Б.Кострова // Тенденции экономического

развития в XXI веке: Материалы II МНПК. – Минск: Белорусский государственный университет, 2020. – С. 546–549.

28. Лукьянов, А.В. Методология исследования, основанного на социальном самосознании / А.В. Лукьянов, Е.Ю. Бикметов, К.В. Храмов // Современная наука: актуальные проблемы теории и практики. Серия: Познание. – 2023. – № 9. – С. 85–88.

29. Морозов, И. Л. Государственное управление в сфере информационной безопасности современной России: учеб.–метод. Пос. / И. Л. Морозов. – Волгоград: Изд–во Волгоградского института управления, 2021. – 88 с.

30. Московские финансисты внедряют сервисы на основе искусственного интеллекта [Электронный ресурс]. – Режим доступа: https://www.mos.ru/news/item/142678073//. – Дата обращения: 01.05.2025

31. Национальная программа «Цифровая экономика Российской Федерации» [Электронный ресурс]. – Режим доступа: https://digital.gov.ru/target/naczionalnaya–programma–czifrovaya–ekonomika–rossijskoj–federaczii – Дата обращения: 03.05.2025

32. Национальная система пространственных данных запущена в пилотных регионах // Аналитический центр при Правительстве Российской Федерации. – [Электронный ресурс]. – Режим доступа: https://clck.ru/3dtjty – Дата обращения: 25.05.2025.

33. Национальный проект «Экономика данных и цифровая трансформация государства» [Электронный ресурс]. – Режим доступа: **https://digital.gov.ru/target/naczionalnyj–proekt–ekonomika–dannyh–i–czifrovaya–transformacziya–gosudarstva** – Дата обращения: 22.05.2025.

34. Национальный центр развития искусственного интеллекта при Правительстве Российской Федерации [Электронный ресурс]. – Режим доступа: https://ai.gov.ru/ncpii/. – Дата обращения: 03.04.2025

35. Норина, В.Н. Экономико–географическая характеристика Башкортостана / В.Н.Норина // Образовательный портал «Справочник». – Дата последнего обновления статьи: 24.05.2024. – [Электронный ресурс]. – Режим доступа: https://spravochnick.ru/geografiya/ekonomiko–geograficheskaya_harakteristika_bashkortostana/ – Дата обращения: 13.07.2024.

36. О безопасности критической информационной инфраструктуры Российской Федерации. Федеральный закон от 26 июля 2017 г. N 187–ФЗ. [Электронный ресурс]. – Режим доступа: https://base.garant.ru/71730198/ – Дата обращения: 01.05.2025.

37. О намерениях между Правительством Российской Федерации и заинтересованными организациями в целях развития высокотехнологичного направления «Искусственный интеллект». Распоряжение Правительства РФ от 28 декабря 2022 г. N 4267–р [Электронный ресурс]. – Режим доступа: https://rulaws.ru/goverment/Rasporyazhenie–Pravitelstva–RF–ot–28.12.2022–N–4267–r/. – Дата обращения: 03.10.2024.

38. О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года : Указ Президента РФ от 07.05.2018 года № 204 // «КонсультантПлюс» : [офиц. Сайт]. [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_297432/ – Дата обращения: 01.05.2025.

39. О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года. Указ Президента Российской Федерации от 07.05.2024 г. № 309 [Электронный ресурс]. – Режим доступа: http://www.kremlin.ru/acts/bank/50542 – Дата обращения: 01.05.2025.

40. О развитии искусственного интеллекта в Российской Федерации. Указ Президента Российской Федерации от 10.10.2019 г. № 490 [Электронный

ресурс]. – Режим доступа: **http://www.kremlin.ru/acts/bank/44731** – Дата обращения: 01.05.2025.

41. О Центре управления Республикой Башкортостан [Электронный ресурс]. – Режим доступа: https://docs.cntd.ru/document/578143664 – Дата обращения: 01.05.2025.

42. О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных». Федеральном законе от 24.04.2020 N 123–ФЗ. [Электронный ресурс]. – Режим доступа: http://www.kremlin.ru/acts/bank/45475 – Дата обращения: 01.05.2025.

43. О развитии искусственного интеллекта в Российской Федерации. Указ Президента Российской Федерации от 10.10.2019 г. № 490 [Электронный ресурс]. – Режим доступа: **http://www.kremlin.ru/acts/bank/44731** – Дата обращения: 26.05.2025.

44. Об утверждении перечня инициатив социально–экономического развития Российской Федерации до 2030 года. Распоряжение Правительства РФ от 06.10.2021 N 2816–р (ред. от 08.05.2025). [Электронный ресурс]. – Режим доступа: **https://www.garant.ru/products/ipo/prime/doc/402792803/** – Дата обращения: 11.05.2025.

45. Перечень поручений Президента РФ от 30 марта 2024 г. № Пр–616 по реализации Послания Президента Федеральному Собранию. [Электронный ресурс]. – Режим доступа: http://www.kremlin.ru/acts/assignments/orders/73759 – Дата обращения: 01.05.2025.

46. Подольская, Т. В. Тенденции и перспективы применения технологий govtech в процессе цифровизации государственного сектора / Т. В. Подольская, Ф. Д. Ульбашева, Е. А. Васюта // Государственное и

муниципальное управление. Ученые записки. – 2024. – № 2. – С. 147–158. – DOI 10.22394/2079–1690–2024–1–2–147–158. – EDN YAGTCK

47. Попкова, А. А. Факторы и направления политики обеспечения информационной безопасности России / А. А. Попкова, К. В. Парфенов // Известия высших учебных заведений. Социология. Экономика. Политика. – 2024. – Т. 17, № 1. – С. 101–115. – DOI 10.31660/1993–1824–2024–1–101–115. – EDN QIVK

48. Развитие искусственного интеллекта [Электронный ресурс]. – Режим доступа: https://www.economy.gov.ru/material/departments/d01/razvitie_iskusstvennogo_intellekta/ – Дата обращения: 06.05.2025

49. Россия вошла в топ–10 стран–лидеров в области цифровизации госуправления [Электронный ресурс]. – Режим доступа: **https://d–russia.ru/rossija–voshla–v–top–10–stran–liderov–v–oblasti–cifrovizacii–gosupravlenija–vsemirnyj–bank.html** – Дата обращения: 06.05.2025

50. Сахалинская область внедрит ИИ для мастер–планирования и ускорения процессов развития территорий [Электронный ресурс]. – Режим доступа: https://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B5%D0%BA%D1%82:%D0%A1%D0%B0%D1%85%D0%B0%D0%BB%D0%B8%D0%BD%D1%81%D0%BA%D0%B0%D1%8F_%D0%BE%D0%B1%D0%BB%D0%B0%D1%81%D1%82%D1%8C_%D0%B2%D0%BD%D0%B5%D0%B4%D1%80%D0%B8%D1%82_%D0%98%D0%98_%D0%B4%D0%BB%D1%8F_%D0%BC%D0%B0%D1%81%D1%82%D0%B5%D1%80–%D0%BF%D0%BB%D0%B0%D0%BD%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F_%D0%B8_%D1%83%D1%81%D0%BA%D0%BE%D1%80%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BF%D1%80%D0%BE%D1%86%D0%B5%D1%81%D1%81%D0%BE%D0%B2_%D1%80%D0%B0%D0%B7%D0%B2%D0%B8%D1%82%D0

%B8%D1%8F_%D1%82%D0%B5%D1%80%D1%80%D0%B8%D1%82%D0%BE%D1%80%D0%B8%D0%B9 – Дата обращения: 04.05.2025

51. Сборник кейсов и лучших практик цифровизации государственного управления [Электронный ресурс]. – Режим доступа: **https://intosairussia.org/ru/novosti–media/novosti/sbornik–kejsov–i–luchshikh–praktik–tsifrovizatsii–gosudarstvennogo–upravleniya.html** – Дата обращения: 04.05.2025.

52. Свинухова, Ю.Н. Модели управления качеством жизни в регионе: Национальная социальная инициатива (на примере Республики Башкортостан) / Ю.Н.Свинухова // Социодинамика. 2023. № 11. С. 109–125.

53. Сизоненко, З. Л. Цифровые платформы в государственном управлении: проблемы и достижения / З. Л. Сизоненко, О. Н. Игнатьева, В. А. Ковшечникова // Экономические, информационные и социокультурные основания управления в современных условиях : Сборник научных трудов. – Уфа : ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ", 2023. – С. 107–112. – EDN MZKJVO.

54. Системный проект электронного правительства Российской Федерации. [Электронный ресурс]. – Режим доступа: https://digital.gov.ru/uploaded/presentations/prezentatsiya–sistemnogo–proekta–ep.pdf – Дата обращения: 10.04.2025

55. Стратегические направление в области цифровой трансформации отрасли культуры РФ: Распоряжение Правительства РФ №3550–р от 11.12.2023. [Электронный ресурс]. – Режим доступа: http://publication.pravo.gov.ru/document/0001202312180033. – Дата обращения: 13.05.2025.

56. Топ 10 лучших BI–систем: сравнение и обзор систем аналитики // Первый бит: #Бизнес анализ (BI). – [Электронный ресурс]. – Режим доступа:

https://nizhniy.1cbit.ru/blog/top–10–luchshikh–bi–sistem–sravnenie–i–obzor–sistem–analitiki/?Utm_referrer=https%3A%2F%2Fwww.bing.com%2F – Дата обращения: 25.05.2025.

57. Тюрин В. В. Управление цифровой трансформацией. Точка зрения / Владислав Владимирович Тюрин. – [б. М.] : Издательские решения, 2023. –284 с

58. Филиппова А.С., Дяминова Э.И., Забихуллин Ф.З. Курс лекций по дисциплине «Цифровые технологии в научно–исследовательской и управленческой деятельности»: учебно–методическое пособие / – Уфа: Издательство БГПУ, 2025. – 112 с. – ISBN 978–5–907730–90–8

59. Цифровая экосистема в сфере государственного управления, в том числе строительной отрасли, взаимодействие информационных систем [Электронный ресурс]. – Режим доступа: **https://sudact.ru/law/pismo–minstroia–rossii–ot–06072023–n–39972–iia14/prilozhenie/4/** – Дата обращения: 05.05.2025.

60. Цифровизация публичного управления : учебное пособие / С. Н. Костина, Д. Л. Сивоволов, Г. А. Банных, Т. М. Резер, О. Г. Александров ; под общ. Ред. С. Н. Костиной ; Министерство науки и высшего образования Российской Федерации, Уральский федеральный университет. – Екатеринбург : Изд–во Урал. Ун–та, 2022. – 111 с. : ил. – 30 экз. – ISBN 978–5–7996–3570–1. – Текст :непосредственный.

61. Цифровое государство и экономика : учебник / С. Е. Прокофьев, О. В. Панина, Н. Л. Красюкова [и др.] ; под общ. Ред. С. Е. Прокофьева, О. В. Паниной, К. В. Харченко. – Москва : кнорус, 2024. – 345 с. – ISBN 978–5–406–12473–4. – [Электронный ресурс]. – Режим доступа:https://book.ru/book/951781 – Дата обращения: 24.04.2025.

62. Цифровые платформы и экосистемы в государственном управлении : монография / под ред. Е.В. Васильевой, Б.Б. Славина. – Москва : ИНФРА–М, 2024. – 204 с. – (Научная мысль). – DOI 10.12737/2021353. – ISBN

978–5–16–018537–8. – Текст : электронный. – [Электронный ресурс]. – Режим доступа: https://znanium.ru/catalog/product/2021353 – Дата обращения: 28.04.2025.

63. Чапис, М. А. Информационная безопасность государства как правовой порядок обеспечения национальной безопасности в информационной сфере / М. А. Чапис // Наукосфера. – 2024. – № 6–1. – С. 551–557. – DOI 10.5281/zenodo.11638587. – EDN JKTRGZ.

64. Шашкова, Н. И. Цифровое государственное управление: роль, риски и новые парадигмы развития / Н. И. Шашкова // Вестник экономики, права и социологии. – 2023. – № 3. – С. 55–59. – EDN WPZULA.

65. Швайка, О.И. Цифровизация права и экономики в России и за рубежом: эволюция и тенденции развития / О.И.Швайка // Вестник Московского университета им. С.Ю. Витте. Серия 1: Экономика и управление. – 2022. – № 4 (43). – С. 17–29.