АНАЛИЗ ПРОБЕЛОВ И КОЛЛИЗИЙ

В НОРМАТИВНОЙ ПРАВОВОЙ БАЗЕ КЫРГЫЗСКОЙ РЕСПУБЛИКИ С ОБЗОРОМ ЛУЧШИХ МИРОВЫХ И РЕГИОНАЛЬНЫХ ПРАКТИК

МАЙ 2022

Г. БИШКЕК, КЫРГЫЗСКАЯ РЕСПУБЛИКА

КОНТРАКТ NO. CS-QCBS-3-1-1

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Об этом документе

Консультант - Консорциум по разработке цифрового законодательства (далее – Консультант) в составе ОФ «Гражданская Инициатива Интернет Политики» (Ведущий партнер Консорциума, Кыргызская Республика) и Эстонской Академии э-управления (e-Governance Academy Foundation, eGA) (Участник Консорциума, Эстония), задействован в рамках проекта «Digital CASA-Кыргызская Республика» (далее - Проект) по Контракту # CS-QCBS-3-1-1 "Консультационные услуги по **проведению детального анализа действующей нормативно-правовой базы и разработке необходимых нормативных актов для создания благоприятных условий для цифровой экономики"**.

Данный отчет предоставляется в исполнение услуг Консультанта и представляет собой Результат 2 в рамках 1-го Этапа проекта.

Услуги Консультанта являются частью многокомпонентного многолетнего национального проекта «Digital CASA - Кыргызская Республика», охватывающего развитие региональной инфраструктуры связи, региональных центров обработки данных, цифровых платформ и интеллектуальных решений, а также создание благоприятной среды для цифровой экономики.

Целью развития проекта на страновом уровне является расширение доступа к более доступному интернету, привлечение частных инвестиций в сектор ИКТ и улучшение возможностей государства по предоставлению цифровых государственных услуг в Кыргызской Республике путем содействия развитию региональной интегрированной цифровой инфраструктуры и благоприятной среды.

Компонент проекта, посвященный созданию благоприятной среды, направлен на укрепление и согласование на региональном и национальном уровнях законов, нормативных актов, институционального и кадрового потенциала. Он также предназначен для развития различных партнерских отношений, необходимых для полного использования преимуществ быстро развивающихся цифровых технологий, инфраструктуры и платформ, повышения конкурентоспособности на рынке, стимулирования инноваций и создания рабочих мест. Также будут поддерживаться цифровое лидерство, развитие навыков и потенциала, и стратегические коммуникации.

Данный компонент включает в себя три подкомпонента: 3.1. Правовые, нормативные и институциональные основы цифровой экономики, 3.2. Региональные партнерства в области навыков, рабочих мест и инноваций в области цифровой экономики и 3.3. Цифровое лидерство и стратегические коммуникации. Услуги Консультанта являются частью подкомпонента 3.1. Правовые, нормативные и институциональные основы цифровой экономики, направленные на поддержку создания правовой и нормативной среды для цифровой экономики на основе углубленного анализа пробелов в законодательстве и регулировании.

В результате Проект должен создать основу для внедрения и устойчивого развития цифровой инфраструктуры, развития цифровых платформ и облачных технологий и цифровых сервисов, с учетом целей и показателей Проекта, а также внедрения механизмов государственно-частного партнерства и вопросов кибербезопасности в качестве приоритетных направлений.

Данный анализ, в соответствии с Техническим заданием на услуги Консультанта, содержит:

- углубленное описание пробелов и недостатков нормативных правовых актов;
- классификацию выявленных вопросов по воздействию на установленную сферу деятельности (например, повышение операционных издержек является препятствием, снижение капитализации, предотвращение появление новых услуг или рынков, риск рыночной нестабильности);
- описание лучших международных и региональных практик, направленных на решение поставленных вопросов.

Результаты проведенного в настоящем отчете анализа систематизированы таким образом, чтобы они могли быть использованы для разработки нормативной правовой базы Кыргызской Республики, предложенной в рамках Результата 1.

Резюме

Кыргызская Республика целенаправленно проводит работу в сфере внедрения электронного управления и цифровизации страны, и связанные задачи поставлены в целом ряде стратегических документов, включая концепции, программы и планы действия цифровой трансформации и цифрового развития. Однако разрозненность и неоднородность законодательства, в том числе исторически сложившиеся, являются существенными препятствиями для построения благоприятной нормативно-правовой среды необходимой для развитой, конкурентоспособной цифровой экономики. Это подтверждается выводами различных международных индексов и рейтингах цифрового регулирования, где страновые оценки Кыргызской Республики остаются на переходном или начальном уровне как это видно по индексу последнего поколения цифрового регулирования G5 Benchmark Международного союза электросвязи.

Эффективное регулирование - сочетающее в себе передовой международный опыт, лучшие практики и доказательную основу - является важнейшим ключом к ускоренной цифровой трансформации Кыргызской Республики. Даже небольшие улучшения регулятивной среды приводят к измеримому прогрессу и улучшению по ряду экономических показателей. Последние исследования по 145 странам демонстрируют, что оптимизация и модернизация регулятивной среды существенно увеличивают объем инвестиций в фиксированную и мобильную инфраструктуру. К примеру, улучшение регулятивного индекса ICT Regulatory Tracker на 10% приводит к росту инвестиций в среднем на 7%.

В то же время лучшая международная практика последних лет показывает, что отраслевое разделение правовых актов для целей регулирования цифровой трансформации стало менее актуальным, поскольку каждое направление затрагивает остальные, и может содержать в себе сквозные приоритеты – например цифровые навыки, цифровое правительство и данные. Стремительность, взаимосвязанность и комплексность процессов цифрового развития делают неприемлемыми стандартные подходы к нормативно-правовому регулированию. В целом, международные исследования проблем регулирования в цифровой сфере подталкивают к выводу о необходимости реализации системного подхода к построению применимого законодательства.

Данный анализ регуляторных пробелов функционально направлен на то, чтобы представить законодательство Кыргызской Республики в сфере цифровой экономики в качестве единой системы. За основу анализа была взята структура, предложенная на предыдущем этапе работы. В качестве исходной информации для анализа по каждому разделу составлен перечень нормативных правовых актов. Выявленные недостатки были классифицированы по четырем видам - пробелы, устаревшие нормы, барьеры и неработающие нормы.

В анализ включены области законодательства, в которые ожидаются существенные изменения. В то же время, анализ сфокусирован на основных направлениях развития правового регулирования в сфере цифровой экономике и потому не включает в себя те правовые акты, куда возможны изменения технического характера (в частности, в законодательство о регистрации), либо развитие которых должно быть предметом отдельной работы (например, финансовое законодательство).

Анализ правовых основ цифрового управления **проводился в соответствии с принципами лучших практик регулирования**: цифровая трансформация процессов; платформонезависимость и ориентация на мобильные устройства; независимость от поставщиков и переносимость данных; ориентированность на пользователя и право пользователя на информационное самоопределение; цифровизация на всех этапах формирования и предоставления государственной услуги или бизнес-процесса; правительство как платформа; принятие управленческих решений на основе цифровых данных; использование открытых данных; использование открытых стандартов и свободного программного обеспечения; технологическая нейтральность и открытость для инноваций и «подрывных» технологий; и презумпция общедоступности информации.

Выводы анализа пробелов подтверждают необходимость проведения большого объема работ по модернизации и развитию действующего законодательства. Краткие итоги в виде статуса каждого раздела суммированы ниже.

Регулятивный пробел	✗
Существенные недостатки	!
Соответствует стандартам	✓

Правовые и институциональные основы	Правовые основы цифрового управления, органы цифрового управления	✗
Терминология	Глоссарий в области правового регулирования цифровой экономики	✗
Объекты цифрового управления	электронные сообщения	✗
	записи	✗
	документы	✓
	информресурсы	✓
	информсистемы	✓
	распределённые информсистемы и реестры (блокчейн)	✗
	технологические системы (ЦОДы)	✗
	телекоммуникационные сети	✓
	приложения	✗
	цифровые услуги (сервисы), в том числе государственные и муниципальные	!
Субъекты цифрового управления	операторы технологических систем	✗
	операторы информсистем	✓
	операторы телекоммуникационных сетей	✓
	провайдеры услуг (сервисов)	✗
	аутсорсеры (обработчики)	✗
	владельцы информационных ресурсов	!
	принципалы данных (лица, к которым относятся данные – субъекты персональных данных, источники промышленных данных и т.п.)	✗
	пользователи данных и сервисов (профессиональные пользователи и конечные пользователи)	✗
Основания возникновения, изменения, прекращения правоотношений в цифровой среде	официальные источники информации;	✓
	смартконтракты;	✗
	результаты цифровых услуг	✗
Информационные правоотношения	виды информации	✓
	распространение, предоставление информации	✓
	доступ к информации	✓
	открытые данные	✓
	защита информации и	✓
	кибербезопасность	!

Персональные данные	принципы и основания обработки	!
	категории данных	!
	права субъекта	!
	обязанности оператора	✓
	трансграничная передача	✓
	контроль и надзор	!
Большие данные	принципалы, операторы и пользователи данных	✗
	переносимость данных	✗
	локализация данных	✗
	искусственный интеллект и нейросети	✗
Пространственные данные	национальная инфраструктура пространственных данных	✗
	портал пространственных данных	✗
	создание пространственных данных	✗
	доступ к пространственным данным, пространственные метаданные	✗
Электронное сообщение, запись, документ	правовой режим электронных сообщений	✗
	правовой режим цифровой записи, создание и использование цифровых записей	✗
	электронные документы: правовой режим документов, копий и оригиналов, перенос между носителями и т.п.	!
Цифровая идентификация	способы идентификации (коды, токены, подписи, биометрическая идентификация)	✗
	средства идентификации	✗
	системы идентификации	✗
Цифровые сервисы	регулирование цифровых сервисов в киберпространстве	✗

Государственные и муниципальные цифровые услуги	обеспечение процесса цифровой трансформации государственного управления	✗
	принципы предоставления государственных и муниципальных услуг в цифровой форме	✓
	координация в сфере цифровой трансформации государственного управления (между органами ответственными за цифровую трансформацию, развитие экономики и госуправление)	✗
Цифровое здоровье и благополучие	подходы к управлению данными о состоянии человека в течение всей его жизни	✗
	возможность установления требований к программным и аппаратным средствам для обеспечения здоровья и благополучия человека (отсылочная норма)	✗
	применение этических норм	✗
Технологическая инфраструктура цифрового управления	принципы использования инфраструктуры (повторное использование, недискриминационный доступ к инфраструктуре и т.п.)	✗
	полномочия по установлению технических требований к отдельным видам инфраструктуры	✗
Сети и ресурсы электросвязи	построение и использование сетей	✓
	распределение и использование ограниченных ресурсов	✓
Взаимодействие операторов связи и межсетевые соединения:	межсетевые соединения и недискриминационный доступ	✗
	сетевая нейтральность	✗
Услуги связи	права и обязанности пользователей, провайдеров и операторов	✓
	надзор и контроль	!
ГЧП в условиях цифровой трансформации	объекты ГЧП (информсистемы, информресурсы, технологические системы и телекоммуникационные сети)	✗
	особый порядок использования и монетизации объектов ГЧП	✗
Инновации	Закон об экспериментальных правовых режимах (регуляторных песочницах)	✗

Контекст для анализа

Внутригосударственный контекст

Кыргызская Республика с 2016 года целенаправленно проводит работу в сфере внедрения электронного управления и цифровизации страны. Основываясь на положении Конституции Кыргызской Республики о том, что развитие общества и государства опирается на научные исследования, современные технологии и инновации, Президент и Жогорку Кенеш последовательно реализуют политику инновационного развития в сфере цифровой экономике. В 2017 году были приняты Законы Кыргызской Республики «Об электронном управлении» и «Об электронной подписи», внесены изменения в законы Кыргызской Республики «Об информации персонального характера», «О государственных и муниципальных услугах», «О доступе к информации, находящееся в ведении государственных органов и органов местного самоуправления». В 2018 году Правительством Кыргызской Республики было принято решение о запуске системы «Түндүк», которая является одним из ключевых элементом электронного управления. В связи с этим были приняты ряд подзаконных актов по реализации системы «Түндүк» и определен ее оператор.

Задачи цифровизации страны и ускоренного развития с опорой на цифровые технологии поставлены в целом ряде стратегических документов:

- Национальной стратегии развития Кыргызской Республики на 2018-2040 годы и «Таза Коом[1]» как Национальной программе цифровой трансформации;
- Концепции цифровой трансформации “Цифровой Кыргызстан” - 2019-20232;
- Основных направлений деятельности Правительства Кыргызской Республики;
- Программы развития Кыргызской Республики на период 2018-2022 годов «Единство. Доверие. Созидание»3 (утверждена постановлением Жогорку Кенеша Кыргызской Республики от 20 апреля 2018 года № 2377-VI);
- Национальной программе развития Кыргызской Республики до 2026 года4.

Однако процессы цифровизации в среднесрочной перспективе оказались подчинены целому ряду объективных тенденций, вызванных как двухлетней эпидемией COVID-19 на территории Кыргызской Республики, так и политическими потрясениями второй половины 2020 года. Первоначальный всплеск использования цифровых технологий при массовом переводе государственных органов на удаленный режим работы во второй половине года резко замедлился, а потом и вовсе остановился. Государственные органы, выйдя на оффлайновый режим работы, вновь стали возвращаться к бумажному документообороту из-за его привычности, а также низкой степени прослеживаемости и контроля со стороны ответственных лиц.

---

[1] «Таза Коом» так и не была утверждена в качестве Национальной программы цифровой трансформации (хотя было несколько обсуждений, вариантов самой программы). В 2019 году Советом безопасности Кыргызской Республики была одобрена Концепция цифровой трансформации “Цифровой Кыргызстан” - 2019-2023 (вместо «Таза коом»)

[2] Несмотря на то, что Правительством был утвержден план реализации указанной Концепции, по факту она не исполняется, ее исполнение никто не контролирует, мероприятия из плана реализации «перетекают» в планы Кабинета министров, к самой Концепции, по-видимому, потерян интерес, о чем говорят неоднократные попытки в 2020-2021 г.г. разработать и принять новую концепцию цифровой экономики, проект которой проходил процедуры согласования, но в итоге не был утвержден в качестве НПА

[3] Публичных отчетов в открытых источниках о результатах исполнения данной программы не имеется

[4] Указывается, что данная программа разработана в рамках Национальной стратегии развития Кыргызской Республики до 2040 года с сохранением принципа преемственности на основе долгосрочных стратегических целей развития страны с ориентацией на человека и акцентом на основополагающее обязательство «не оставить никого позади» Целей устойчивого развития. Публичных отчетов в открытом доступе о ходе реализации указанной программы не имеется

В рассмотренном контексте приходится говорить о неустойчивости процессов цифровизации в Кыргызской Республике, вызванной факторами как объективного, так и субъективного плана.

Международный контекст

На международном уровне давно ведется работа по выработке регуляторных подходов, способных повысить устойчивость процессов развития на основе цифровых технологий. Результаты данной работы отражены в целом ряде отчетов и обзоров международных организаций и экспертных площадок, многие из которых используют методику рейтингования, то есть сравнительного анализа разных стран с использованием тех или иных численных метрик (коэффициентов).

Исследования Международного союза электросвязи показывают, что даже небольшие улучшения регулятивной среды приводят к измеримому прогрессу и улучшению по ряду экономических показателей. Обобщенные по 145 странам за период 2008–2019 гг данные демонстрируют, что оптимизация и модернизация регулятивной среды увеличивают объем инвестиций в фиксированную и мобильную инфраструктуру. К примеру, улучшение регулятивного индекса ICT Regulatory Tracker (о нем подробнее рассказывается ниже) на 10% приводит к росту инвестиций в среднем на 7%, а снижение бюрократических издержек наполовину увеличивает инвестиции на 17%. Отдельные регулятивные меры приводят к значимым улучшениям показателей покрытия, проникновения и ценовой доступности для пользователей мобильной связи (ITU, 2021b).

Почти все периодически обновляемые индексы, ставящие целью композитные измерения цифрового развития, как правило, включают в себя компоненты, измеряющие различные параметры нормативно-правовой базы цифрового развития. Среди общих индексов, имеющих отдельно выделенную регулятивную компоненту, можно отметить Network Readiness Index, индексы ICT Regulatory Tracker и G5 Benchmark Международного союза электросвязи, индекс ОЭСР Going Digital.

Network Readiness Index измеряет готовность среды цифрового регулирования по пяти направлениям – общая среда ИКТ регулирования, адаптивность правовой базы для новейших технологий, законодательство по электронной коммерции и защита конфиденциальных данных. По данному компоненту индекса последняя оценка за 2021 год для Кыргызской Республики выводит страну лишь на 110 место из 130 экономик мира, включенных в индекс, причем наиболее низкую оценку получила адаптивность правовой базы для новейших технологий (Portulans Institute, 2021).

По мере развития технологий начинают формироваться индексы, охватывающие исключительно регулирование цифрового пространства. Начальной базой для многих из них, а также подкомпонентом множества цифровых индексов и страновых оценок является **ICT Regulatory Tracker** Международного союза электросвязи (ITU, 2020). Он является сравнительным инструментом, помогающим определить статус регулирования по четырем кластерам регулятивной среды – регуляторный орган, мандат, регуляторный режим и защита конкуренции в ИКТ. Включая в себя более 50 индикаторов, индекс констатирует наличие или отсутствие определенных элементов регулирования и не ставит целью оценку качества регулирования.[5] Страновая оценка Кыргызской Республики за 2020 год (77.5 баллов из ста возможных) показывает пробелы регулирования по таким элементам, как требования для операторов по публикации информации, необходимой для присоединения к сетям, стоимость

[5] Сопроводительным документом к Трекеру в практической плоскости регулирования является Справочник по цифровому регулированию Международного союза электросвязи (ITU and The World Bank, 2020). Справочник содержит подробный обзор следующих ключевых тем: регуляторное управление и регуляторная независимость, конкуренция, доступ, интересы потребителей, защита данных, доверие, управление спектром, новые технологии, техническое регулирование и связь во время чрезвычайных ситуаций.

услуг присоединения, доступность переноса номеров для пользователей фиксированной и мобильной связи, возможность использования VoIP физлицами.

В 2021 году Международный союз электросвязи подготовил пробный «индекс» **G5 Benchmark** из 70 индикаторов регулирования и нормотворчества (ITU, 2021a). Индекс составлен в привязке к пяти уровням и поколениям регулирования цифровых технологий (G1-G2-G3-G4-G5) и ставит конечной целью G5 как самое последнее и современное поколение подходов и практик регулирования. Методика оценки включает четыре компонента, и все из них имеют регулятивные основы. Самая первая страновая оценка Кыргызской Республики на 2021 год (45 баллов из ста возможных) выявила следующие пробелы по методике G5:

1) национальное управление, основанное на сотрудничестве, или же уровень сотрудничества между регуляторными органами и другими государственными институтами. По данному компоненту отмечается, что в Кыргызстане отсутствуют механизмы сотрудничества с национальным CERT, независимым органом по защите данных, министерствами или агентствами по регулированию энергетики и окружающей среды (электронные отходы).

2) принципы разработки политик - участие, вовлеченность заинтересованных сторон, прозрачность принимаемых решений и процессов. Применительно к Кыргызстану отмечается отсутствие законных возможностей для затронутых сторон потребовать пересмотра или обжалования принятых правил в соответствующем административном органе (по всем секторам). Отмечается также выборочное применение принципа технологической нейтральности регулирования.

3) инструментарий цифрового развития – наличие национальных стратегий цифрового развития с отраслевыми требованиями и согласованность с Целями устойчивого развития. Здесь страновая оценка Кыргызстана выявила пробелы по множеству направлений.

- По отдельным тематическим приоритетам отмечается отсутствие правовых актов, регулирующих вопросы защиты детей в Интернете, концептов умного города, подписанных или ратифицированных соглашений по кибербезопасности (Будапештская конвенция о кибербезопасности), регулированию трансграничных потоков данных в отношении конфиденциальности, и о связи в чрезвычайных ситуациях (Конвенция Тампере).
- По инфраструктурной составляющей отмечено отсутствие официального реестра или карты всей инфраструктуры электросвязи/ИКТ; процедур по межотраслевому совместному использование инфраструктуры или правил, соглашений, инициатив продвижения совместной прокладки волоконно-оптических сетей.
- Кроме того, широкополосная связь не рассматривается как часть услуги унифицированного доступа, а планы действий в области развития широкополосной связи не включает в себя четкие шаги по оказанию услуг широкополосной связи для нужд социально незащищенных лиц.
- Цифровая стратегия, не ориентирована на цели устойчивого развития, не определены документы, поддерживающие переход к устойчивому потреблению и производству, отсутствуют правила обращения с электронными отходами, не разработана и введена в действие глобальная стратегия трудоустройства молодежи и не осуществляется реализация Глобального пакта о рабочих местах Международной организации труда.

4) повестка цифровой экономики – наличие стратегических документов по гармонизации, инновации, цифровой трансформации на основе прорывных технологий, налогообложения и кодексов поведения участников рынка. Страновая оценка отмечает отсутствие целостных политик по инновациям в сфере ИКТ/цифровизации, регулирования

цифровых рынков, искусственного интеллекта, специальных налоговых режимов для телекоммуникационного и цифрового сектора или интернет-услуг, добровольным или обязательным кодексам поведения.

Индекс ОЭСР **Going Digital** (OECD, 2020a) охватывает семь взаимосвязанных направлений регулирования - 1) Доступ; 2) Эффективное использование; 3) Инновации; 4) Занятость; 5) Социальное благополучие; 6) Доверие; и 7) Открытость рынка. Каждое направление состоит из ключевых приоритетов, представляющих собой итоговые цели регулирования – например, ими могут выступать инфраструктурные инвестиции, цифровая безопасность и конкурентность рынка.

Составители индекса исходят из того, что отраслевое разделение правовых актов для целей регулирования цифровой трансформации стало менее актуальным, поскольку каждое направление затрагивает остальные, и может содержать в себе сквозные приоритеты – например цифровые навыки, цифровое правительство и данные. Именно поэтому необходимо объединенно и целостно рассматривать все области регулирования цифровой экономики. Также необходимо сделать упор на координацию и сотрудничество между всеми участниками.

В ключевой обзорной публикации ОЭСР **Векторы Цифровой Трансформации** (OECD, 2020b) подчеркивается стремительность, взаимосвязанность и комплексность процессов цифрового развития, что делает неприемлемым стандартные подходы к нормативно-правовому регулированию. Особенности технологий, бизнес-моделей, поведения компаний и потребителей накладывают серьезные ограничения на традиционное регулятивное мышление. Например, возможности цифрового масштабирования позволяют компаниям и платформам расти на глобальном уровне с небольшим количеством сотрудников, капитала и физического присутствия – что может означать необходимость пересмотреть такие критерии применения правовых актов, как размер капитала или количество сотрудников. Сложная структура и комплексность цифровых продуктов стимулирует переход к конвергентным регулятивным подходам, сочетающим в себе межотраслевые полномочия и функции регулирования. Цифровые модели бизнеса также могут функционировать без привязки к юрисдикциям, снижая зависимость от принципов территориальности и суверенитета и заставляя правительства укреплять региональное, глобальное и тематическое сотрудничество в целях интероперабельности и гармонизации политик. Цифровая деятельность может опережать процессы институционального развития и нормативно-правовые рамки – требуя проактивной разработки таких мер, как регулятивные песочницы.

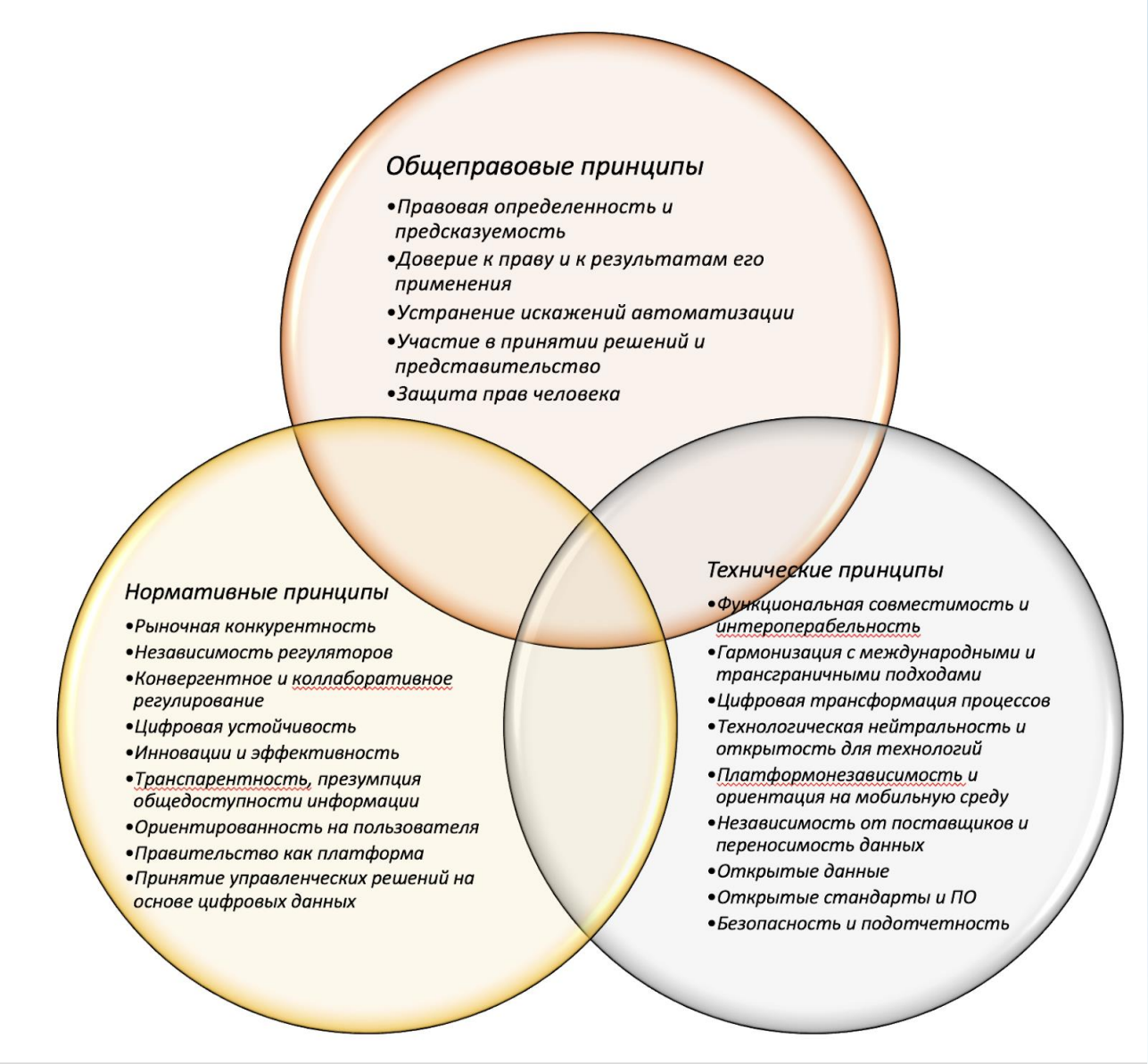
В целом, международные исследования проблем регулирования в цифровой сфере подталкивают к выводу о необходимости реализации системного подхода к построению применимого законодательства, что в случае Кыргызской Республики означает необходимость ориентации на существующие в мире стандарты регулирования в целях создания унифицированного и безбарьерного правового поля для деятельности в глобальном киберпространстве.

Правовые основы и принципы построения благоприятной нормативно-правовой среды для развитой, конкурентоспособной цифровой экономики в Кыргызской Республике

Разрозненность и неоднородность законодательства Кыргызской Республики, в том числе исторически сложившиеся, являются существенными препятствиями для реализации задач настоящего Проекта. В связи с этим проведенный анализ регуляторных пробелов функционально направлен на то, чтобы представить законодательство Кыргызской Республики в сфере цифровой экономики в качестве единой **системы**. Функциональный подход позволяет оценить целевое положение каждого действующего правового акта в системе, выявить и описать пробелы в регулировании, в том числе, вызванные развитием системы отношений в цифровой экономике и связанным с этим отставанием законодательства.

Недостатки в регулировании, выявляемые в ходе регуляторного анализа, не сводятся только к пробелам, поскольку они могут быть обусловлены фактической неработоспособностью правовых норм или их несоответствием изменившимся общественным отношениям в ходе развития цифровой экономики. Также вполне работающие и применимые нормы могут более не отвечать целям инновационного развития, закрепленных в Конституции Кыргызской Республики, законах и актах Президента, а потому должны считаться барьерами. Восполнение пробелов и устранение барьеров - то есть следующий этап реализации проекта - должны, во-первых, ориентироваться на лучшие практики с учетом их применимости к Кыргызской Республике и, во-вторых, учитывать базовые требования к правовому регулированию, рассмотренные ниже.

Работа по проекту будет основываться на **общеправовых принципах**, включающих в себя основополагающие ценности, такие как уважение и защита прав человека; защита персональных данных и право на неприкосновенность частной жизни; открытое и прозрачное нормативное регулирование, обеспечение недискриминационного, инклюзивного подхода, основанного на вовлечении и учете мнений при принятии решений всех заинтересованных сторон; уважение права активно искать и распространять информацию, получать доступ к ней на справедливых условиях. Также учтены основные **технические и нормативные принципы**, включающие функциональную совместимость политики и процедур, гармонизацию нормативной правовой базы с признанной лучшей мировой практикой, использование передового опыта лидеров в области цифровых преобразований; поддержку рыночной конкуренции и инноваций.



Эффективное регулирование - сочетающее в себе передовой международный опыт, лучшие практики и доказательную основу - является важнейшим ключом к ускоренной цифровой трансформации Кыргызской Республики. Основу эффективного регулирования составляют **базовые свойства права** как регулятора деятельности человека, на которых необходимо остановиться подробнее. Первым из них выступает **принцип правовой определённости** (legal certainty). Принцип правовой определённости – это ясность и четкость действующих правовых норм, устойчивость законных и обоснованных судебных актов, стабильность складывающихся на их основе правоотношений, чтобы заинтересованные лица с разумной степенью вероятности могли предвидеть последствия применения к ним судом действующих правовых предписаний и в соответствии с этим предвидеть последствия выбора того или иного варианта своего поведения (Масаладжиу, 2009). Принцип правовой определенности означает, что правило должно быть доступно и понятно тем, кому оно адресовано. Любое развитие права, в том числе, предполагающее или допускающее автоматизацию тех или иных областей человеческой деятельности, должно повышать, а не понижать правовую определенность.

Правовые нормы работают, поскольку они увеличивают доверие, а не уменьшают его. Поэтому вторым (после принципа правовой определённости) требованием к правовому регулированию является **принцип доверия** к праву и доверия как результата действия права. Право работает тогда, когда ему доверяют, договор подписывают, предполагая, что он будет

исполнен, государственной услугой пользуются в расчете на получение официального результата.

Внедрение современных правовых инструментов, таких как смарт-контракты, а также цифровизация государственного управления не могут уменьшать доверие и не должны лишать людей возможности проверить действие правила. Нельзя полностью доверяться тем нормам, которые были полностью или частично автоматизированы. Любая техническая система не обладает 100% надёжностью. Появляется всё больше исследований, подтверждающих феномен слепого доверия автоматизированным системам (Skitka et al., 1999; Parasuraman and Manzey, 2010). Объясняется это одним из присущих человеческому мышлению когнитивных искажений, **искажению автоматизации** (automation bias). Данное искажение приводит к том, что индивид упускает из внимания факторы и элементы, которые прямо не обозначены автоматизированной системой. Например, из двух равных вариантов система случайным образом выбрала один, в результате чего возникает возможность для дискриминации второго и всех последующих вариантов. Исследования также показывают склонность людей совершать ошибочные действия по рекомендации автоматизированной системы, даже если рекомендация противоречит опыту и другим доступным лицу достоверным данным. Например, многие поворачивают на улицу с односторонним движением в неправильном направлении по подсказке навигатора – хотя и видят запрещающие знаки.

Три перечисленных базовых свойства права как социального регулятора (содействие правовой определенности, повышение доверия к праву, устранение искажения автоматизации) выступают основными метриками (или, иначе говоря, критериями применения) как при проведении анализа регуляторных пробелов, так и при последующей разработке предложений по устранению выявленных недостатков законодательства. Четвертое базовое свойство относится не столько к результату, сколько к процессу правового регулирования: это необходимость **участия (представительства)** в ходе выработки подходов к правовому регулированию в сфере цифровой экономики - об этом уже говорилось выше применительно к международным подходам. Как будет показано ниже при рассмотрении лучшей практики по выработке концептуальных рамок для анализа, цифровая дискриминация является одним из самых существенных рисков для создаваемого цифрового общества. Поэтому максимально широкое привлечение всех заинтересованных сторон к обсуждению проекта, агрегация и учет их интересов являются базовым требованием как к выполнению проекта, так и к использованию его результатов.

Методика анализа

С учетом правовых основ и принципов, рассмотренных выше, анализ регулятивных пробелов проводился в соответствии со следующей методикой. За основу анализа была взята **структура**, предложенная на предыдущем этапе работы. В качестве исходной информации для анализа по каждому разделу изменений в законодательство составлен **перечень нормативных правовых актов**. Анализ сфокусирован на основных направлениях развития правового регулирования в сфере цифровой экономике.

Результаты анализа регулятивных пробелов изложены в краткой (табличной) и более полной форме (в форме комментариев). Табличное изложение выявленных недостатков законодательства является заделом для последующих этапов работы, в частности, для составления дорожной карты по внесению изменений в законодательство и её последующего обсуждения на специально созданной для этого цифровой платформе. Каждому выявленному недостатку в таблице присвоен **уникальный номер**, который необходим для отслеживания работы над выявленным недостатком на следующих этапах работы. Идеальным образом результата для проекта является устранение всех выявленных недостатков. Данная методология анализа регуляторных пробелов допускает её многократное применение, что позволит оценить результативность проекта по мере подготовки, а также принятия и вступления в силу изменений в законодательство.

На основе правовых основ и принципов, а также международного контекста, описанных выше, была подготовлена классификация выявленных недостатков. Классификация включает в себя четыре класса нормативных положений действующего законодательства Кыргызской Республики:

- **(П) пробел** - недостаток относится к классу пробелов, если, в соответствии с применимыми правовыми основами и принципами регулирование требуется, но соответствующие положения отсутствуют в законодательстве Кыргызской Республики;
- **(У) устаревшая норма** - положение относится к классу устаревших норм, если оно действует и применяется, но не соответствует применимым правовым основам и принципам, описанным выше, в силу чего оно подлежит замене или отмене;
- **(Б) барьер** - положение препятствует осуществлению чьих-либо интересов, при этом сами такие интересы могут считаться законными, а цель установления препятствия в нормативном правовом акте не соответствует применимым правовым основам и принципам, описанным выше, в силу чего устанавливающая препятствие норма подлежит замене или отмене;
- **(Н) неработающая норма** - положение закона или подзаконного нормативного правового акта фактически не применяется, исходя из имеющейся практики или экспертных оценок.

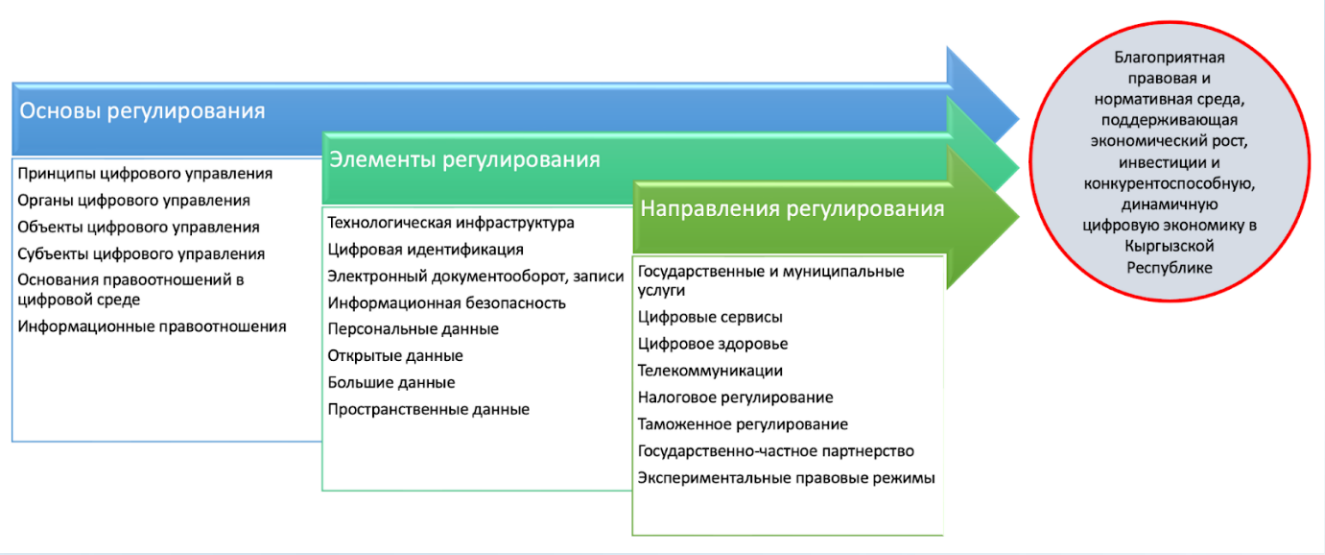
Каждому выявленному недостатку в рамках анализа сопоставляется применимая лучшая **зарубежная практика**, соответствующая применимым правовым основам и принципам, описанным выше. В рамках анализа, по возможности, был описан опыт нескольких стран или международных организаций, относящийся к рассматриваемому вопросу и так или иначе соответствующий применимым правовым основам и принципам. Хотя описанные при проведении анализа лучшие зарубежные практики не являются заведомым решением того регуляторного недостатка, к которому они относятся, информация о них может способствовать выработке решения по устранению недостатка.

Основные выводы по направлениям анализа

В соответствии с техническим заданием на услуги Консультанта, анализ был проведен, в частности, в отношении следующих сфер регулирования:

- Данные и цифровые/ИКТ технологии (распределение и доступ к информации в форме открытых данных, электронный документооборот, обработка и защита персональных данных, использование информационных ресурсов и систем, включая распределенный облачный документооборот, искусственный интеллект, блокчейн технологию, дата центры и их каналы передачи данных, защита цифровой информации, интернет-сервисы, мобильные приложения, электронные платежи, электронная идентификация, инфраструктура открытого ключа и цифровые подписи);
- Телекоммуникации (лицензирование и вопросы технического регулирования включая цифровые и телекоммуникационные инфраструктуры, лицензирование радиочастотного спектра, управление и мониторинг, управление ресурсами адресации и нумерации, сетевая взаимосвязанность, доступ к ключевым объектам и политикам «открытого доступа», кросс-инфраструктурное «dig once» регулирование, сетевая нейтральность, регулирование конвергированных голосовых данных, антимонопольное регулирование);
- Кибербезопасность (вопросы кибербезопасности, использование цифрового доказывания, криминализация и расследование киберпреступлений, защита критической инфраструктуры);
- Государственно-частное партнерство (внедрение моделей ГЧП в ИКТ сектор);
- Гражданский сектор (вопросы подписания и исполнения сделок и договоров присоединения в цифровой форме, обеспечение прав на цифровые активы, проведение сделок с такими активами, платежи в электронной форме);
- Банковский сектор и финансовые технологии (вопросы электронных денег, платежных систем, электронные платежные инструменты, передача электронных денежных средств, внедрение финансовых технологий в заинтересованные ведомства (Министерство финансов КР, Счетная палата КР, Национальный банк КР);
- Налоги (вопросы бухгалтерской и других отчетностей в цифровой форме, цифровая маркировка товаров, взаимодействие налогоплательщиков с налоговыми органами посредствам электронного документооборота;
- Таможенный сектор (вопросы таможенной очистки и контроля с использованием цифровых средств, таможенный контроль интеллектуальной собственности);
- Государственное управление и оказание государственных услуг (электронное управление, цифровые правительственные порталы, регулирование облачных технологий, предоставление государственных и муниципальных услуг в цифровой форме, электронный документооборот, платформа взаимосвязанности, повышение компетенций, улучшение цифровых навыков государственных служащих).

В целях последующего использования для разработки нормативной правовой базы Кыргызской Республики, материалы анализа расположены в соответствии со структурой, предложенной в рамках Результата 1.



Анализ **правовых основ цифрового управления** проводился в соответствии со следующими отраслевыми принципами, вытекающими из лучших практик регулирования в данной сфере:

- Цифровая трансформация процессов;
- Платформонезависимость и ориентация на мобильные устройства;
- Независимость от поставщиков и переносимость данных;
- Ориентированность на пользователя и право пользователя на информационное самоопределение;
- Цифровизация на всех этапах формирования и предоставления государственной услуги или бизнес-процесса;
- Правительство как платформа;
- Принятие управленческих решений на основе цифровых данных;
- Использование открытых данных;
- Использование открытых стандартов и свободного программного обеспечения;
- Технологическая нейтральность и открытость для инноваций и «подрывных» технологий
- Презумпция общедоступности информации

Главным выводом по результатам анализа стало то, что **в законодательстве Кыргызстана отсутствует описание структуры законодательных и иных нормативных правовых актов, содержащих нормы по регулированию цифровой экономики,** не содержится правил разрешения коллизий между различными актами, регулирующими отношения в цифровой среде. Законы Кыргызской Республики в цифровой сфере принимаются без учета друг друга, что порождает множество правовых коллизий. Снять эти коллизии позволяет выстраиваемая единая система цифрового управления в Кыргызской Республике.

Кроме того, **структура органов цифрового управления является фактически неработающей.** В ней также не представлены другие, кроме государства, субъекты цифрового управления, отсутствует разграничений полномочий по защите цифровой информации. Также предусмотренные в действующем законодательстве принципы электронного управления являются устаревшими, отражающими логику предыдущих этапов реформы государственного управления, поэтому они должны быть обновлены в соответствии с приведенными выше принципами и регуляторными рамками.

В рамках проводимого анализа регуляторных пробелов не проводился централизованный анализ терминологии, используемой в законодательстве. Анализ используемых терминов был проведен по отдельным направлениям регулирования в

соответствии с присущей им спецификой, составление же полноценного **глоссария** для регулирования цифровой экономики.

Перечисленные выше принципы должны учитываться относительно **объектов и субъектов цифрового управления**. В настоящее время законодательство не создает условий для цифрового управления, то есть управления, основанного на данных. Данные из государственных информационных систем не используются для принятия решений и аналитики как в государственном, так и в частном секторе, форматы данных и интерфейсы обмена данными в разных органах разные и несовместимые между собой, что препятствует построению интероперабельной системы принятия решений.

Закрепленная в статье 18 Закона КР «Об электронном управлении» многоуровневая модель регулирования отношений в зависимости от их объекта (инфраструктура, приложения, данные, сервисы) распространяется только на государственный сектор и, кроме того, не отражена в других законодательных актах КР, в том числе принятых позднее. При этом многоуровневый характер отношений в рамках цифровой экономики является данностью, которую нельзя не учитывать при регулировании отношений в данной области. В законодательстве КР отсутствует правовой режим распределенных информационных систем, а также отсутствуют условия для необходимого в условиях цифровой экономике перехода от электронного документооборота к управлению, основанному на записях в информационных системах, в том числе распределенных.

Отсутствие норм, допускающих возможность исключительно цифрового взаимодействия, не позволяет переходить в цифровое взаимодействие полноценно, так как государственные органы требуют бумажные документы. Отсутствует стандартизация в сфере электронного документооборота или оборота цифровых записей. Не урегулированы вопросы электронного документооборота с негосударственными организациями и физическими лицами, целые отрасли отрезаны от электронного документооборота или иного цифрового взаимодействия.

Внедрение цифровой национальной валюты также до настоящего момента не регламентировано, при том, что эмиссия и обращение такой валюты избавляет Национальный банк от расходов на печать реальной валюты, а ее распространенность будет способствовать развитию рынка цифровых платежей. Необходимо вносить пакетные изменения в налоговое, гражданское и банковское законодательство для полноценного внедрения цифровых финансовых активов и криптовалют, а для надзора и администрирования - в административное и уголовное законодательство, создав в совокупности легальную систему по нормированию различного вида денежных единиц на рынке Кыргызской Республики.

В действующем законодательстве отсутствует система основных акторов (субъектов) цифрового управления, что не позволяет выстроить систему отношений в цифровой среде именно как систему. При этом регулирование статуса каждого из этих субъектов должно осуществляться в рамках регулирования соответствующего вида деятельности в цифровой экономике. В области цифровой экономики появляющиеся новые субъекты, такие как владельцы цифровых платформ или экосистем, остаются невидимыми для отраслевого и антимонопольного законодательства, которое не в состоянии сдерживать концентрацию в их руках значительной рыночной власти и, как следствие, не могут устранять неравенство в экономической сфере. Эффективное цифровое управление требует, прежде всего, регулирования деятельности таких новых субъектов на межотраслевой базе.

Правовые основы регулирования **отношений в цифровой среде, в том числе оснований их возникновения** также должны основываться на принципах презумпции общедоступности информации, равенства участников отношений в цифровой среде и технологической нейтральности. Законодательство Кыргызстана в данной сфере нуждается в унификации разных источников информации, выступающих в виде «старых» (СМИ) и «новых» (соцсети, каналы в мессенджерах и т.п.) медиа, что требует пересмотра деятельности различных медиа на базе общих принципов свободы слова, законности и справедливости распространения информации. С точки зрения базовых требований к правовому

регулированию в условиях цифровой экономики важным выводом по результатам анализа является то, что в законодательстве Кыргызской Республики отсутствует правовой режим доверенных услуг (таких как гарантированная доставка или отметка времени), что препятствует развитию отношений в цифровой экономике и повышению уровня доверия в ней.

Проблемой является то, что в законодательстве, прежде всего, в статье 12 Закона КР «Об электронном управлении» общедоступная информация рассматривается как правовой режим информации, противостоящий конфиденциальной информации. Такой подход является устаревшим, поскольку не создает условий для закрепления баланса между интересом общества в использовании информации (в частности, выраженном в свободе слова) и правами обладателей информации на ограничение доступа к ней, если им соответствующее полномочие предоставлено законом. Режим доступа к информации плохо структурирован и не систематизирован, что приводит к значительным наложениям и нестыковкам между режимами разных тайн, значительно затрудняющим использование соответствующей информации, в том числе такое использование, которое не может нарушать права лиц, к которым относится та или иная тайна.

Размещение информации из информационных систем государственных органов и органов местного самоуправления на сайтах государственных органов и органов местного самоуправления в Интернете в формате открытых данных фактически не производится из-за того, что в законодательстве отсутствуют процедуры (практические рекомендации) по публикации открытых данных. Также, **в законе не закреплены правовые основания для использования свободных программных продуктов и открытого API** (Application Programming Interface).

В законодательстве КР отсутствуют базовые положения о защите информации и обеспечении **кибербезопасности**. Профильный закон, в котором такого рода положения должны содержаться – об электронном управлении – содержит лишь положения о защите права на доступ к информации и защите прав обладателя информации. Эти права являются важными элементами кибербезопасности, однако ни защита информации, ни обеспечение кибербезопасности не могут быть сведены лишь к правам основных участников правоотношений в цифровой среде. В связи с этим базовые положения об обеспечении кибербезопасности, в частности, о стандартизации и техническом регулировании в данной области должны быть закреплены на уровне закона.

Ситуация с защитой **персональных данных**, прежде всего, осложняется устаревшим законодательством – с момента принятия Закона «Об информации персонального характера» прошло более 10 лет, за это время произошли глобальные технологические изменения, внедряются новые информационные и коммуникационные технологии. Изменился не только подход к сбору личной информации, но и отношение общества к этой проблематике.

Одно из таких глобальных изменений в международных стандартах защиты персональных данных - определение новых прав, предоставляемых гражданам, для управления своими персональными данными при их обработке, в том числе на основе математических алгоритмов, искусственного интеллекта; обязанность держателей персональных данных уведомлять уполномоченный орган и граждан об утечках персданных. Еще одним недостатком действующего закона об информации персонального характера является требование к форме согласия на обработку персональных данных – в письменной (оффлайн) или в электронной (онлайн) форме, подписанное электронной подписью.

Действующий закон не признает выражение лицом своей воли с помощью электронных или иных технических средств. В законе не установлены все признаваемые международными актами юридические основания для работы с персональными данными (например, наличие договора), не ясны исключения на получение согласия для законной обработки данных, например, для школ, которые не являются государственными органами, имеющими исключение на получение согласия при исполнении своих функций.

В общем контексте современных подходов к защите прав граждан на неприкосновенность частной жизни является право на получение информации о несанкционированном доступе третьих лиц к их персональным данным, право заявить о своем несогласии, независимо от места жительства получать квалифицированную защиту, в том числе и от уполномоченного органа. Эти нормы также отсутствуют в кыргызском законодательстве, как и меры ответственности за правонарушения и преступления с персональными данными, в связи с чем необходимы дополнения в кодексы – о правонарушениях, уголовный.

Определяющими факторами при этом должны стать вопросы не столько наказаний за допущенные нарушения, сколько восстановления нарушенных прав субъектов и восстановлением причиненного им незаконными действиями вреда. Режим трансграничных потоков данных также является вызовом в рамках интеграции Кыргызстана в Евразийском экономическом союзе, в цифровой повестке которого создание общего для ЕАЭС рынка и оборота (свободного перемещения) персональных данных граждан. Также до сих пор недостаточно четко определены полномочия и компетенция уполномоченного государственного органа по защите персональных данных.

В Кыргызской Республике отсутствует законодательство, регулирующее использование технологий **больших данных и искусственного интеллекта.** Ещё один важнейший для цифровой экономики вид данных - **пространственные данные** - основан на устаревшем Законе Кыргызской Республики «О геодезии и картографии», который не удовлетворяет существующие потребности по обеспечению правового регулирования пространственных данных и не содержит достаточных условий для создания и развития национальной инфраструктуры. Действующими нормативными правовыми актами Кыргызской Республики не урегулированы вопросы сбора, хранения, обработки, распространения, защиты, пользования пространственными данными и метаданными, отсутствует правовое регулирование вопросов стандартизации пространственных данных.

Проблемы **управления идентичностью** в Кыргызской Республике связаны с тем, что полноценно не развернута инфраструктура электронных подписей или иных, более современных способов управления идентичностью, а применимые стандарты являются коммерческими, и разрабатываются Российской Федерацией и Республикой Казахстан, что ставит внутренний рынок Кыргызской Республики в зависимое положение. Необходимо внедрение на национальном уровне требований, правил и стандартов по генерации электронных подписей в соответствии с международными требованиями, одновременно с принятием единых требований к сертификатам электронных подписей на уровне Евразийского экономического союза.

Органы судебной системы в настоящее время не признают цифровые доказательства в судебных разбирательствах из-за отсутствия компетенций и непонимания цифрового законодательства. Отсутствует порядок хранения электронных документов, записей (информации) в цифровой форме, законодательство о цифровом (электронном) архиве. Законодательство, регулирующее использование идентификационной карты – паспорта гражданина (ID-карты), не позволяют широко использовать возможности данного инструмента, отсутствуют возможности использования иных средств, таких как токены, коды, идентификация по sms, видеоидентификация.

Законодательные возможности цифровой идентификации существенно ограничены сферой государственного управления – предоставлением государственных услуг и участия избирателей в выборах и референдумах. Например, не предусматриваются возможности цифровой идентификации при взаимодействии в рамках электронной коммерции. Законодательное регулирование биометрической идентификации ограничено сферами миграционных и избирательных правоотношений, а законодательство, регулирующее правовой статус Единой системы идентификации, не предполагают возможностей её

широкого использования непосредственно в целях идентификации, не предполагают подключения к ней коммерческих банков и иных организаций. Все эти недостатки особенно ярко проявляются в свете активной работы на различных международных площадках, прежде всего, ЮНСИТРАЛ, по определению принципов и механизмов управления идентичностью, а, следовательно, результаты работы международных групп экспертов на этих площадках должны учитываться при разработке кыргызского законодательства в сфере управления идентичностью.

Анализ в сфере правового регулирования **цифровых сервисов** основывался на принципах безопасности цифровой среды, здоровой конкуренции между цифровыми сервисами в рамках деятельности цифровых платформ, свободы перехода пользователей между цифровыми сервисами, свободы распоряжения пользователями своими данным, гарантий открытости информации о сервисе. С этой точки зрения необходимо закрепить отсутствующие в настоящий момент в законодательстве требования, позволяющих обеспечить добросовестную конкуренцию в информационном поле, и предусмотреть гарантии обеспечения защиты персональных данных пользователей.

Аналогично и в законодательстве о предоставлении **государственных и муниципальных услуг** должны быть реализованы отсутствующие в настоящее время принципы проактивности предоставления государственных и муниципальных услуг, электронного способа подачи заявлений, приоритета «реестровой» модели, преимущественно или только исключительное цифровое взаимодействие между органом при предоставлении услуги с получателем, «опережающее» предложение о возможности получения той или иной услуги еще до момента наступления юридического события.

В законодательстве Кыргызской Республики в настоящее время также отсутствует однозначный запрет обуславливать предоставление государственных и муниципальных услуг обработкой биометрических данных, в связи с чем необходимо закрепление гарантий реализации права на отказ от предоставления своей биометрической информации без утраты возможности получить государственные и муниципальные услуги в электронной форме.

В сфере сервисов **цифрового здоровья и благополучия** не закреплены основополагающие принципы развития системы электронного здравоохранения, а также выявлены отдельные пробелы в части вопросов обеспечения безопасности медицинских персональных данных, например:

- не определен порядок выдачи и получения информированного добровольного согласия и согласия на обработку персональных данных пациента на основе конклюдентных действий при получении медицинских услуг с использованием телемедицинских технологий;
- не определен порядок и случаи передачи персональных медицинских данных третьей стороне;
- не урегулированы отдельные вопросы обработки персональных медицинских данных в медицинских информационных системах.

Из других выявленных пробелов в данной области можно указать то, что не определен порядок сооплаты при получении медицинских услуг с использованием телемедицинских технологий для участия частных компаний в рамках государственно-частного партнерства, не урегулирован порядок использования устройств дистанционного мониторинга состояния здоровья и физиологических параметров домашнего применения и стационарозамещающих технологий, не предусмотрен порядок использования со стороны пациента простой электронной подписи при получении медицинских услуг с использованием телемедицинских технологий.

Самостоятельные (отдельные) правовые акты в сфере **технологической инфраструктуры цифрового управлени**я в Кыргызской Республике отсутствуют, в связи с чем анализ проводился в отношении соответствующих нормативных и ненормативных правовых актов по вопросам создания и эксплуатации отдельных видов и даже объектов инфраструктуры (в том числе, документы стратегического планирования). Закон Кыргызской Республики «Об электронном управлении» предусматривает регулирование только государственных центров обработки данных. Законодательно не закреплены вопросы стандартизации центров обработки данных. Законодательством о техническом регулировании не предусмотрены достаточные механизмы принятия на национальном уровне международных стандартов.

Данные пробелы в законодательстве требуют устранения путем создания и эксплуатации технологической инфраструктуры цифрового управления в Кыргызской Республике с учетом принципов недискриминационного доступа к инфраструктуре; отчуждаемости инфраструктуры электронного взаимодействия от ее разработчиков, поставщиков и эксплуатирующих организаций; определенности порядка использования инфраструктуры электронного взаимодействия; взаимной совместимости информационных систем инфраструктуры электронного взаимодействия; стабильности и преемственности характеристик инфраструктуры электронного взаимодействия; максимального использования возможностей рынка; безопасности персональных данных и информации ограниченного доступа.

Законодательные нормы, регулирующие вопросы создания **сетей связи**, их эксплуатации, а также использования ресурсов электросвязи, включены в различные отраслевые законодательные акты и зачастую не согласованы между собой. В связи с этим необходимо системное приведение норм, относящихся к вопросам сетей и ресурсов электросвязи (телекоммуникаций), в соответствии с отраслевым (специальным) законодательством, с возможным исключением их из иных законодательных актов в целях избежания ненужного дублирования и избыточного регулирования. В законе КР об электрической и почтовой связи необходимо исключить положения, касающиеся почтовой связи ввиду наличия отраслевого (специального) закона КР «О почтовой связи».

Закрепленный законом принцип всемерной поддержки предоставления высококачественных традиционных и инновационных услуг электрической и почтовой связи не конкретизирован и на практике никак не реализуется. В частности, закон не содержит положений, облегчающих использование радиоспектра для оказания перспективных услуг и освоения новых технологий («интернет вещей», системы искусственного интеллекта и т.п.). Терминологию данного закона необходимо привести в соответствие с глоссарием Международного союза электросвязи.

В законе также содержится неработающая норма о компенсации убытков, понесенных оператором услуг электросвязи из-за приостановления его деятельности, в связи с чем требуется регламентация порядка соответствующей компенсации из бюджета. Не работает и положение об учёте строительными и иными организациями требований операторов связи о размещении их технических средств, поскольку отсутствует ответственность застройщика за неисполнение этой нормы. Также не работают или содержат в себе существенные барьеры нормы об отчислениях на развитие отрасли связи и дополнительном налогообложении телекоммуникационных услуг, а методика расчёта ежегодной платы за использование номиналов и (или) полос радиочастот радиочастотного спектра не направлена на стимулирование расширения сети и снижения финансового бремени на оператора связи.

Ст. 30 закона КР об электрической и почтовой связи «**Межсетевое соединение** (сопряжение)» адресована в основном «доминирующим» операторам, содержит неоднозначную терминологию и не даёт возможности развитию межоператорских отношений на основе равноправных соглашений между операторами, отходя от логики построения телефонных (фиксированных) сетей связи.

Общемировая тенденция в сфере регулирования межоператорских отношений основана на принципе технологической нейтральности при пропуске межсетевого трафика, и отказа от жёстких требований к построению иерархических сетей фиксированной связи, и на снижение тарифов на интерконнект: «операторы должны зарабатывать на своих клиентах, а не на своих конкурентах». Правила межсетевого соединения в Кыргызской Республике также сохраняют устаревшую логику требований к сетям, функционирующих на основе коммутации каналов, а не маршрутизации пакетов. Кроме того, действующее законодательство в сфере связи не содержит положений об устранении (или существенном сокращении) тарифов на интерконнект, в первую очередь при трансграничном межоператорском взаимодействии в рамках интеграционных объединений с участием Кыргызской Республики (ЕАЭС, СНГ и др.) – вопрос о снижении (до минимального уровня) ставки интерконнекта и отмены международного роуминга.

В законодательстве Кыргызской Республики вопросы, относящиеся к регулированию **услуг связи**, правам и обязанностям пользователей (абонентов) и операторов (поставщиков) услуг электросвязи в целом решены на достаточно удовлетворительном уровне, без тех особенностей и неопределённости регулирования, которые в последние годы стали характерны для телекоммуникационного законодательства ряда стран СНГ. В то же время остаются открытыми (требующими нормативного уточнения) вопросы не сколько об объёме правомочий и обязанностей операторов связи, а о том, кто именно и по каким критериям может или должен быть отнесён к числу операторов. Это возвращает проблематику правового регулирования услуг связи к более фундаментальным вопросам – о принципах лицензионно-разрешительной деятельности в области электросвязи, о стимулировании развития и потребления новых услуг, создающих добавленную стоимость, а также о порядке взаимодействия между сетями электросвязи лицензированных операторов и техническими средствами владельцев OTT-сервисов. Также нельзя не отметить, что действующее законодательство Кыргызской Республики не содержит положений о подлинно независимом статусе регулятора в сфере электросвязи.

Международный опыт (в том числе в странах СНГ) свидетельствует о желательности и **необходимости обеспечения независимого статуса регулирующего органа в сфере электросвязи.** Независимость регулирующего органа в сфере электросвязи является важнейшим фактором повышения взаимного доверия и плодотворного взаимодействия между государственными и негосударственными организациями в области цифровой трансформации.

Анализ проводился также в отношении тех отраслей и актов законодательства, в которые могут потребоваться изменения в связи с разработкой цифрового законодательства Кыргызской Республики. Так, в области **государственно-частного партнерства** был выявлен ряд недостатков существующего регулирования, связанных с тем, что Закон Кыргызской Республики «О государственно-частном партнерстве» не допускает включение в другие законы норм, предметом регулирования которых является государственно-частное партнерство.

В существующем законе отсутствуют механизмы, обеспечивающие конкуренцию и создание равных и справедливых условия для всех участников процесса прохождения отбора конкурса, и как следствие нарушение принципов государственно-частного партнерства (прозрачности деятельности, справедливости, справедливого распределения рисков) при отборе победителя конкурса. И напротив, хотя в законе упоминается возможность присуждения проекта государственно-частного партнерства путем прямых переговоров, сама процедура проведения прямых переговоров отсутствует.

Специфика развития информационных технологий и постоянно растущего объёма элементов базы данных не может быть предметом соглашения о государственно-частном партнерстве, финансируемого за счет государственного бюджета (при отсутствии бюджетных средств), поскольку необходимо постоянное непрерывное совершенствование и модернизация информационных систем, и возможности этого процесса могут быть объектом долгосрочной

поддержки частных инвестиций нежели государства. И в этой связи, может оказаться целесообразным разработать отдельный закон о государственно-частном партнерстве в цифровой сфере.

В **Гражданском кодексе** Кыргызстана не упомянут смарт-контракт, не определен гражданско-правовой режим цифровых прав и виртуальных активов, не определены связанные с этим понятия, что требует внесения соответствующих изменений. Законодательство, регулирующее профессиональную переподготовку и повышение **квалификации государственных служащих**, не содержит в себе требований по обучению цифровым навыкам и компетенциям. Также в нём отсутствуют установленные показатели эффективности, не предусмотрены онлайн-обучение и сертификация, возможность создания цифровых команд в ведомствах.

В **налоговом законодательстве** не определены базовые принципы, конкретные задачи и насущные приоритеты налоговой политики в рамках перехода к цифровой экономике, не определены базовые понятия, а в отношении уже введенного “цифрового налога” недостаточно четко определены критерии, относящиеся к субъектам и объектам налогообложения.

В сфере **таможенного законодательства** приходится сделать вывод о неполном использовании потенциала института электронного предварительного информирования, о дублировании при проведении государственных видов контроля на границе, о необходимости упрощения и оптимизация контроля доставки товаров, а также о необходимости разработать технологии совершения операций в упрощенном, ускоренном режиме для отдельных категорий товаров. Законодательство Кыргызской Республики прямо не регулирует вопросы использования **облачных технологий** и не закрепляет соответствующие понятия.

По результатам анализа также важно обратить внимание, что закон о "**регуляторных песочницах**” в Кыргызской Республике отсутствует. Это запрещает возможность использования механизма "регулятивной песочницы" при апробировании новых правоотношений, поддержки инноваций в цифровой сфере, также нет механизмов партнерства, государственной поддержки технологических стартапов.

Источники

1. ITU (2020) *ITU | ICT Regulatory Tracker*. Available at: https://app.gen5.digital/tracker/metrics (Accessed: May 7, 2022).
2. ITU (2021a) *Benchmark of fifth-generation collaborative regulation*.
3. ITU (2021b) *The impact of policies, regulation, and institutions on ICT sector performance*.
4. ITU and The World Bank (2020) *Digital Regulation Handbook International Telecommunication Union*. Geneva.
5. OECD (2020a) *Going Digital integrated policy framework*. Paris. Available at: https://doi.org/10.1787/dc930adc-en (Accessed: May 4, 2022).
6. OECD (2020b) "Vectors of digital transformation," *OECD Digital Economy Papers*, No. 273. Available at: https://doi.org/10.1787/5ade2bba-en (Accessed: May 5, 2022).
7. Portulans Institute (2021) *Network Readiness Index 2021 Kyrgyzstan*. Available at: https://networkreadinessindex.org/country/kyrgyzstan/ (Accessed: May 7, 2022).
8. Масаладжиу Р. Принцип правовой определенности в науке, практике ЕСПЧ и его влияние на доступность правосудия на стадии надзорного производства в гражданском и арбитражном процессе // Арбитражный и гражданский процесс. 2009. № 7.
9. LINDA J. SKITKA, KATHLEEN L. MOSIER, MARK BURDICK. Does automation bias decision-making? International Journal of Human-Computer Studies, Volume 51, Issue 5, 1999, Pages 991-1006, ISSN 1071-5819, https://doi.org/10.1006/ijhc.1999.0252
10. Parasuraman R, Manzey DH. Complacency and Bias in Human Use of Automation: An Attentional Integration. Human Factors. 2010; 52(3): 381-410. doi:10.1177/0018720810376055

Раздел 1. Правовые основы цифрового управления

Содержание

- структура (с учётом текущей цифровой повестки)
- соотношение правовых актов
- регулируемые отношения
- принципы цифрового управления
- органы цифрового управления; участие всех заинтересованных сторон в управлении

Текущее регулирование (действующее законодательство):

1. Закон Кыргызской Республики «Об электронном управлении»
2. Закон Кыргызской Республики «Об электронной подписи»
3. Закон Кыргызской Республики «Об инновационной деятельности»
4. Закон Кыргызской Республики «О виртуальных активах»
5. Закон Кыргызской Республики «Об электронной торговле»
6. Закон Кыргызской Республики «Об электрической и почтовой связи»
7. Закон Кыргызской Республики «О доступе к информации, находящейся в ведении государственных органов и органов местного самоуправления Кыргызской Республики»
8. Закон Кыргызской Республики «О государственных закупках»
9. Закон Кыргызской Республики «Об информации персонального характера»
10. Закон Кыргызской Республики «О биометрической регистрации граждан Кыргызской Республики»
11. Закон Кыргызской Республики «Об органах национальной безопасности Кыргызской Республики»
12. Указ Президента Кыргызской Республики «О Национальной программе развития Кыргызской Республики до 2026 года» от 12 октября 2021 года УП №435
13. Указ Президента Кыргызской Республики «О дальнейших мерах цифровой трансформации Кыргызской Республики» от 21 июля 2021 года УП №305
14. Указ Президента Кыргызской Республики «О неотложных мерах по активизации внедрения цифровых технологий в государственное управление Кыргызской Республики» от 17 декабря 2020 года УП №64
15. Постановление Кабинета Министров Кыргызской Республики «Об утверждении Плана мероприятий Кабинета Министров Кыргызской Республики по реализации Национальной программы развития Кыргызской Республики до 2026 года» от 25 декабря 2021 года №352
16. Постановление Кабинета Министров Кыргызской Республики «О создании государственного учреждения «Проектный офис» от 16 августа 2021 года № 137
17. Постановление Правительства Кыргызской Республики «Об утверждении Правил пользования Государственным порталом электронных услуг» от 7 октября 2019 года № 525
18. Постановление Правительства Кыргызской Республики «Об утверждении Требований к защите информации, содержащейся в базах данных государственных информационных систем» от 21 ноября 2017 года №762
19. Постановление Правительства Кыргызской Республики «Об утверждении Положения о государственной системе электронных платежей» от 28 октября 2017 года № 709
20. Постановление Правительства Кыргызской Республики «Об утверждении Требований к взаимодействию информационных систем в системе межведомственного электронного взаимодействия "Түндүк"» от 11 апреля 2018 года № 200
21. Постановление Правительства Кыргызской Республики «О реализации пилотного проекта "Государство как платформа" по внедрению инновационных способов

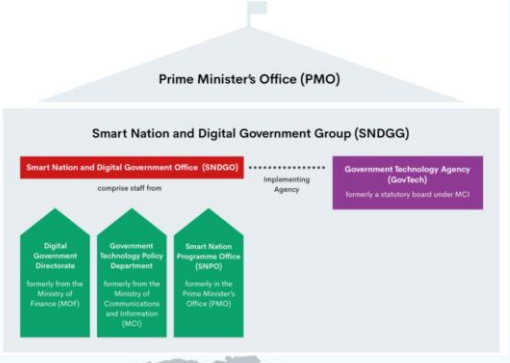
предоставления государственных и муниципальных услуг и сервисов» от 25 февраля 2020 года №113

22. Постановление Правительства Кыргызской Республики «О некоторых вопросах, связанных с использованием электронной подписи» от 31 декабря 2019 года № 742
23. Постановление Правительства Кыргызской Республики «Об утверждении Положения о государственной системе электронных сообщений и правилах ее использования» от 31 декабря 2019 года № 745
24. Постановление Правительства Кыргызской Республики «Об утверждении Положения об автоматизированной информационной системе «Государственная система электронного документооборота» от 30 октября 2020 года № 526
25. Постановление Правительства Кыргызской Республики «О Типовой инструкции по делопроизводству в Кыргызской Республике» от 3 марта 2020 года № 120
26. Постановление Правительства Кыргызской Республики «О некоторых вопросах, связанных с государственными информационными системами» от 31 декабря 2019 года № 744
27. Постановление Правительства Кыргызской Республики «Об утверждении Требований к государственным центрам обработки данных и соединяющим их каналам связи» от 31 декабря 2019 года № 747
28. Постановление Правительства Кыргызской Республики «Об отдельных вопросах осуществления электронного управления в Кыргызской Республике» от 31 декабря 2019 года № 748
29. Постановление Правительства Кыргызской Республики «О некоторых вопросах, связанных с государственной инфраструктурой электронного управления» от 5 декабря 2019 года № 661
30. Постановление Правительства Кыргызской Республики «Об отдельных вопросах, связанных с базовыми государственными информационными ресурсами» от 6 февраля 2020 года № 66
31. Распоряжение Кабинета Министров Кыргызской Республики от 2 июля 2021 года № 74-р
32. Распоряжение Кабинета Министров Кыргызской Республики от 12 января 2022 года №2-р
33. Концепция цифровой трансформации «Цифровой Кыргызстан 2019-2023»

Краткое описание выявленных недостатков и ориентиров из мировой практики

№	Описание недостатка	Тип[6]	Лучшая практика
1.1	В законодательстве отсутствует описание структуры законодательных и иных нормативных правовых актов, содержащих нормы по регулированию цифровой экономики, не содержится правил разрешения коллизий между различными актами, регулирующими отношения в цифровой среде	**П**	Проект разработки законодательства в цифровой сфере в Кыргызской Республике является уникальным и не имеет аналогов в мировой практике. В то же время, является, во многом, вынужденной мерой, вызванной тем, что законы Кыргызской Республики в цифровой сфере принимаются без учета друг друга, что порождает множество правовых коллизий. Снять эти коллизии позволяет выстраиваемая единая система цифрового

[6] В таблице приводятся следующие типы недостатков регулирования:
(П) пробел в регулировании (регулирование требуется, но его нет)
(У) устаревшая норма (норма есть, но её нужно менять)
(Н) неработающая норма (норма есть, но в силу описанных причин она не работает)
(Б) действующая норма является необоснованным препятствием для осуществления деятельности

			управления в Кыргызской Республике
1.2	Структура органов цифрового управления является фактически неработающей. Кроме того, в ней не представлены другие, кроме государства, субъекты цифрового управления. Координацию перехода к электронному управлению в Кыргызской Республике осуществляют: 1) Совет по электронному управлению и развитию информационно-коммуникационных технологий при Правительстве Кыргызской Республики (далее - Совет), являющийся высшим органом по координации перехода к электронному управлению в Кыргызской Республике; 2) Межведомственная комиссия по координации информатизации (далее - Комиссия), обеспечивающая межведомственное согласование и координацию ведомственных проектов перехода к электронному управлению в органах исполнительной власти Кыргызской Республики, органах местного самоуправления, государственных и муниципальных предприятиях и учреждениях, в том числе в процессе внедрения и предоставления электронных государственных и муниципальных услуг. Однако данные совещательные органы последние 4 года не собирали совет и комиссию и не выполняли свою деятельность в рамках законодательства Кыргызской Республики. К примеру, в законе прописывается, что совет согласовывает НПА в сфере электронного управления, при этом на практике в последние годы НПА принимались согласно законодательству и регламенту Правительства без согласования с Советом. В рамках Указа Президента Кыргызской Республики “О дальнейших мерах цифровой	**Н**	В США в рабочую группу Электронного правительства входит около 90 государственных служащих, представляющих около 50 государственных структур. Нормативно деятельность рабочей группы закреплена «Стратегией электронного правительства». Рабочая группа электронного правительства определила ключевые федеральные проблемы, которые можно решить с помощью концепций электронного правительства и электронного бизнеса. В Сингапуре органы цифрового управления подчиняются напрямую премьер-министру (главе государства) и подразделяются на Офис Умного Народа и Электронного Управления (координационный орган, включающий представителей министерства финансов, министерства коммуникаций и информации, администрации премьер-министра) и Агентства по технологиям управления (исполнительный орган, реализующий государственную политику в сфере цифровой трансформации). Прямая координация планов цифровой трансформации и их имплементации является наиболее эффективной формой управления цифровой трансформацией. l 

	трансформации КР” от 21 июля 2021 года УП №305 был реализован Наблюдательный совет по вопросам цифровизации при Президенте Кыргызской Республики, однако и он функционирует фрагментарно и не формирует единую картину цифрового развития в целом.		
1.3	Отсутствие разграничения полномочий по защите цифровой информации (Пример: ГКНБ является основным органов по защите государственных секретов, в том числе конфиденциальной информации, однако именно ГАЗПД является органом по защите ПД, что должно быть реализовано, однако именно в этом моменте имеется проблема защиты данных, поскольку в силу своей специфики ГКНБ реализует необходимые мероприятия по защите государственных секретов, а не ПД) Вывод: необходимо строгое разграничение полномочий, которые относятся к защите отдельных видов информации, либо закрепление этих полномочий за единственным органом цифрового управления	**Б**	Данная ситуация является специфической для структуры государственных органов Кыргызской Республики, с учетом истории их создания и развития
1.4	Предусмотренные в действующем законодательстве принципы электронного управления являются устаревшими По сути, электронное правительство является самой первой начальной стадией зрелости, и двигаться нужно к цифровому управлению, которое (как и цифровая экономика) характеризуется массовым использованием данных, когда операции автоматизированы и решения принимаются на основе данных	**У**	Страны, которые проходят через цифровую трансформацию и строят цифровую экономику, внедряют полностью «цифровое» и «умное» правительство, а не электронное. Ключевое различие между моделями электронного правительства и цифрового заключается в переходе от предоставления онлайновых гос.услуг к подходу, ориентированному на использование данных. Цифровые сервисы, ориентированные на пользователя, требуют горизонтальной интеграции и взаимодействия различных государственных органов. Инициативы по созданию цифрового правительства часто предполагают также изменения в организации системы управления. Чтобы идти в одном фарватере цифрового развития со всеми странами, провозгласившими

			построение цифровой экономики парадигмой собственного развития, необходимо разрабатывать правовые основы цифрового управления – как управления основанного на данных. Простой «апгрейд» уже устаревших подходов «электронного» правительства не сработает, необходимы инновационные регуляторные меры, экосистемный подход.

Комментарии

В целях построения информационного общества, а также консолидации усилий государственных органов, бизнеса и гражданского сообщества, направленных на ускорение цифровой трансформации и социально-экономического развития страны важнейшей задачей госорганов и органов МСУ принята концепция цифровой трансформации «Цифровой Кыргызстан 2019-2023». В рамках реализации дорожной карты указанной Концепции государственными органами власти проводятся различные мероприятия и реализуются проекты, направленные на построение цифровой инфраструктуры, повышения человеческого потенциала, реинжиниринга процессов государственного взаимодействия и управления.

В то же время, в законодательстве Кыргызстана отсутствует описание структуры законодательных и иных нормативных правовых актов, содержащих нормы по регулированию цифровой экономики, не содержится правил разрешения коллизий между различными актами, регулирующими отношения в цифровой среде. Законы Кыргызской Республики в цифровой сфере принимаются без учета друг друга, что порождает множество правовых коллизий. Снять эти коллизии позволяет выстраиваемая единая система цифрового управления в Кыргызской Республике.

В соответствии с Законом КР «Об электронном управлении», государственное регулирование электронного управления осуществляется Правительством Кыргызской Республики. Координацию перехода к электронному управлению в Кыргызской Республике осуществляют:

1) Совет по электронному управлению и развитию информационно-коммуникационных технологий при Правительстве Кыргызской Республики (далее - Совет), являющийся высшим органом по координации перехода к электронному управлению в Кыргызской Республике;

2) Межведомственная комиссия по координации информатизации (далее - Комиссия), обеспечивающая межведомственное согласование и координацию ведомственных проектов перехода к электронному управлению в органах исполнительной власти Кыргызской Республики, органах местного самоуправления, государственных и муниципальных предприятиях и учреждениях, в том числе в процессе внедрения и предоставления электронных государственных и муниципальных услуг.

Однако данные совещательные органы последние 4 года не собирали совет и комиссию и не выполняли свою деятельность в рамках законодательства Кыргызской Республики. К примеру, в законе прописывается, что совет согласовывает НПА в сфере электронного управления, при этом на практике в последние годы НПА принимались согласно законодательству и регламенту Правительства без согласования с Советом.

В рамках Указа Президента Кыргызской Республики “О дальнейших мерах цифровой трансформации КР” от 21 июля 2021 года УП №305 был реализован Наблюдательный совет по вопросам цифровизации при Президенте Кыргызской Республики, однако и он функционирует фрагментарно и не формирует единую картину цифрового развития в целом.

Необходимость в пересмотре структуры органов по управлению цифровой трансформацией подсказывает и мировой опыт. В Соединенных Штатах Америки в качестве электронного правительства выступают федеральные информационные системы, которые осуществляют взаимодействие Правительства с гражданами, с неправительственными организациями и сообществами.

Основы электронного правительства США были заложены формированием и функционированием www.data.gov. Особенностью данного портала является то, что его формирование и развитие происходит только с помощью административного воздействия на государственных служащих. К примеру, в 2009 году на директивном уровне предписывалось всем органам государственной власти опубликовывать информацию, представляющую хоть какую-нибудь ценность. На указанном портале находится достаточно много полезных приложений для пользователей.

В США в рабочую группу Электронного правительства входит около 90 государственных служащих, представляющих около 50 государственных структур. Нормативно деятельность рабочей группы закреплена «Стратегией электронного правительства». Рабочая группа электронного правительства определила ключевые федеральные проблемы, которые можно решить с помощью концепций электронного правительства и электронного бизнеса. Обзор деятельности рабочей группы показал, что основным препятствием на пути создания электронного правительства, ориентированного на граждан, является избыточность и дублирование функций и видов деятельности в различных государственных органах.

К примеру, в 2010 году было выявлено, что из 30 функций 22 исполняются в министерствах и ведомствах, а каждое министерство в среднем исполняет 19 различных функций. Такое положение приводит к разработке большого количества отчетов-дубликатов, для создания которых необходимо посетить десятки и сотни веб-страниц и обратиться в сотни call-центров для того, чтобы получить запрашиваемую услугу.

В настоящее время деятельность американского электронного правительства использует следующие фундаментальные принципы:

- цель – это граждане, а не бюрократия;
- конкретный результат действия Электронного правительства;
- инновационность в развитии.

Электронное правительство является необходимым фактором деятельности органов государственной власти, поскольку первым пользователем информационных технологий являются сами государственные служащие.

Основные причины, которые тормозят продвижение информационных технологий в государственном управлении, следующие:

1) для правительственных учреждений важна собственная оценка и собственный самоанализ без учета гражданских потребностей;

2) чиновники в большинстве своем используют информационные технологии в качестве пишущих машинок и калькуляторов, но не для принятия управленческого решения;

3) правительственные чиновники считают, что информационные технологии несут угрозу их командному положению, поэтому не стоит инвестировать финансы в развитие информационно-коммуникационных технологий;

4) большинство правительственных учреждений не организуют совместное функционирование собственных информационных потоков.

В настоящее время американское правительство поддерживает проектную деятельность, которая направлена на организацию совместной деятельности всех государственных структур, при этом применяются самые разнообразные форматы: формат электронного снабжения, формат электронных грантов, формат электронного регулирования, формат электронной подписи.

Таким образом, по США можно сделать вывод о том, что формат электронного правительства предполагает запрос требований для собственной деятельности, то есть оно

исполняет функции для внешний пользователей и не исполняет внутренние управленческие функции.

В **европейских государствах** информационное общество определяется следующими факторами и условиями:

- национальная информационная инфраструктура;
- интегрированная экономика;
- востребованность информационных ресурсов;
- свободная конкуренция.

Изначально незаменимый положительный опыт информационного обеспечения управленческих процессов накоплен в Соединенных Штатах Америки, поэтому проанализируем процессы информационной поддержки и информационного обеспечения в США с точки зрения возможностей применения данного опыта в Кыргызской республики. Интернет-ресурсы изначально были сформированы и применены в оборонном ведомстве (Пентагон) – это была первая сеть ARPAnet. Далее «Калифорнийское чудо» («кремневая долина») явилось следствием «Вашингтонского консенсуса» (американская модель развития).

Указанная модель развития была направлена на:

- снижение роли государства в экономическом развитии (выводы государства из регулировочных процессов);
- использование системы налоговых льгот и налоговых каникул для фирм, участвующих в данном проекте;
- всемерный рост процессов реальной (не монополистической) конкуренции.

В результате успешных реальных приватизационных процессов к оборонным программам получили доступ представители частного бизнеса и предпринимательства, что заставило их активно исследовать и применять информационные процессы в собственном бизнесе. А это была уже первая ступень к созданию фундамента серьезных революционных информационных преобразований.

Отсутствие нормативно-правовой базы по использованию информационных ресурсов и технологий для информационного обслуживания населения могло привести в США к информационному кризису, но этого не произошло, так как Конгрессом и Президентом были пересмотрены основные законодательные акты в данном контексте, тем самым законодательно закреплялось участие органов государственной власти в процессах информатизации страны. США в то время занимали лидирующие позиции среди всех мировых держав по всем критериям использования Интернет-пространства (скорость передачи данных, количество ИКТ, численность пользователей сети), поэтому именно в этой стране было создано реально действующее «Электронное правительство», что сразу же вывело на высокий уровень взаимоотношения государства с населением, тем самым повысив эффективность всей системы государственного управления.

Но использование «Электронного Правительства» не стало самоцелью, оно предоставило большое количество эффективных инструментов административного и государственного реформирования, к таковым на данный момент относятся следующие:

- федеральная инфраструктура публичных ключей (FPKI);
- системная авторизация доступа (ACES);
- общеправительственная система федеральных форм (Fed Forms);
- GILS - поиск информационных ресурсов по всем государственным структурам;
- система федеральных государственных закупок (FedBizOpps).

В европейских государствах проект «Технология формирования и развития информационного общества» был разработан как Пятая рамочная программа информационных изысканий.

Первый год осуществления проектных мероприятий был признан неудовлетво рительным. Европейская комиссия выступила с новым программным материалом, получившим наименование «Электронной Европы», цель которой заключалась в формировании объединенного межгосударственного общества информационного типа.

К ключевым задачам «Электронной Европы» были отнесены следующие:

- формирование инфраструктурного информационно-коммуникационного пространства;
- свободный вход в это пространство всех заинтересованных пользователей;
- нормативно-правовое обеспечение информационных проектов: «Мультимедийная коммуникация», «Электронная коммерция», «Защита сделки»;
- эффективное функционирование электронного правительства в различных его формах;
- повышение профессионализма, образованности и квалифицированности всех граждан;
- формирование и поддержание в рабочем состоянии глобальной сети Европейского Союза.

Ключевые цели программных материалов в западных странах состоят в том, чтобы занять лидирующие позиции в экономической, социальной и духовной сферах. Кыргызские законодатели прогнозируют экономический рост (в перспективе и экономическое лидерство) через устойчивое и эффективное государственное управление. В этом и заключается разность подходов: в западных странах в центре программ развития помещена личность с ее запросами, потребностями и интересами и цель – социально-экономическое развитие для повышения уровня материального благосостояния населения; а кыргызские программные продукты ориентированы на государственные интересы, и только опосредованно – на личностные потребности граждан.

При совпадении в приоритетных направлениях (право, кадры, инфраструктура) в Европе и в Кыргызстане, европейские концепции выстроены на формировании уважительного и доверительного отношения граждан к информационным технологиям в государственной жизни, к электронному правительству в самых различных форматах, к малому и среднему бизнесу; в то время как кыргызская концепция основывается на сильных государственных институтах, а не на человеческом потенциале. Так же отметим, что в европейских государствах электронная коммерция, электронные правительства интегрированы в единую онлайн-технологию, которая представляет собой основу выхода на цифровую экономику и информационное общество. Кыргызстан же пытается цифровизовать ключевые отрасли экономики и общественную жизнь.

Третий путь в развитии цифровой трансформации представляет собой **Сингапур**, поставивший задачу формирования Умного народа (Smart Nation). В Сингапуре органы цифрового управления подчиняются напрямую премьер-министру (главе государства) и подразделяются на Офис Умного Народа и Электронного Управления (координационный орган, включающий представителей министерства финансов, министерства коммуникаций и информации, администрации премьер-министра) и Агентства по технологиям управления (исполнительный орган, реализующий государственную политику в сфере цифровой трансформации). Прямая координация планов цифровой трансформации и их имплементации является наиболее эффективной формой управления цифровой трансформацией.

Особое внимание необходимо обратить на разграничение полномочий в сфере цифровой безопасности. В настоящее время основным органом в соответствии со статьей 15 Закона КР «Об органах национальной безопасности Кыргызской Республики» является Государственный комитет национальной безопасности Кыргызской Республики, однако полномочия не определены четко. Вместе с тем, необходимо понимать, что вопросы сохранности государственных секретов - это несомненная прерогатива органов национальной безопасности, но вопросы обеспечения информационной безопасности в части контрольных функций по цифровой информации в рамках цифровой экономики мог бы исполнять уполномоченный государственный орган в сфере цифрового управления, за которым должны быть закреплены необходимые административные полномочия и механизмы воздействия на обладателей информации, и который также мог бы выступать в защиту владельцев данных. Кроме этого создается угроза, когда участники рынка с частной формой собственности пытаются взаимодействовать с государственными участниками, возникают значительные

различия в уровнях безопасности информационных систем, что влечет за собой определенные административные проволочки, даже в тех случаях, когда уровни безопасности частного сектора превосходят уровни безопасности информационных систем государственного сектора. В связи со стремительным развитием общих угроз безопасности цифровой информации как внешних, так и внутренних, развитием мошеннических схем, а также ускоренным развитием мировых практик по обеспечению безопасности информационных систем, имеющиеся инструктивные нормативы должны постоянно пересматриваться для приведения их в соответствие с международными практиками обеспечения информационной безопасности. Также необходим гибкий механизм, позволяющий прямое действие таких стандартов и правил в национальном законодательстве без дополнительных мероприятий по их легализации. Отдельным этапом единообразного обеспечения безопасности должна стать площадка взаимодействия частного и государственного секторов по вопросам выработки единообразной практики обеспечения безопасности цифровых данных.

В данном контексте немаловажную роль будет играть и уполномоченный государственный орган в области персональных данных, который в том числе должен быть наделен функциями контроля безопасности информационных систем в части персональных данных, своего рода независимый арбитр, определяющий и устанавливающий внутренние правила для участников рынка, а также обладающий достаточными полномочиями и административными ресурсами.

В качестве применимого международного опыта в данной сфере можно сослаться на США, где административно-организационное обеспечение информационной безопасности направлено на координацию всех действий по защите информации и проведении единой государственной политики информационной безопасности, а также на опыт развитых стран Европы, которые также большое внимание уделяют всестороннему обеспечению в рамках национальной политики безопасности гражданского общества от информационных угроз, возникающих в современном глобальном информационном обществе.

Завершая рассмотрение общих вопросов регулирования цифрового управления в Кыргызской Республике, нельзя не отметить, что оно опирается на устаревшие в настоящий момент принципы, закрепленные в Законе КР «Об электронном управлении». По сути, электронное правительство является самой начальной стадией зрелости, и двигаться нужно к цифровому управлению, которое (как и цифровая экономика) характеризуется массовым использованием данных, когда решения принимаются на основе данных в интерактивном взаимодействии с потребителями (заказчиками) того или иного сервиса.

Цифровое управлении должен устанавливать следующие векторы/принципы/логику выстраивания управленческих процессов:

- ориентация на нужды и потребности граждан, выливающаяся в использование инструментов и методов процессных изменений, зависящих от жизненных ситуаций граждан;
- принятие управленческих решений на основе анализа актуальных и достоверных данных (Data Driven Government);
- формирование современной системы управления изменениями, обеспечивающей реализацию стратегических приоритетов, которые основаны на потребностях общества;
- создание современной системы управления кадрами, формирование профессиональных команд на государственной службе;
- формирование культуры поведения государственных служащих, отвечающей меняющимся задачам, которые поставлены перед системой государственного управления;
- прозрачная система госуправления, основанная на процессном подходе;
- сквозная межведомственная цифровизация;
- синхронизация государственных информационных систем в части функционала и интеграции данных на основе единых нормативных правил;
- оптимизация затрат на госаппарат через централизацию вспомогательных процессов.

Принципами цифрового управления должны стать:

- Цифровые услуги по умолчанию (не перевод офлайн услуг в цифровой формат, а «рождение» цифровых сервисов);
- Платформонезависимость и ориентация на мобильные устройства;
- Проектирование услуг, ориентированное на пользователя;
- Цифровые от начала до конца;
- Правительство как платформа;
- реализация стратегии, основанной на использовании данных;
- содействие использованию открытых данных;
- использование открытых стандартов и программного обеспечения с открытым исходным кодом;
- открытость для инноваций и «подрывных» технологий.

Страны, которые проходят через цифровую трансформацию и строят цифровую экономику, внедряют полностью «цифровое» и «умное» правительство, а не электронное. Ключевое различие между моделями электронного правительства и цифрового заключается в переходе от предоставления онлайновых гос.услуг к подходу, ориентированному на использование данных. Цифровые сервисы, ориентированные на пользователя, требуют горизонтальной интеграции и взаимодействия различных государственных органов. Инициативы по созданию цифрового правительства часто предполагают также изменения в организации системы управления.

Чтобы идти в одном фарватере цифрового развития со всеми странами, провозгласившими построение цифровой экономики парадигмой собственного развития, необходимо разрабатывать правовые основы цифрового управления – как управления основанного на данных. Простой «апгрейд» уже устаревших подходов «электронного» правительства не сработает, необходимы инновационные регуляторные меры и экосистемный подход.

Раздел 3. Объекты цифрового управления

Содержание

Правовой режим следующих объектов цифрового управления:
- электронные сообщения
- записи
- документы
- информресурсы
- информсистемы, в т.ч. распределённые (блокчейн)
- технологические системы (ЦОДы)
- телекоммуникационные сети
- приложения
- цифровые услуги (сервисы), в том числе государственные и муниципальные

Текущее регулирование (действующее законодательство):

1. Закон Кыргызской Республики «Об электронном управлении»
2. Закон Кыргызской Республики «Об электронной подписи»
3. Закон Кыргызской Республики «Об инновационной деятельности»
4. Закон Кыргызской Республики «О виртуальных активах»
5. Закон Кыргызской Республики «Об электронной торговле»
6. Закон Кыргызской Республики «Об электрической и почтовой связи»
7. Закон Кыргызской Республики «О доступе к информации, находящейся в ведении государственных органов и органов местного самоуправления Кыргызской Республики»
8. Закон Кыргызской Республики «О государственных закупках»
9. Закон Кыргызской Республики «Об информации персонального характера»
10. Закон Кыргызской Республики «О биометрической регистрации граждан Кыргызской Республики»
11. Закон Кыргызской Республики «Об органах национальной безопасности Кыргызской Республики»
12. Указ Президента Кыргызской Республики «О Национальной программе развития Кыргызской Республики до 2026 года» от 12 октября 2021 года УП №435
13. Указ Президента Кыргызской Республики «О дальнейших мерах цифровой трансформации Кыргызской Республики» от 21 июля 2021 года УП №305
14. Указ Президента Кыргызской Республики «О неотложных мерах по активизации внедрения цифровых технологий в государственное управление Кыргызской Республики» от 17 декабря 2020 года УП №64
15. Постановление Кабинета Министров Кыргызской Республики «Об утверждении Плана мероприятий Кабинета Министров Кыргызской Республики по реализации Национальной программы развития Кыргызской Республики до 2026 года» от 25 декабря 2021 года №352
16. Постановление Кабинета Министров Кыргызской Республики «О создании государственного учреждения «Проектный офис» от 16 августа 2021 года № 137
17. Постановление Правительства Кыргызской Республики «Об утверждении Правил пользования Государственным порталом электронных услуг» от 7 октября 2019 года № 525
18. Постановление Правительства Кыргызской Республики «Об утверждении Требований к защите информации, содержащейся в базах данных государственных информационных систем» от 21 ноября 2017 года №762
19. Постановление Правительства Кыргызской Республики «Об утверждении Положения о государственной системе электронных платежей» от 28 октября 2017 года № 709

20. Постановление Правительства Кыргызской Республики «Об утверждении Требований к взаимодействию информационных систем в системе межведомственного электронного взаимодействия "Түндүк"» от 11 апреля 2018 года № 200
21. Постановление Правительства Кыргызской Республики «О реализации пилотного проекта "Государство как платформа" по внедрению инновационных способов предоставления государственных и муниципальных услуг и сервисов» от 25 февраля 2020 года №113
22. Постановление Правительства Кыргызской Республики «О некоторых вопросах, связанных с использованием электронной подписи» от 31 декабря 2019 года № 742
23. Постановление Правительства Кыргызской Республики «Об утверждении Положения о государственной системе электронных сообщений и правилах ее использования» от 31 декабря 2019 года № 745
24. Постановление Правительства Кыргызской Республики «Об утверждении Положения об автоматизированной информационной системе «Государственная система электронного документооборота» от 30 октября 2020 года № 526
25. Постановление Правительства Кыргызской Республики «О Типовой инструкции по делопроизводству в Кыргызской Республике» от 3 марта 2020 года № 120
26. Постановление Правительства Кыргызской Республики «О некоторых вопросах, связанных с государственными информационными системами» от 31 декабря 2019 года № 744
27. Постановление Правительства Кыргызской Республики «Об утверждении Требований к государственным центрам обработки данных и соединяющим их каналам связи» от 31 декабря 2019 года № 747
28. Постановление Правительства Кыргызской Республики «Об отдельных вопросах осуществления электронного управления в Кыргызской Республике» от 31 декабря 2019 года № 748
29. Постановление Правительства Кыргызской Республики «О некоторых вопросах, связанных с государственной инфраструктурой электронного управления» от 5 декабря 2019 года № 661
30. Постановление Правительства Кыргызской Республики «Об отдельных вопросах, связанных с базовыми государственными информационными ресурсами» от 6 февраля 2020 года № 66
31. Распоряжение Кабинета Министров Кыргызской Республики от 2 июля 2021 года № 74-р
32. Распоряжение Кабинета Министров Кыргызской Республики от 12 января 2022 года №2-р
33. Концепция цифровой трансформации «Цифровой Кыргызстан 2019-2023»

Краткое описание выявленных недостатков и ориентиров из мировой практики

№	Описание недостатка	Тип[7]	Лучшая практика
3.1	Существующее законодательство не создает условий для цифрового управления, то есть управления, основанного на данных. Данные из государственных информационных систем не используются для принятия решений и аналитики как в	**Н**	В Докладе Всемирного банка «Данные для лучшей жизни» (2021) отмечается, что по мере увеличения объема совместно и повторно используемых данных (особенно персональных) потенциальные выгоды, извлекаемые населением в

[7] В таблице приводятся следующие типы недостатков регулирования:
(П) пробел в регулировании (регулирование требуется, но его нет)
(У) устаревшая норма (норма есть, но её нужно менять)
(Н) неработающая норма (норма есть, но в силу описанных причин она не работает)
(Б) действующая норма является необоснованным препятствием для осуществления деятельности

	государственном, так и в частном секторе. Каждое ведомство работает со своим набором данных, не согласованных с другими ведомствами, — применяются разные методики формирования данных, разное понимание состава данных, эти данные принципиально друг с другом не выверены. Большая часть ГИС документоориентирована: как правило, в системах хранятся документы в формате Word, либо отсканированные подписанные вручную документы pdf, а не данные, к которым эти документы привязаны, — с такими данными работать практически невозможно.		виде повышения качества государственной политики и оказания услуг, могут быстро увеличиваться, но наряду с этим будут также расти риски злоупотребления данными. Эти потенциальные выгоды зависят такого фактора, как распространение или обмен данными между сторонами. Однако для того, чтобы стороны добровольно участвовали в этом процессе, они должны доверять системам, правилам и институтам, определяющим безопасность такого обмена. Как люди могут быть уверены в том, что их данные будут защищены и что они получат свою долю ценности, которые могут создать данные? Рост подобных опасений говорит о необходимости нового общественного договора относительно данных, т.е. соглашения между всеми участниками процесса создания, совместного и повторного использования данных, способствующего укреплению уверенности в том, что они не пострадают и получат справедливую долю ценности, которую эти данные создадут
3.2	Закрепленная в статье 18 Закона КР «Об электронном управлении» многоуровневая модель регулирования отношений в зависимости от их объекта (инфраструктура, приложения, данные, сервисы) распространяется только на государственный сектор и, кроме того, не отражена в других законодательных актах КР, в том числе принятых позднее. При этом многоуровневый характер отношений в рамках цифровой экономики является данностью, которую нельзя не учитывать при регулировании отношений в данной области	**Н**	Данная проблема является специфической для законодательства КР и вызвана тем, что иные законодательные акты не были приведены в соответствие с Законом КР «Об электронном управлении»
3.3	В законодательстве КР отсутствует правовой режим распределенных информационных систем	**У**	Существующее правовое регулирование создания и эксплуатации информационных систем можно считать, в целом, сложившимся. Информационная система является базовым понятием,

			используемым в различных отраслях права, при этом объем этого понятия не вызывает споров. В то же время, понятие и классификация видов информационных систем требуют дальнейшего развития для того, чтобы отразить развитие отношений в данной области, прежде всего, появление т.н. распределенных реестров, а также активное создание информационных систем в ходе государственно-частного партнерства
3.4	В законодательстве КР отсутствуют условия для необходимого в условиях цифровой экономике перехода от электронного документооборота к управлению, основанному на записях в информационных системах. Также в законодательстве не созданы условия для использования записей в информационных системах в юридически значимых целях	**П**	Следует выделять, во-первых, информацию в форме сведений, данных, регулирование которой связано с содержанием информации. Далее, квалифицированной формой информации следует признавать запись, то есть информацию, хранимую и передаваемую в электронной или иной форме, которая пригодна для хранения, обработки и передачи, в том числе в информационных системах, посредством сетей электросвязи, сети Интернет. Введение понятия «запись» в базовый закон в сфере информации необходимо для того, чтобы оно могло применяться к различным по своей природе правоотношениям, в том числе гражданско-правовым, в которых фигурируют новые информационные технологии. Здесь необходимо опираться также и на опыт зарубежных стран, прежде всего, США, в сфере перевода информации в отдельных сферах в формат электронных записей (а не документов), например, в сфере здравоохранения. Это позволило резко повысить доступность и связность накапливаемой информации за счет снижения требований к её реквизитам. Выделение записей связано с необходимостью регулирования процессов обработки (хранения, передачи) конкретных единиц информации, в том числе установления порядка ограничения доступа к информации, распространение которой запрещено,

			принятием мер по обеспечению надлежащей охраны информации. Новое понятие – «запись» является наиболее пригодным для использования в цифровой среде. Кроме того, введение понятия «запись» позволит изменить подход к определению понятия «документ», что необходимо для того, чтобы, во-первых, сохранить преемственность регулирования с правилами оборота документов на бумажном носителе, и, во-вторых, создать условия для оборота электронных документов наряду с документами на бумажном носителе без утраты юридической силы теми или другими видами документов.
3.5	Отсутствуют нормы, допускающие возможность исключительно цифрового взаимодействия, что не позволяет переходить в цифровое взаимодействие полноценно, так как государственные органы требуют бумажные документы. Отсутствует стандартизация в сфере электронного документооборота или оборота цифровых записей. Не урегулированы вопросы электронного документооборота с негосударственными организациями и физическими лицами, которые могли бы направлять в государственные органы электронные письма и получать ответы, целые отрасли отрезаны от электронного документооборота и не могут полноценно участвовать во взаимообмене перепиской в электронном виде Имеющиеся нормы направлены только на регулирование электронного документооборота в государственном секторе, при этом не имеется нормативов, которые бы закрепляли возможность взаимодействия частных информационных систем по делопроизводству с государственными.	**П**	Стандартизация в области СЭД может очень серьезно помочь в налаживании межведомственного и межкорпоративного взаимодействия, особенно если на соответствии закупаемого программного обеспечения такого рода стандартам будут настаивать государственные органы. Функциональные требования к электронным системам управления документами (в нашей терминологии - к системам электронного документооборота) разрабатываются в основном в интересах государственных органов. Подобные требования служат ориентиром (а иногда и обязательным требованием) при закупках, что позволяет выдержать единую техническую политику в государственном секторе и создать необходимые условия для межведомственного взаимодействия. Проще говоря, использование такого рода требований - это возможность для государства решить ряд серьезных проблем за счет поставщиков СЭД, сэкономив тем самым немалые средства. За рубежом требования к системам электронного документооборота начали появляться в начале 1990-х гг. Сейчас стандарты такого рода существуют в США, Англии, Германии, Австрии, Норвегии,

			Голландии, Австралии, ряде других стран. В 2007 - 2008 гг. стали появляться требования к СЭД третьего поколения, начиная с 3-й редакции известного американского стандарта DoD 5015.2. Наиболее заметным событием стал выход в свет в феврале 2008 г. европейских требований MoReq2, разработанных по заказу Еврокомиссии (правительства Евросоюза). Сейчас на основе MoReq2 в Словении и Чехии разработаны собственные национальные стандарты, а в Украине подобный стандарт разрабатывается в ходе проекта MOREQ-UA. Зарубежный опыт показывает, что использование ЭЦП окупается при оперативной работе с ответственными электронными документами. Использование ЭЦП для менее значимых документов (включая внутреннюю переписку, которая ведется в рамках защищенной корпоративной СЭД) считается неоправданным. Применение ЭЦП при работе с документами постоянного и длительного (свыше 7–10 лет) срока хранения в настоящее время не рекомендуется, поскольку технологии обеспечения длительной проверяемости ЭЦП еще не отработаны. Опыт также показывает, что для автоматизации массовых рассылок извещений и других подобных документов необходимо, по мере возможности, отказаться от использования подлинных подписей и печатей на таких документах. В этом плане интересен опыт Евросоюза, где соответствующие европейские директивы запрещают национальным правительствам требовать наличие личных подписей на электронных счетах и счетах-фактурах. Аутентичности и целостности документов способствует соблюдение норм соответствующих стандартов и правил «хорошей деловой практики». В настоящее время можно найти зарубежные стандарты практически

			по всем аспектам управления электронными документами. Сегодня известны два основных метода организации хранения электронных документов (которые могут использоваться и в комбинации). Первый метод предусматривает хранение документов на съемных носителях, предпочтительно, на носителях однократной записи типа WORM (CD, DVD и т.п.). При использовании второго метода документы онлайн хранятся в системах электронного документооборота или электронных архивах (ЭА). В этом случае защита целостности и аутентичности обеспечивается средствами СЭД/ЭА. За рубежом накоплен большой опыт использования государственного регулирования в целях обеспечения качества и совместимости программного обеспечения и аппаратных средств, закупаемых государственными органами как для внутреннего использования, так и для решения задач в рамках программы создания «электронного правительства». Особо следует отметить стандарты функциональных требований к СЭД (в США это DoD 5015.2, в Европе – MoReq2).
3.6	Закон КР “Об электронном управлении” предусматривает, что создание, развитие и эксплуатация государственной инфраструктуры электронного управления осуществляются с учетом требований, предусмотренных Законом Кыргызской Республики "О государственных закупках", который создает трудности при закупке информационных систем, в результате чего поставщики могут внедрять не вполне соответствующее требованиям информационные системы. Порядок разработки и ввода в эксплуатацию негосударственных информационных систем в законодательстве вообще не предусмотрен.	**Б**	Проблема соотношения законодательства об информации с законодательством о государственных закупках, в целом, решена в Российской Федерации, где государственные и муниципальные информационные системы создаются и вводятся в эксплуатацию на основании соответствующего порядка (подзаконного акта, утвержденного правительством), и, кроме того, существует механизм координации создания госинформсистем на базе профильного министерства

Комментарии

В целях построения информационного общества, а также консолидации усилий государственных органов, бизнеса и гражданского сообщества, направленных на ускорение цифровой трансформации и социально-экономического развития страны важнейшей задачей госорганов и органов МСУ принята концепция цифровой трансформации «Цифровой Кыргызстан 2019-2023». В рамках реализации дорожной карты указанной Концепции государственными органами власти проводятся различные мероприятия и реализуются проекты, направленные на построение цифровой инфраструктуры, повышения человеческого потенциала, реинжиниринга процессов государственного взаимодействия и управления.

Основным пробелом действующего законодательства Кыргызской Республики применительно к объектам цифрового управления является то, что оно не создает собственно условий для цифрового управления, то есть управления, основанного на данных. Данные сейчас лежат мертвым грузом в госинформсистемах, не используются для принятия решений и аналитики как в государственном, так и в частном секторе. Каждое ведомство работает со своим набором данных, не согласованных с другими ведомствами, — применяются разные методики формирования данных, разное понимание состава данных, эти данные принципиально друг с другом не выверены. Большая часть ГИС документоориентирована: как правило, в системах хранятся документы в формате Word, либо отсканированные подписанные вручную документы pdf, а не данные, к которым эти документы привязаны, — с такими данными работать практически невозможно.

В Докладе Всемирного банка «Данные для лучшей жизни» (2021) отмечается, что по мере увеличения объема совместно и повторно используемых данных (особенно персональных) потенциальные выгоды, извлекаемые населением в виде повышения качества государственной политики и оказания услуг, могут быстро увеличиваться, но наряду с этим будут также расти риски злоупотребления данными. Эти потенциальные выгоды зависят такого фактора, как распространение или обмен данными между сторонами. Однако для того, чтобы стороны добровольно участвовали в этом процессе, они должны доверять системам, правилам и институтам, определяющим безопасность такого обмена.

Как люди могут быть уверены в том, что их данные будут защищены и что они получат свою долю ценности, которые могут создать данные? Рост подобных опасений говорит о необходимости нового общественного договора относительно данных, т.е. соглашения между всеми участниками процесса создания, совместного и повторного использования данных, способствующего укреплению уверенности в том, что они не пострадают и получат справедливую долю ценности, которую эти данные создадут. Инструментами формирования, содействия реализации и контроля за соблюдением общественных договоров можно считать правовые системы и государственное управление в целом. Убедить стороны придерживаться правил общественного договора непросто, и решение этой задачи зависит от того, будет ли обеспечено справедливое распределение выгод, связанных с использованием данных – иными словами, каждый должен что-то выиграть. В этом процессе страны с более низким уровнем доходов слишком часто оказываются в невыгодном положении, поскольку у них, как это нередко бывает, нет инфраструктуры и квалифицированных специалистов, необходимых для получения данных и их преобразования в ценность, институциональных и регуляторных систем, необходимых для формирования доверия к системам сбора и обработки данных, а также масштабов деятельности и организационных структур, обеспечивающих справедливое участие в работе глобальных рынков данных и управлении ими. Продуманная система управления данными позволяет странам в полном объеме извлекать социальную и экономическую ценность данных публичного и частного назначения и использовать эффект взаимодействия между ними. Это требует укрепления доверия к надежности системы сбора, обработки и хранения данных наряду с обеспечением справедливого распределения выгод.

Поддержанию доверия к операциям с данными могут способствовать надежные нормативно-правовые основы, предусматривающие как защитные механизмы, так и инструменты реализации. Защитные механизмы повышают доверие к операциям с данными, поскольку они предотвращают или ограничивают ущерб, который наносит злоупотребление

данными. Важнейшей предпосылкой доверия к системам сбора, обработки и хранения данных является информационная безопасность. Для достижения надлежащего уровня информационной безопасности необходимо формирование правовых основ, обязывающих держателей и обработчиков данных внедрять системы технической защиты данных. На сегодняшний день надлежащие правовые основы информационной безопасности созданы лишь в незначительном меньшинстве стран с низким и средним уровнем доходов. На их фоне выделяется Кения, чей новый Закон о защите данных является хорошим примером всеобъемлющих правовых норм в области информационной безопасности.

Создание надлежащих правовых основ защиты данных также имеет огромное значение. Эти основы должны четко разграничивать персональные данные (данные, позволяющие идентифицировать личность) и неперсональные данные (данные, не содержащие информации, позволяющей идентифицировать личность). Среди стран со средним уровнем доходов относительно хорошо развитыми механизмами защиты персональных данных выделяется Маврикий. Фактически это была первая страна Субсахарской Африки, которая ратифицировала “Конвенцию 108+” (Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных). Инструменты реализации облегчают доступ к данным и их повторное использование внутри и между различными группами заинтересованных сторон, чтобы обеспечить извлечение социально-экономической ценности данных в полном объеме. Между данными публичного и частного назначения существуют заметные различия в характере и сфере действия положений, регулирующих совместное использование данных. Во всем мире проведена большая работа для того, чтобы обеспечить безопасное раскрытие данных публичного назначения за счет проведения политики открытых данных (она стимулирует заблаговременную публикацию государственных данных) и принятия законов, регулирующих доступ к информации (они дают гражданам юридически закрепленное право требовать раскрытия информации). Однако для того, чтобы политика открытых данных оказала реальное воздействие, она должна опираться на единый протокол определения степени конфиденциальности данных в сочетании с функционально совместимыми техническими стандартами, машиночитаемыми форматами и открытыми лицензиями, облегчающими последующее повторное использование данных. Всё это в настоящий момент отсутствует в законодательстве Кыргызской Республики.

Цифровое взаимодействие, то есть взаимодействие в цифровой форме с использованием электронных документов и записей предусматривает собой возможность упрощения процедуры официального взаимодействия между государственными органами, органами местного самоуправления, их структурными подразделениями и должностными лицами, а также упрощение процесса учета входящей и исходящей корреспонденции и контроля исполнительской дисциплины.

Электронный документооборот в настоящее время основывается на Автоматизированной информационной системе “Государственная система электронного документооборота”, которая создана в соответствии с постановлением Правительства Кыргызской Республики “Об утверждении Положения об автоматизированной информационной системе "Государственная система электронного документооборота" от 30 октября 2020 года № 526.

Законом Кыргызской Республики “Об электронном управлении” предусматривается наличие электронных документов во взаимодействии участников электронного управления, что закреплено в 1 статье Закона, а также получает легализацию непосредственно в статьях вышеназванного Закона. Статья 16 этого же Закона устанавливает случаи и порядок обмена электронными документами.

Помимо прочего, электронные документы должны обладать соответствующими реквизитами, которые обеспечиваются посредством подписания документа электронной подписью в соответствии с Законом Кыргызской Республики “Об электронной подписи”. Согласно указанному Закону, информация в электронной форме, подписанная квалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью,

за исключением случаев, когда законами или иными нормативными правовыми актами установлен запрет составления такого документа в электронной форме. Также установлена недопустимость признания подписанного электронной подписью электронного документа не имеющими юридической силы только на том основании, что подпись в электронном документе не является собственноручной.

Активизация процесса внедрения электронного документооборота была заложена в Концепции цифровой трансформации “Цифровой Кыргызстан 2019-2023”, а необходимость внедрения электронного документооборота получила отражение в Дорожной карте по реализации Концепции цифровой трансформации «Цифровой Кыргызстан 2019-2023», утвержденной распоряжением Правительства Кыргызской Республики от 15 февраля 2019 года № 20-р.

Мероприятия “Дорожной карты” по внедрению электронного документооборота должны были быть завершены в декабре 2020 года, а в декабре 2021 года система электронного документооборота должна была быть внедрена в органах судебной системы.

При этом, активное внедрение системы началось только в контексте мероприятий по противодействию распространению COVID-19 на территории Кыргызской Республики при массовом переводе государственных органов на удаленный режим работы, а также объявлением в городе Бишкек и Ош режима чрезвычайного положения.

Между тем, внедрение и распространение электронного документооборота в контексте COVID-19, не нашла особой поддержки, как на уровне государственных органов, так и на управленческом уровне, в государственных органах все равно приоритетом являлся бумажный документооборот.

Вследствие общественно политических потрясений октября 2020 года и последовавших изменений в структуре органов исполнительной власти, а также оптимизации государственных предприятий, процесс внедрения электронного документооборота остановился. Однако, до активной фазы перехода к электронному документообороту была проведена работа по обновлению документации в области документооборота. Так, была разработана и утверждена постановлением Правительства Кыргызской Республики от 3 марта 2020 года № 120 новая Типовая инструкция по делопроизводству в Кыргызской Республике.

Вместе с тем, несмотря на проводимые мероприятия, государственные органы, выйдя на оффлайновый режим работы, вновь стали возвращаться к бумажному документообороту из-за его привычности, а также низкой степени прослеживаемости и контроля со стороны ответственных лиц. Такая ситуация потребовала исправления на нормативном уровне: Указом Президента Кыргызской Республики “О неотложных мерах по активизации внедрения цифровых технологий в государственное управление Кыргызской Республики” от 17 декабря 2020 года УП № 64 была закреплена необходимость повсеместного внедрения электронного документооборота в государственных органах.

Основной проблемой внедрения электронного документооборота и отказа от бумажного остается высокая степень бумажной забюрократизированности государственных органов, низкий уровень понимания государственными органами пользы для них от внедрения электронного документооборота.

Таким образом, внедрение электронного документооборота застопорилось из-за “человеческого фактора”, в том числе привычности бумажного документооборота. Приведение правового регулирования информационных отношений в систему требует дифференциации регулирования в зависимости от формы и способов обработки информации. Информация как предмет деятельности участников информационных правоотношений выступает в самых различных формах.

Следует выделять, во-первых, информацию в форме сведений, данных, регулирование которой связано с содержанием информации. Далее, квалифицированной формой информации следует признавать запись, то есть информацию, хранимую и передаваемую в электронной или иной форме, которая пригодна для хранения, обработки и передачи, в том числе в информационных системах, посредством сетей электросвязи, сети Интернет.

Введение понятия «запись» в базовый закон в сфере информации необходимо для того, чтобы оно могло применяться к различным по своей природе правоотношениям, в том числе гражданско-правовым, в которых фигурируют новые информационные технологии. Здесь необходимо опираться также и на опыт зарубежных стран, прежде всего, США, в сфере перевода информации в отдельных сферах в формат электронных записей (а не документов), например, в сфере здравоохранения. Это позволило резко повысить доступность и связность накапливаемой информации за счет снижения требований к её реквизитам. Выделение записей связано с необходимостью регулирования процессов обработки (хранения, передачи) конкретных единиц информации, в том числе установления порядка ограничения доступа к информации, распространение которой запрещено, принятием мер по обеспечению надлежащей охраны информации. Новое понятие – «запись» является наиболее пригодным для использования в цифровой среде.

Кроме того, введение понятия «запись» позволит изменить подход к определению понятия «документ», что необходимо для того, чтобы, во-первых, сохранить преемственность регулирования с правилами оборота документов на бумажном носителе, и, во-вторых, создать условия для оборота электронных документов наряду с документами на бумажном носителе без утраты юридической силы теми или другими видами документов.

Документ - запись, содержащая реквизиты, позволяющие ее идентифицировать. Регулирование документов должно быть связано с определением требований к реквизитам документа и иным обстоятельствам, определяющих его юридическое значение, а также с процессами обработки, в том числе хранения, документов. Документ как квалифицированная запись может иметь в тех или иных правоотношениях юридическое значение, в том числе выражать содержание сделок, иных волевых или властных актов.

Одной из основных проблем перевода в настоящее время становится законодательство в сфере архива, где предусматривается хранение документов, которые подходят хранению бумажных документов. Отсутствует порядок хранения электронных документов и электронной информации.

Существующее правовое регулирование создания и эксплуатации информационных систем можно считать, в целом, сложившимся. Информационная система является базовым понятием, используемым в различных отраслях права, при этом объем этого понятия не вызывает споров. В то же время, понятие и классификация видов информационных систем требуют дальнейшего развития для того, чтобы отразить развитие отношений в данной области, прежде всего, появление т.н. распределенных реестров, а также активное создание информационных систем в ходе государственно-частного партнерства.

В законодательстве должен быть определен правовой режим такой разновидности информационной системы как распределенная информационная система и ее оператора. Эти изменения являются необходимыми для регулирования отношений, связанных с оборотом цифровых прав, возникших в связи с принятием закона КР «О виртуальных активах».

Предлагается определить, что оператором распределенной информационной системы (информационной системы, в которой создание, обработка, в том числе хранение, содержащейся в ней информации осуществляются с использованием или посредством технических средств, принадлежащих пользователям такой системы) является лицо, самостоятельно или совместно с другими лицами определяющее порядок обработки содержащейся в ней информации с использованием технических средств пользователей такой информационной системы. Также в целях отражения существа распределенных информационных систем необходимо определить понятие оператора узла распределенной информационной системы как участника информационной системы, не являющегося оператором информационной системы в целом, но обеспечивающего тождественность информации в данной информационной системе посредством заданных в ней алгоритмов.

Необходимо выделить в законодательстве, помимо государственных информационных систем, также совместные (государственно-частные, муниципально-частные) информационные системы, создаваемые и эксплуатируемые на основании соглашений между государственными или муниципальными органами и частными лицами. Такие системы

позволят осуществлять публичные функции на основании инфраструктуры, совместно используемой с частными организациями, что снижает затраты на развитие информационной инфраструктуры.

В целях упорядочения отношений по использованию информационных систем необходимо закрепить презумпцию достоверности сведений, содержащихся в государственных информационных системах и обязанность операторов систем обеспечивать такую достоверность. Специальными актами могут устанавливаться процедуры устранения несоответствии между сведениями, содержащимися в разных государственных информационных системах.

В Законе “Об электронном управлении” оговаривается, что включение информационных систем, центров обработки данных, иных элементов в состав государственной инфраструктуры электронного управления осуществляется:

1) в отношении элементов, введенных в эксплуатацию до вступления в силу настоящего Закона - на основании акта Правительства Кыргызской Республики;

2) в отношении элементов, вводимых в эксплуатацию в соответствии с настоящим Законом - на основании акта Правительства Кыргызской Республики.

Данный метод включения в состав государственной инфраструктуры электронного управления является неэфективным и забюрокртизированным. Каждое включение в данный состав проходит множество этапов согласования с государственными органами.

Необходимо утвердить требования для включения в состав государственной инфраструктуры электронного управления, которые будут предусмотрены в Реестре инфраструктуры электронного управления, где после соответствия определенным параметрам будет включен в состав государственной инфраструктуры электронного управления.

Также закон предусматривает, что создание, развитие и эксплуатация государственной инфраструктуры электронного управления осуществляются с учетом требований, предусмотренных Законом Кыргызской Республики "О государственных закупках", который создает определенные трудности при закупке информационных систем, в результате чего поставщики могут внедрять не вполне соответствующее требованиям информационные системы.

В итоге государственные органы сталкиваются с большими проблемами:

в случае, если разработчик - иностранный поставщик, который может не знать структуру электронного управления и может создавать информационную систему, которую невозможно модернизировать;

разработчик создает системы на платных лицензиях, оплату к последующем которых госорган не может осуществить в связи с бюджетом;

разработчик не передает исходные коды государственному органу, так как это не было предусмотрено в договоре;

технические задания составлены неправильно, так как госорган не понимает техническую часть. В итоге создается система, которая сложная для использования и сопровождения.

В связи с этим для исключения таких проблем необходимо предусмотреть, что для создания и эксплуатации государственных информационных систем заключаются договоры с прямым заключением соглашений с государственными предприятиями, которые имеют опыт по разработке информационных систем. Также необходимо заметить, что проблема соотношения законодательства об информации с законодательством о государственных закупках, в целом, решена в Российской Федерации, где государственные и муниципальные информационные системы создаются и вводятся в эксплуатацию на основании соответствующего порядка (подзаконного акта, утвержденного правительством), и, кроме того, существует механизм координации создания госинформсистем на базе профильного министерства.

Раздел 4. Субъекты цифрового управления

Содержание

Субъекты цифрового управления
- операторы технологических систем
- операторы информсистем
- операторы телекоммуникационных сетей
- провайдеры услуг (сервисов)
- цифровые платформы и экосистемы
- аутсорсеры (обработчики)
- владельцы информационных ресурсов
- принципалы данных (лица, к которым относятся данные – субъекты персональных данных, источники промышленных данных и т.п.)
- пользователи данных и сервисов (профессиональные пользователи и конечные пользователи)

Текущее регулирование (действующее законодательство):

1. Закон Кыргызской Республики «Об электронном управлении»
2. Закон Кыргызской Республики «Об электронной подписи»
3. Закон Кыргызской Республики «Об инновационной деятельности»
4. Закон Кыргызской Республики «О виртуальных активах»
5. Закон Кыргызской Республики «Об электронной торговле»
6. Закон Кыргызской Республики «Об электрической и почтовой связи»
7. Закон Кыргызской Республики «О доступе к информации, находящейся в ведении государственных органов и органов местного самоуправления Кыргызской Республики»
8. Закон Кыргызской Республики «О государственных закупках»
9. Закон Кыргызской Республики «Об информации персонального характера»
10. Закон Кыргызской Республики «О биометрической регистрации граждан Кыргызской Республики»
11. Закон Кыргызской Республики «Об органах национальной безопасности Кыргызской Республики»
12. Указ Президента Кыргызской Республики «О Национальной программе развития Кыргызской Республики до 2026 года» от 12 октября 2021 года УП №435
13. Указ Президента Кыргызской Республики «О дальнейших мерах цифровой трансформации Кыргызской Республики» от 21 июля 2021 года УП №305
14. Указ Президента Кыргызской Республики «О неотложных мерах по активизации внедрения цифровых технологий в государственное управление Кыргызской Республики» от 17 декабря 2020 года УП №64
15. Постановление Кабинета Министров Кыргызской Республики «Об утверждении Плана мероприятий Кабинета Министров Кыргызской Республики по реализации Национальной программы развития Кыргызской Республики до 2026 года» от 25 декабря 2021 года №352
16. Постановление Кабинета Министров Кыргызской Республики «О создании государственного учреждения «Проектный офис» от 16 августа 2021 года № 137
17. Постановление Правительства Кыргызской Республики «Об утверждении Правил пользования Государственным порталом электронных услуг» от 7 октября 2019 года № 525
18. Постановление Правительства Кыргызской Республики «Об утверждении Требований к защите информации, содержащейся в базах данных государственных информационных систем» от 21 ноября 2017 года №762

19. Постановление Правительства Кыргызской Республики «Об утверждении Положения о государственной системе электронных платежей» от 28 октября 2017 года № 709
20. Постановление Правительства Кыргызской Республики «Об утверждении Требований к взаимодействию информационных систем в системе межведомственного электронного взаимодействия "Түндүк"» от 11 апреля 2018 года № 200
21. Постановление Правительства Кыргызской Республики «О реализации пилотного проекта "Государство как платформа" по внедрению инновационных способов предоставления государственных и муниципальных услуг и сервисов» от 25 февраля 2020 года №113
22. Постановление Правительства Кыргызской Республики «О некоторых вопросах, связанных с использованием электронной подписи» от 31 декабря 2019 года № 742
23. Постановление Правительства Кыргызской Республики «Об утверждении Положения о государственной системе электронных сообщений и правилах ее использования» от 31 декабря 2019 года № 745
24. Постановление Правительства Кыргызской Республики «Об утверждении Положения об автоматизированной информационной системе «Государственная система электронного документооборота» от 30 октября 2020 года № 526
25. Постановление Правительства Кыргызской Республики «О Типовой инструкции по делопроизводству в Кыргызской Республике» от 3 марта 2020 года № 120
26. Постановление Правительства Кыргызской Республики «О некоторых вопросах, связанных с государственными информационными системами» от 31 декабря 2019 года № 744
27. Постановление Правительства Кыргызской Республики «Об утверждении Требований к государственным центрам обработки данных и соединяющим их каналам связи» от 31 декабря 2019 года № 747
28. Постановление Правительства Кыргызской Республики «Об отдельных вопросах осуществления электронного управления в Кыргызской Республике» от 31 декабря 2019 года № 748
29. Постановление Правительства Кыргызской Республики «О некоторых вопросах, связанных с государственной инфраструктурой электронного управления» от 5 декабря 2019 года № 661
30. Постановление Правительства Кыргызской Республики «Об отдельных вопросах, связанных с базовыми государственными информационными ресурсами» от 6 февраля 2020 года № 66
31. Распоряжение Кабинета Министров Кыргызской Республики от 2 июля 2021 года № 74-р
32. Распоряжение Кабинета Министров Кыргызской Республики от 12 января 2022 года №2-р
33. Концепция цифровой трансформации «Цифровой Кыргызстан 2019-2023»

Краткое описание выявленных недостатков и ориентиров из мировой практики

№	Описание недостатка	Тип[8]	Лучшая практика
4.1	В действующем законодательстве КР отсутствует система основных акторов (субъектов) цифрового	**П**	Данный пробел вызван несистемным развитием законодательства КР в сфере цифровой экономики, в

[8] В таблице приводятся следующие типы недостатков регулирования:
(П) пробел в регулировании (регулирование требуется, но его нет)
(У) устаревшая норма (норма есть, но её нужно менять)
(Н) неработающая норма (норма есть, но в силу описанных причин она не работает)
(Б) действующая норма является необоснованным препятствием для осуществления деятельности

	управления, что не позволяет выстроить систему отношений в цифровой среде именно как систему. При этом регулирование статуса каждого из этих субъектов должно осуществляться в рамках регулирования соответствующего вида деятельности в цифровой экономике		частности, принятием Закона КР «Об электронной торговле» без учета уже действующего Закона КР «Об электронном управлении». Предотвращение подобных коллизий в дальнейшем требует разработки системы законодательства в сфере цифрового управления.
4.2	В области цифровой экономики появляющиеся новые субъекты, такие как владельцы цифровых платформ или экосистем, остаются невидимыми для отраслевого и антимонопольного законодательства, которое не в состоянии сдерживать концентрацию в их руках значительной рыночной власти и, как следствие, не могут устранять неравенство в экономической сфере. Эффективное цифровое управление требует, прежде всего, регулирования таких новых субъектов на межотраслевой базе	**П**	В настоящее время система регулирования деятельности субъектов цифровой экономики разрабатывается в рамках стратегии Цифрового единого рынка ЕС и должна быть воплощена в двух базовых актах ЕС – о цифровом рынке и цифровых услугах. Эти акты предполагают комплексное регулирование деятельности цифровых платформ в ЕС

Комментарии

Законодательство КР нуждается в серьезной модернизации в части регулирования деятельности принципиально новых субъектов – так называемых «чемпионов цифровой экономики» или цифровых платформ. Чтобы идти в одном фарватере цифрового развития со всеми странами, провозгласившими построение цифровой экономики парадигмой собственного развития, необходимо разрабатывать правовые основы цифрового управления – как управления основанного на данных. Простой «апгрейд» уже устаревших подходов «электронного» правительства не сработает, необходимы инновационные регуляторные меры и экосистемный подход. Здесь стоит обратить внимание, прежде всего, на опыт Европы. В течение многих лет регулирование цифровых рынков было ключевым приоритетом в Европе. В 2015 году Европейская комиссия обязала ЕС создать единый цифровой рынок, и это обязательство породило ряд разнообразных инициатив и нормативных изменений, затрагивающих поставщиков и пользователей цифровых товаров и услуг. Даже между государствами — членами ЕС стандарты цифрового регулирования различались — и продолжают различаться - и многие вопросы остаются на усмотрение местных органов власти. А в 2016 году Великобритания проголосовала за выход из ЕС – процесс, который приведет к дальнейшему расхождению в цифровом регулировании по всей Европе.

В результате продолжающейся эволюции европейского цифрового регулирования процесс цифрового соответствия стал гораздо более приоритетным для любой организации, предоставляющей или потребляющей цифровые товары и услуги в Европе. По мере развития цифровых технологий организациям становится все сложнее обеспечивать постоянное соблюдение нормативных требований. В декабре 2020 года Европейская комиссия опубликовала два основных предлагаемых законопроекта, направленных на реализацию цифровой стратегии ЕС. Вместе Закон о цифровых услугах (DSA) и Закон о цифровых рынках (DMA) призваны создать более безопасное цифровое пространство и создать равные условия для стимулирования инноваций и роста как в ЕС, так и во всем мире.

DSA, как одна половина этого законодательного пакета, сосредоточена на регулировании поставщиков цифровых услуг, или “посредников”. Он направлен на решение проблемы доминирования “очень крупных” платформ (охватывающих более 10% из 450 миллионов потребителей в Европе) и ответственности компаний за контент третьих лиц. Нарушения DSA могут повлечь за собой единовременные штрафы в размере до 6% от годового глобального оборота или периодические выплаты штрафов в размере не более 5% от среднесуточного оборота. Важно отметить, что DSA будет применяться к любому поставщику, предлагающему свои услуги пользователям в ЕС. Посредники, регулируемые DSA, будут иметь различные обязательства в зависимости от их роли, размера и влияния на онлайн-экосистему. Цифровые платформы будут нести ответственность за удаление незаконного контента, выполнение обязательств по прозрачности и проведение дополнительной проверки. DSA стремится дополнить и развить Директиву ЕС об электронной торговле, одновременно гармонизируя регулирование по всему ЕС и проясняя такие вопросы, как ответственность за контент третьих лиц.

После вступления в силу Закон о DSA и цифровых рынках вступит в силу непосредственно на всей территории ЕС и, следовательно, не потребует национального применения каждым государством-членом.

Вторая половина законодательного дуэта ЕС, описанного выше, - это Закон о цифровых рынках (DMA). DMA будет нацелена на “привратников” — основные платформы, которые действуют как шлюз между бизнес-пользователями и клиентами. Предлагаемые правила выражают обеспокоенность по поводу “укоренившихся и прочных” позиций таких платформ, которые, по мнению ЕС, приводят к недобросовестной практике и отсутствию конкуренции, что приводит к более высоким ценам, более низкому качеству и меньшему количеству инноваций в цифровой экономике.

Поставщик базовой платформы будет считаться «привратником», если он:

оказывает значительное влияние на внутренний рынок ЕС (в настоящее время годовой оборот ЕЭЗ превышает 6,5 млрд евро в течение трех лет или справедливая рыночная стоимость предприятия или его материнской компании составляет 65 млрд евро);

управляет одним или несколькими важными шлюзами для клиентов (в настоящее время насчитывается более 45 миллионов конечных пользователей в ЕС и более 10 000 активных бизнес-пользователей в год); и

пользуется или, как ожидается, будет занимать прочное и прочное положение в своей деятельности.

В то время как проект DMA устанавливает эти пороговые значения для предположения, что поставщик является привратником, он также позволяет Европейской комиссии назначать статус привратника на основе других оценок.

Привратники будут, среди прочего:

должны соблюдать новые правила обмена данными;

должны разрешить удаление своего собственного программного обеспечения и приложений с аппаратного обеспечения и разрешить бизнес-пользователям заключать контракты с конечными пользователями за пределами платформы gatekeeper.;

им будет запрещено продвигать свои собственные продукты по сравнению с другими бизнес-пользователями.

DMA происходит в то время, когда несколько государств-членов ЕС обсуждают или уже приняли новые нормативные акты, также направленные на регулирование гейткиперов или “крупных цифровых компаний” в более общем плане с целью обеспечения того, чтобы соответствующие рынки оставались открытыми и конкурентоспособными (например, немецкое регулирование UPSCAM, вступившее в силу в январе 2021 года). Учитывая, что DMA претендует на то, чтобы быть единственным инструментом, обеспечивающим такое регулирование во всем ЕС, еще предстоит выяснить, как в конечном итоге сложатся его отношения с этими национальными режимами.

После Brexit Великобритания не будет принимать DSA или DMA. Но Великобритания также стремится изменить способ регулирования цифровых рынков, что, по всей вероятности,

означает попытку достичь той же цели, что и ЕС, с точки зрения регулирования “крупных технологических” компаний.

Ряд ключевых регулирующих органов Великобритании (Управление по конкуренции и рынку (CMA), Управление Комиссара по информации, Управление по финансовому надзору и Ofcom) объединили усилия для консультирования по стратегии Великобритании по регулированию цифровых рынков. Вместе они составляют Британскую целевую группу по цифровым технологиям, которая опубликовала свой первый рекомендательный документ.

Режим регулирования, предложенный Digital Task Force, предусматривает юридически обязательный кодекс поведения (с различными правилами для разных типов компаний), меры по защите конкуренции (включая такие средства защиты, как мобильность и совместимость персональных данных) и расширенные правила слияний, и все это будет контролироваться новым подразделением по цифровым рынкам (DMU), заседающий в CMA. Правительство Великобритании учредило DMU в апреле 2021 года и обязалось провести консультации по стимулирующему конкуренцию режиму позднее в 2021 году с целью иметь возможность регулировать крупных глобальных поставщиков цифровых технологий к 2022 году.

Режим Цифровой целевой группы нацелен на цифровые компании со “стратегическим статусом рынка” (SMS), который будет определен на основе оценки, основанной на фактических данных. Это отражает стратегию ЕС (как описано выше), направленную против тех компаний, которые, как считается, обладают укоренившейся рыночной властью. Но, в отличие от подхода ЕС, Целевая группа Великобритании по цифровым технологиям предлагает, чтобы такая оценка SMS применялась к конкретной деятельности компании, а не к компании в целом.

В то время как Целевая группа по цифровым технологиям предусматривает активный режим и открытые и продуктивные отношения с компаниями, занимающимися SMS, она идет дальше, чем ЕС, в своих предлагаемых санкциях. Целевая группа рекомендует Соединенному Королевству пресекать нарушения режима штрафами в размере до 10% от мирового оборота, что рассматривается как эффективная мера воздействия, однако до момента её применения судить об эффективности пока не представляется возможным.

Раздел 5. Основания возникновения, изменения, прекращения правоотношений в цифровой среде

Содержание

- источники информации;
- смарт-контракты;
- результаты цифровых услуг

Текущее регулирование (действующее законодательство):

1. Закон Кыргызской Республики «Об электронном управлении»
2. Закон Кыргызской Республики «Об электронной подписи»
3. Закон Кыргызской Республики «Об инновационной деятельности»
4. Закон Кыргызской Республики «О виртуальных активах»
5. Закон Кыргызской Республики «Об электронной торговле»
6. Закон Кыргызской Республики «Об электрической и почтовой связи»
7. Закон Кыргызской Республики «О доступе к информации, находящейся в ведении государственных органов и органов местного самоуправления Кыргызской Республики»
8. Закон Кыргызской Республики «О государственных закупках»
9. Закон Кыргызской Республики «Об информации персонального характера»
10. Закон Кыргызской Республики «О биометрической регистрации граждан Кыргызской Республики»
11. Закон Кыргызской Республики «Об органах национальной безопасности Кыргызской Республики»
12. Указ Президента Кыргызской Республики «О Национальной программе развития Кыргызской Республики до 2026 года» от 12 октября 2021 года УП №435
13. Указ Президента Кыргызской Республики «О дальнейших мерах цифровой трансформации Кыргызской Республики» от 21 июля 2021 года УП №305
14. Указ Президента Кыргызской Республики «О неотложных мерах по активизации внедрения цифровых технологий в государственное управление Кыргызской Республики» от 17 декабря 2020 года УП №64
15. Постановление Кабинета Министров Кыргызской Республики «Об утверждении Плана мероприятий Кабинета Министров Кыргызской Республики по реализации Национальной программы развития Кыргызской Республики до 2026 года» от 25 декабря 2021 года №352
16. Постановление Кабинета Министров Кыргызской Республики «О создании государственного учреждения «Проектный офис» от 16 августа 2021 года № 137
17. Постановление Правительства Кыргызской Республики «Об утверждении Правил пользования Государственным порталом электронных услуг» от 7 октября 2019 года № 525
18. Постановление Правительства Кыргызской Республики «Об утверждении Требований к защите информации, содержащейся в базах данных государственных информационных систем» от 21 ноября 2017 года №762
19. Постановление Правительства Кыргызской Республики «Об утверждении Положения о государственной системе электронных платежей» от 28 октября 2017 года № 709
20. Постановление Правительства Кыргызской Республики «Об утверждении Требований к взаимодействию информационных систем в системе межведомственного электронного взаимодействия "Түндүк"» от 11 апреля 2018 года № 200
21. Постановление Правительства Кыргызской Республики «О реализации пилотного проекта "Государство как платформа" по внедрению инновационных способов

предоставления государственных и муниципальных услуг и сервисов» от 25 февраля 2020 года №113

22. Постановление Правительства Кыргызской Республики «О некоторых вопросах, связанных с использованием электронной подписи» от 31 декабря 2019 года № 742
23. Постановление Правительства Кыргызской Республики «Об утверждении Положения о государственной системе электронных сообщений и правилах ее использования» от 31 декабря 2019 года № 745
24. Постановление Правительства Кыргызской Республики «Об утверждении Положения об автоматизированной информационной системе «Государственная система электронного документооборота» от 30 октября 2020 года № 526
25. Постановление Правительства Кыргызской Республики «О Типовой инструкции по делопроизводству в Кыргызской Республике» от 3 марта 2020 года № 120
26. Постановление Правительства Кыргызской Республики «О некоторых вопросах, связанных с государственными информационными системами» от 31 декабря 2019 года № 744
27. Постановление Правительства Кыргызской Республики «Об утверждении Требований к государственным центрам обработки данных и соединяющим их каналам связи» от 31 декабря 2019 года № 747
28. Постановление Правительства Кыргызской Республики «Об отдельных вопросах осуществления электронного управления в Кыргызской Республике» от 31 декабря 2019 года № 748
29. Постановление Правительства Кыргызской Республики «О некоторых вопросах, связанных с государственной инфраструктурой электронного управления» от 5 декабря 2019 года № 661
30. Постановление Правительства Кыргызской Республики «Об отдельных вопросах, связанных с базовыми государственными информационными ресурсами» от 6 февраля 2020 года № 66
31. Распоряжение Кабинета Министров Кыргызской Республики от 2 июля 2021 года № 74-р
32. Распоряжение Кабинета Министров Кыргызской Республики от 12 января 2022 года №2-р
33. Концепция цифровой трансформации «Цифровой Кыргызстан 2019-2023»

Краткое описание выявленных недостатков и ориентиров из мировой практики

№	Описание недостатка	Тип[9]	Лучшая практика
5.1	Законодательство КР нуждается в унификации разных источников информации, выступающих в виде «старых» (СМИ) и «новых» (соцсети, каналы в мессенджерах и т.п.) медиа, что требует пересмотра деятельности различных медиа на базе общих принципов свободы слова, законности и справедливости распространения информации	**П**	Регулирование источников информации в мире основывается на уважении свободы слова и необходимости ограничения ответственности информационных посредников, как это сделано, например, в Акте о пристойности коммуникаций США. Данный механизм может быть дополнен уведомлением как средством опровержения иммунитета информационного посредника, когда посредник, получивший

[9] В таблице приводятся следующие типы недостатков регулирования:
(П) пробел в регулировании (регулирование требуется, но его нет)
(У) устаревшая норма (норма есть, но её нужно менять)
(Н) неработающая норма (норма есть, но в силу описанных причин она не работает)
(Б) действующая норма является необоснованным препятствием для осуществления деятельности

			уведомление, не может ссылаться на то, что он не знал о незаконном характере распространяемой информации (либо её недостоверности или неактуальности)
5.2	Понятия «смарт-контракт» в Законах КР “О виртуальных активах” и «Об электронной торговле» противоречат друг другу и ограничивают его применение ввиду того, что соответствующие изменения не закреплены в гражданском законодательстве, а правовой режим смарт-контракта регулируется как обычные программы для ЭВМ. Необходимо закрепление смарт-контрактов в качестве основания для возникновения, изменения, прекращения прав и обязанностей в цифровой сфере для придания его использованию более детализированной правовой основы	**Н**	Современные правовые системы Франции, Германии, Швейцарии, Бельгии, Великобритании, не содержат норм, содержащих определение смарт-контракта, однако технологии блокчейн и смарт контракты используются исходя из традиционного гражданского права, основываясь на общем договорном праве, при этом Италия реализовала законодательное закрепление понятия смарт-контракт и применяет нормы гражданского права непосредственно к регулированию правоотношений возникающих из смарт-контрактов.
5.3	В законодательстве КР отсутствует правовой режим доверенных услуг (таких как гарантированная доставка или отметка времени), что препятствует развитию отношений в цифровой экономике	**П**	Наиболее актуальной на настоящий момент лучшей практикой в мире является Типовой закон ЮНСИТРАЛ об использовании и трансграничном признании управления идентификационными данными и удостоверительных услуг (УУ). Закон устанавливает общее правило о юридическом признании УУ, а также закрепляет обязанности основных участников отношений (поставщиков УУ, абонентов и пользователей) и ответственность поставщиков УУ. Закон определяет требования к УУ, выполнение которых необходимо для обеспечения их надёжности, а также содержит положения, относящиеся к отдельным видам УУ: электронным подписям, электронным печатям, электронным архивам, услугам гарантированной доставки сообщений, услугам аутентификации веб-сайтов

Комментарии

Главным основанием возникновения, изменения, прекращения правоотношений в цифровой среде является получение информации (в результате её распространения или доступа к ней). В Законе КР «Об электронном управлении» в настоящий момент уже установлено, что информация является общедоступной, если доступ к ней не ограничен в

соответствии с законом или решением обладателя информации. Также законом закреплено, что запрещаются распространение и публикация информации, направленной на пропаганду войны, разжигание национальной, межрегиональной, расовой или религиозной ненависти и вражды, а также иной информации, за которые предусмотрена ответственность в соответствии с Уголовным кодексом Кыргызской Республики, Кодексом Кыргызской Республики о проступках и Кодексом Кыргызской Республики о нарушениях. Прежде всего, речь идет об информации, распространение которой нарушает, прежде всего, частные интересы конкретных субъектов, в связи с чем преследуется государством при наличии волеизъявления обладателей информации и иных лиц, которые считают свои права нарушенными в связи с распространением информации.

К данной информации относятся:

- информация, содержащая нецензурную брань;
- персональные данные;
- информация о частной жизни гражданина, полученная с нарушением гражданского законодательства;
- информация, порочащая честь, достоинство и деловую репутацию граждан, деловую репутацию организаций;
- недостоверные данные, требования к достоверности которых установлены законом (недостоверная реклама, недостоверная информация о товаре и др.).

Одной из существенных проблем современного информационного общества является распространение недостоверных новостей («fake news»). Распространение таких новостей может проводить к значительным проблемам на финансовых рынках, приводить к политическим и социальным потрясениям. Борьба с предоставлением недостоверной информацией (дезинформацией) требует реализации иных подходов к регулированию, чем регулирование оборота информации, ограниченной в распространении, так как в данном случае требуется комплексная оценка и проверка фактов на предмет достоверности или недостоверности информации с учетом того, что в данном случае идет речь о тех случаях, когда распространение недостоверной информации прямо не запрещено законом и не нарушает прямо прав и свобод конкретных субъектов (в противном случае недостоверная информация становится информацией, ограниченной в распространении).

В качестве инструментов борьбы с распространением недостоверной информации могут применяться как традиционные механизмы (рассмотрение заявлений и удаление (блокирование) недостоверной информации), так и иные механизмы, например, создание информационного ресурса (сайта, приложения) для проверки фактов и опровержений, проведение программ повышения медиаграмотности, использование новых технологий (искусственный интеллект) для выявления недостоверной информации, изменение алгоритма формирования новостной ленты и т.д.

Значительная часть норм, регулирующих инфокоммуникационные отношения, адресована именно источникам информации. В их роли могут выступать сайты в интернете, средства массовой информации, любые другие организованные и предназначенные для использования массивы информации. В целях упорядочения данных отношений целесообразно использование базового, корневого понятия, коим и должно выступить понятие информационного ресурса как источника информации.

Разновидностями информационных ресурсов должны признаваться средства массовой информации и/или их отдельные выпуски (в том числе газеты, телеканалы и прочие «традиционные» СМИ). Выделение информационного ресурса как самостоятельного объекта регулирования информационного права позволит сблизить правовое регулирование распространения информации в традиционных СМИ и в новых медиа, унифицировать подходы к определению прав и обязанностей владельцев таких ресурсов. Кроме того, важнейшей задачей информационного права должно стать разграничение сферы ответственности владельца информационного ресурса и лица, выступившего инициатором распространения информации. Решение данной задачи требует дальнейшего совершенствования и детализации правового статуса информационного посредника, а также

разработки концепции ответственности владельца информационного ресурса за распространяемую информацию.

Зарубежная практика в этой сфере сложилась еще в конце 20 века и зарекомендовала свою эффективность. В знаковом кейсе, Cubby, Inc. v. CompuServe, суд встал на сторону «доски объявлений» и указал, что, хотя лицо, опубликовавшее клеветнический материал, в принципе несет ту же ответственность, что и лицо, изначально опубликовавшее данный материал, новостные агентства, книжные магазины и библиотеки не могут быть привлечены к ответственности, если они не знали о клеветническом характере данного материала. Кроме того, суд счел, что это «уходит корнями в Первую поправку» – распространитель не может быть привлечен к ответственности, если не знал содержимого публикации. Суд пришел к выводу, что CompuServe имеет не больше возможностей контроля за содержимым материалов, доступных через фирму, чем библиотека, книжный магазин или газетный киоск, и отказал в удовлетворении иска. Следовательно, несмотря на противоправный характер распространяемой информации, CompuServe действовала в рамках своего субъективного права, предоставляя доступ к информации третьих лиц, содержание которой она не контролировала. Во втором деле – Stratton Oakmont v. Prodigy – суд пришел к совершенно противоположному выводу. Истец указал, что Условия оказания услуг Prodigy включают в себя положение об удалении оскорбительных сообщений, следовательно, фирме должно быть известно о них. Кроме того, Prodigy использует автоматическое программное обеспечение, сканирующее все доски объявлений на предмет выявления оскорбительных слов и их удаления, если таковые будут найдены. Суд счел эти факты отличающими дело от Cubby v. CompuServe.

Странным следствием решения по этому делу явилось то, что провайдер, который добросовестно предпринял попытку удалять противоправный контент со своих серверов и тем самым осуществлял определенные меры саморегулирования, подвергается большей ответственности, чем провайдер, самоустранившийся от борьбы с противоправным контентом на своих серверах. Многие провайдеры в связи с этим стали бояться риска непредвиденной ответственности.

Впрочем, нельзя не отметить определенной логики в данном решении суда: если в деле CompuServe способы поведения распространителя информации не отличались в зависимости от ее содержания, то в деле Stratton Oakmont прослеживалось принятие на себя распространителем информации обязанности по контролю контента – за ненадлежащее выполнение данной обязанности к Stratton Oakmont, и были применены меры ответственности.

Американский законодатель обратил внимание на неопределенность, созданную решением по делу Stratton Oakmont, и пришел к выводу, что эта неопределенность выступает препятствием дальнейшему развитию Интернета. Следствием этого явилось включение статьи 230 в Акт о пристойности коммуникаций. В то время как § 223 (a) и § 223(d) Акта, которые устанавливали наказания за передачу непристойного или явно оскорбительного материала, усилили ответственность за собственный контент в Интернете, статья 230 пошла в противоположном направлении и ограничила ответственность за контент третьих лиц.

Центральным положением статьи 230 является статья 230(c)(1):

«Провайдер или пользователь интерактивных компьютерных сервисов не может расцениваться в качестве издателя или выразителя мнения в отношении информации контент-провайдера – третьего лица».

В дополнение к этому статья 230(c)(2) содержит ответ по делу Stratton Oakmont:

«Провайдер интерактивных компьютерных сервисов не может быть привлечен к ответственности на том основании, что он добровольно и добросовестно предпринимал меры по ограничению доступа к материалам, которые он расценивал как вульгарные, непристойные, низменные, нездоровые, чрезмерно насильственные, домогающиеся или иным образом сомнительные».

То есть американский законодатель был вынужден специально ограничить ответственность информационных посредников (к которой их уже начали привлекать суды),

поскольку счел, что это будет иметь охлаждающий эффект как для развития технологий, так и для свободы слова.

Однако с принятием Акта о пристойности коммуникаций стало очевидно, что произошел перекос: нужна была правовая конструкция, которая все-таки позволяла бы заставить информационных посредников удалить противоправный контент, даже если они его не размещали и даже в ситуации, когда они не могли быть за него привлечены к ответственности. Недостающий элемент восполнил Digital Millenium Copyright Act – американский Закон об авторском праве в цифровую эпоху. Воспроизведя нормы Акта о пристойности коммуникаций про освобождение от ответственности, данный закон предусмотрел возможность направить посреднику уведомление о том, что у него на сервере лежит что-то противозаконное. И если посредник в ответ на уведомление не удалял или не блокировал противоправный контент, он мог быть привлечен к ответственности.

Таким образом, кыргызское законодательство, закрепляя механизмы ответственности информационных посредников, будет находиться в общемировом тренде. Посредники действительно влияют на распространение информации, но в то же время они не могут контролировать всю информацию, которая через них проходит. И если накладывать на них чрезмерные обременения, это приведет только к ухудшению качества информационных сервисов, а отнюдь не к повышению контроля за информацией.

По мере развития технологий существенное значение для возникновения, изменения, прекращения правоотношений в цифровой среде приобретают смарт-контракты. Хотя данное понятие уже содержится в новом законодательстве КР, два закона, установивших его (об электронной торговле и о виртуальных активах) противоречат друг другу, что свидетельствует о непонимании сути данного явления. Между тем, термин «смарт-контракт» был впервые введен Н. Сабо в 1994 году, который определил данное явление как компьютерный протокол транзакций, самостоятельно выполняющий условия договора, который разработан с целью соблюдения договорных условий сторонами, минимизации потерь от мошенничества, арбитражных и судебных издержек, сокращении числа лиц, вовлеченных в процесс заключения и исполнения договоров. Однако несмотря на то, что концепция подобной автоматизации договорных отношений появилась еще в конце прошлого столетия, за отправную точку ее фактической реализации и популяризации следует принять запуск проекта Ethereum в 2015 году – платформы, основанной на технологии блокчейна, которая была специально предназначена для размещения и исполнения смарт-контрактов.

Прежде всего, отметим, что существует два подхода к определению понятия «смарт-контракт»: технический и юридический. Так, с точки зрения технологии функционирования, смарт-контракт является компьютерным кодом, предназначенным для выполнения определенных задач при соблюдении заранее установленных условий. В большинстве случаев этот код имплементирован в блокчейн – тип распределенного реестра, представляющий собой децентрализованную базу данных, распределенную между несколькими узлами сети, серверами, пользователями и т.п., в связи с чем блокчейн можно представить в виде единой цепочки блоков информации о подтвержденных транзакциях в отношении определенного цифрового актива , которые последовательно организованы «посредством использования криптографических идентификаторов (хэшей), создаваемых по результатам выполнения сложной математической операции по вычислению, именуемой майнингом, и последующего подтверждения данного результата большинством участников системы (нодов)» . Блоки внутри блокчейна синхронизированы между собой посредством механизма консенсуса; это означает, что ключевым принципом его работы является частичное дублирование информации из каждого блока в последующий, в связи с чем новый блок в цепи невозможно сформировать в противоречие с предыдущим. Так, записанная информация содержится в неизменном виде, а каждая копия обновляется новой информацией автоматически. С описанным принципом функционирования блокчейна связано одно из преимуществ смарт-контракта, по сравнению с традиционным договором – они минимизируют риск несогласованного вмешательства в свое содержание, что гарантирует имущественным интересам сторон большую защиту.

Стоит отметить, что на сегодняшний момент блокчейн является наиболее популярной технологией для выполнения смарт-контрактов, в связи с чем некоторыми исследователями (напр., Ефимова Л.Г. и Сиземова О.Б., Савельев А. И.) выполнение кода в блокчейне указывается в качестве одного из смыслообразующих признаков смарт-контрактов. Сказанное верно в большинстве случаев, однако, с учетом впечатляющих темпов развития научно-технического прогресса, в будущем мыслимо создание альтернативной технологии автоматизированного выполнения договорных условий, записанных в форме программного кода, также обеспечивающей невозможность нарушения обязательства, в связи с чем концепция определения смарт-контракта через блокчейн или иную технологию распределенного реестра потеряет свою актуальность. Так, более адаптивной представляется точка зрения Вашкевича А. М., указывающего, что реализация смарт-контрактов возможна и без распределенного реестра.

Содержание смарт-контракта представляет собой совокупность условий, изложенных на специальном языке программирования в виде кода, который впоследствии «автономно исполняется на множестве компьютеров – узлов блокчейна – неподконтрольных сторонам договора», и не требует участия контрагента после его заключения. Использование смарт-контрактов мыслимо в разнообразных сферах человеческой деятельности (финансовой, риэлтерской, административной, охрана интеллектуальной собственности и проч.), однако посредством них возможно распоряжение только цифровыми активами, т.к. «передача (предоставление) предмета сделки обеспечивается в блокчейне посредством его привязки к конкретному блоку информации в этой системе». Следовательно, если стороны вступают во взаимодействие по поводу распоряжения материальными активами, «необходимо, чтобы актив, являющийся предметом договора, был привязан к виртуальной единице, которой оперирует компьютерная программа». Как справедливо отмечает В. Бутерин, «без криптовалют потенциал умных контрактов не может быть реализован», в связи с чем отметим, что вопрос видимости смарт-контрактов российским правопорядком напрямую зависит от определения правового статуса криптовалюты и, в случае полного запрета на ее использование субъектами гражданского оборота, дальнейшие рассуждения о правовой квалификации данного явления теряют актуальность.

Резюмируя, смарт-контракт с технической точки зрения является «фрагментом программного кода, предназначенным для осуществления определенных задач в случае выполнения заранее установленного в программе условия». Техническая сторона смарт-контракта в контексте блокчейна отражена в его определениях как разновидности кодировки, способа функционирования блокчейна; как фрагменте кода, который реализован на платформе блокчейн и инициируется блокчейн-транзакциями, а также организует внесение записей в базу данных. В этом смысле, смарт-контракт может быть органично встроен в правовую систему как программа для ЭВМ, ведь смарт-контракт тоже является объективизированной совокупностью данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата. Однако при таком положении, вопрос определения смарт-контракта ограничивается рамками технологических принципов его функционирования, в то время как волеизъявление сторон, направленное на возникновение между ними соответствующего правоотношения, понятием смарт-контракта уже не охватывается. Вместе с тем, анализ смарт-контрактов не исчерпывается их рассмотрением в качестве технического явления: объем понятия смарт-контракта в той или иной степени охватывает процесс взаимодействия контрагентов, поскольку оно, в силу своей специфики, не может быть реализовано вне смарт-контракта. В связи с этим, необходимо закрепление смарт-контрактов в качестве основания для возникновения, изменения, прекращения прав и обязанностей в цифровой сфере для придания его использованию более детализированной правовой основы.

Нельзя не отметить, что в законодательстве КР отсутствует правовой режим доверенных (удостоверительных) услуг (таких как гарантированная доставка или отметка времени), что препятствует развитию отношений в цифровой экономике. Наиболее актуальной на настоящий момент лучшей практикой в мире является Типовой закон

ЮНСИТРАЛ об использовании и трансграничном признании управления идентификационными данными и удостоверительных услуг (УУ). Проект Типового закона является итогом работы ЮНСИТРАЛ по созданию правовых условий для развития электронной торговли, продолжающейся уже более четверти века. Положения Типового закона развивают подходы, заложенные в Типовом законе об электронной торговле (ТЗЭТ) и Типовом законе об электронных подписях (ТЗЭП). Целью ТЗЭТ и ТЗЭП было придание юридической силы электронным документам. Они были нацелены на то, чтобы устранить юридические барьеры для использования электронных соглашений, отменить «монополию бумажных документов».

Так, согласно п. 1 ст. 6 ТЗЭТ, когда законодательство требует, чтобы информация была представлена в письменной форме, это требование считается выполненным путём представления сообщения данных, если содержащаяся в нём информация является доступной для её последующего использования. П. 1 ст. 7 ТЗЭТ устанавливает, что, если законодательство требует наличия подписи лица, это требование считается выполненным в отношении сообщения данных, если:

а) использован какой-либо способ для идентификации этого лица и указания на то, что это лицо согласно с информацией, содержащейся в сообщении данных;

б) этот способ является надёжным и соответствующим цели, для которой сообщение данных было подготовлено или передано, с учётом всех обстоятельств, включая любые соответствующие договорённости.

Данные положения не устанавливали критериев оценки соответствия способа перечисленным в них требованиям, и гарантии юридической значимости информации в электронном виде (действительность оферты, акцепта, электронных доказательств) не могли применяться. Поэтому в дальнейшем был разработан специальный ТЗЭП, который уточнил ряд существенных вопросов.

ТЗЭП после его принятия стал эталоном для законодательства об электронных подписях различных стран, в частности, его подходы использованы в российском Федеральном законе №63-ФЗ от 06.04.2011 «Об электронной подписи» и в Законе КР «Об электронной подписи». Основу подхода ТЗЭП составляет наделение особым статусом информационного посредника (посредников) – пользующегося доверием лица, которое могло бы технически удостоверить по требованию одной или обеих сторон, что подпись действительно была совершена лицом, указанным в качестве лица, подписавшего документ.

Подход ТЗЭП развит и усилен в проекте нового Типового закона, описывающего не просто статус информационных посредников, но и в целом инфраструктуру УУ (сервиса доверенной третьей стороны) и УИД как необходимого элемента обеспечения доверия в цифровой экономике. Работа в рамках ЮНСИТРАЛ соответствует актуальной практике работы регуляторов в Европейском союзе: Директиве 1999/93/ЕС об электронных подписях и Директиве 2000/31/ЕС об электронной коммерции. Директива об электронных подписях по содержанию во многом напоминает ТЗЭП, однако структура их различна. Если в ТЗЭП основное внимание обращается на проблемы действительности подписи и права и обязанности сторон, то Директива стремилась, прежде всего, создать организационный аппарат по работе с электронными подписями, установить рамки для работы этого аппарата.

В 2014 году структура регулирования электронных подписей в Европейском союзе была изменена, и вместо директив был принят Регламент, охватывающий, помимо электронных подписей, иные сервисы идентификации и доверенные сервисы. Регламент, в свою очередь, является одним из элементов стратегии цифрового единого рынка Европейского союза. Регламент ставит своей целью свободное обращение на внутреннем рынке продуктов и УУ, соответствующим требованиям регламента: не должно быть никаких ограничений для предоставления УУ на территории одного государства — члена Европейского союза поставщиком УУ, учреждённым в другом государстве-члене.

Глава 3 нового Типового закона полностью посвящена удостоверительным услугам. Данная глава устанавливает общее правило о юридическом признании УУ, а также закрепляет обязанности основных участников отношений (поставщиков УУ, абонентов и пользователей)

и ответственность поставщиков УУ. Глава определяет требования к УУ, выполнение которых необходимо для обеспечения их надёжности, а также содержит положения, относящиеся к отдельным видам УУ: электронным подписям, электронным печатям, электронным архивам, услугам гарантированной доставки сообщений, услугам аутентификации веб-сайтов.

Общие подходы, заложенные в тексте проекта Типового закона, позволяют охарактеризовать его как пример так называемого «мягкого права», то есть документов, которые сами по себе не имеют нормативного характера, но в силу проработанности закреплённых в них подходов и авторитета разработавшего их экспертного сообщества становятся основой для обязательных правил различного уровня (от международных договоров до национального законодательства). С этой точки зрения Типовой закон имеет большое значение для Кыргызстана и стран Евразийского экономического союза, поскольку задаёт высокий стандарт регулирования вопросов идентификации и аутентификации, которые сейчас активно прорабатываются в кыргызском законодательстве и документах Евразийского экономического союза.

Раздел 6. Информационные правоотношения

Содержание

- виды информации
- распространение, предоставление информации
- доступ к информации
- открытые данные
- защита информации и кибербезопасность (полномочия по принятию требований к защите информации в отдельных сферах отношений).

Текущее регулирование (действующее законодательство):

1. Закон Кыргызской Республики «Об электронном управлении»
2. Закон Кыргызской Республики «О доступе к информации, находящейся в ведении государственных органов и органов местного самоуправления Кыргызской Республики»
3. Закон Кыргызской Республики «О защите государственных секретов Кыргызской Республики»
4. Закон Кыргызской Республики «Об информации персонального характера»
5. Закон Кыргызской Республики «О коммерческой тайне»
6. Постановление Правительства Кыргызской Республики «Об утверждении Требований к защите информации, содержащейся в базах данных государственных информационных систем» от 21 ноября 2017 года № 762
7. Постановление Правительства Кыргызской Республики «Об утверждении Требований к обеспечению безопасности и защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных» от 21 ноября 2017 года № 760

Краткое описание выявленных недостатков и ориентиров из мировой практики

№	Описание недостатка	Тип[10]	Лучшая практика
6.1	В законодательстве КР, прежде всего, в статье 12 Закона КР «Об электронном управлении» общедоступная информация рассматривается как правовой режим информации, противостоящий конфиденциальной информации. Такой подход является устаревшим, поскольку не создает условий для закрепления баланса между интересом общества в использовании информации (в частности, выраженном в свободе слова) и правами обладателей информации на ограничение доступа к ней, если им соответствующее полномочие предоставлено законом	**У**	В зарубежных странах общедоступность информации является не столько элементом правового режима самой информации, сколько следствием реализации базового права человека на доступ к информации, предусмотренного статьей 19 Всеобщей декларации прав человека и статьей 19 Пакта Международного пакта о гражданских и политических правах (Нью-Йорк, 16 декабря 1966 г.). Например, в США, по общему правилу, вся информация, находящаяся в открытом доступе, в том числе сведения персонального характера, может быть использована без ограничений, за исключением

[10] В таблице приводятся следующие типы недостатков регулирования:
(П) пробел в регулировании (регулирование требуется, но его нет)
(У) устаревшая норма (норма есть, но её нужно менять)
(Н) неработающая норма (норма есть, но в силу описанных причин она не работает)
(Б) действующая норма является необоснованным препятствием для осуществления деятельности

			случаев, указанных в законе (принцип «разрешено по умолчанию, если иное не установлено законом»). Это основано на Первой поправке к Конституции США о защите свободы слова. Открытый характер сети Интернет подчеркнут в решениях Верховного суда США. Такой подход, с одной стороны, способствует максимально широкому использованию информации в обществе, с другой, не создает условий для нарушения прав обладателей информации, которые могут ограничить доступ к информации, если им на то предоставлено право законом
6.2	В законодательстве Кыргызстана (в иных законодательных актах, кроме закона об электронном управлении) режим доступа к информации плохо структурирован и не систематизирован, что приводит к значительным наложениям и нестыковкам между режимами разных тайн, значительно затрудняющим использование соответствующей информации, в том числе такое использование, которое не может нарушать права лиц, к которым относится та или иная тайна. В целях унификации правовых режимов охраняемых законом тайн в действующем законодательстве необходимо, в соответствии с положениями Конституции, ограничить их применение только к следующим видам данных: данным, составляющим государственную тайну; данным, составляющим коммерческую тайну; данным, представляющим собою профессиональную или процессуальную тайну; данным о частной жизни гражданина.	**Б**	В США и Европе сложилась система тайн, выстроенных как по отраслевому (банковская тайна, тайна связи) признаку, так и по предметному (коммерческая тайна, тайна частной жизни), при этом государственные секреты (государственная тайна) выделены в отдельный институт. Данные правовые режимы имеют значительную историю своего развития и направлены на защиту важнейших интересов тех лиц, к которым они относятся. Основанием для установления режима тайны во всех случаях является то, что разглашение информации, составляющей ту или иную тайну, способно причинить вред тому лицу, к которому относится тайна («принципалу тайны»).
6.3	Фактически не работает норма статьи 9 Закона «Об электронном управлении» о том, что уполномоченный орган в сфере электронного управления	**П**	Великобритания: Подходы к правовому регулированию унификации форматов представления информации и технологий

	осуществляет (в том числе) функции по: «содействию государственным органам и органам местного самоуправления при переходе к электронному управлению, в том числе при разработке и согласовании ими регламентов, стандартов, процедур оказания электронных государственных и муниципальных услуг, создании инструментов открытого и подотчетного управления, механизмов использования моделей открытых данных на основе современных информационных технологий, разработке методик оценки эффективности реализации инициатив в области открытости и подотчетности, создании порталов открытых данных».		информационного обмена в государственных информационных системах регулируют Принципы открытых стандартов (Open Standards Principles 2018), содержащие следующие критерии выбора стандартов, которые должны: – соответствовать потребностям пользователя, – обеспечивать равный доступ поставщиков к гос. контрактам, – быть гибкими и способными к изменениям, – быть обоснованными, – быть транспарентными. Принципы гарантируют, что будущие технологии будут доступными, безопасными и инновационными. Они описывают, как правительство будет определять и выбирать открытые стандарты и как эти стандарты могут быть внедрены в программное обеспечение с открытым исходным кодом и проприетарное программное обеспечение. Все государственные ведомства и агентства должны использовать эти принципы. Открытые стандарты должны отвечать потребностям пользователей: Пользователи могут быть государственными пользователями или гражданами. Основные цели открытых стандартов — позволить пользователям: ● обмениваться данными с помощью программного обеспечения по своему выбору ● улучшить четкость и согласованность данных ● улучшить взаимодействие между отделами ● улучшить взаимодействие между правительством и гражданами. Процесс выбора, который правительство использует для определения межправительственных открытых стандартов для ИТ, начинается с определения потребностей пользователей. Открытые стандарты должны предоставить поставщикам равный доступ к государственным

			контрактам: Европейское законодательство о закупках (статья 42 Директивы 2014/24/ЕС) требует, чтобы технические спецификации предоставляли поставщикам равный доступ к государственным контрактам и не создавали препятствий для открытия государственных закупок для конкуренции. Открытые стандарты должны поддерживать гибкость и изменения: Государственные ведомства должны обмениваться соответствующими данными друг с другом, чтобы предоставлять эффективные услуги гражданам. Используя открытые форматы, подразделения могут: ● стандартизировать данные, что уменьшит вероятность хранения дублирующийся данных. ● интегрировать свои ИТ-системы для улучшения коммуникации и эффективности для пользователей (гибкая ИТ поможет сделать существующие и новые системы совместимыми) ● легко переносить данные и информацию между старой и новой системами ● сделать данные и интерфейсы прикладного программирования (API) доступными — это позволяет другим создавать альтернативные, инновационные представления государственных данных и получать доступ к государственным услугам.
6.4	Размещение информации из информационных систем государственных органов и органов местного самоуправления на сайтах государственных органов и органов местного самоуправления в Интернете в формате открытых данных фактически не производится из-за того, что в законодательстве отсутствуют процедуры (практические рекомендации) по публикации открытых данных, в том числе и на Портале открытых данных, а также требования к технологическим, программным и лингвистическим средствам,	**П**	Законодательство Молдовы содержит специальный Закон «О повторном использовании информации публичного сектора», который обязывает государственные органы и учреждения публиковать на Едином правительственном портале открытых данных, всю информацию, которая накапливается и собирается государственными органами и учреждениями, в формате, позволяющем осуществлять автоматическую обработку документов и метаданных. В целях реализации данного Закона, было принято Постановление

	необходимым для размещения информации государственными органами и органами местного самоуправления в сети Интернет в формате открытых данных. Также, в законе не закреплены правовые основания для использования открытых программных продуктов (Open Source) и открытого API (Application Programming Interface).		Правительства Республики Молдова «Об утверждении Методологии опубликования открытых правительственных данных», в котором описывается: - тип информации, которая будет открыта и опубликована, - порядок ее составления и опубликования, - порядок доступа к этой информации, - использование API (интерфейсы для программирования приложений) и другие вопросы, связанные с взаимодействием с Единым порталом государственных данных государственных органов и учреждений.
6.5	В законодательстве КР отсутствуют базовые положения о защите информации и обеспечении кибербезопасности. Профильный закон, в котором такого рода положения должны содержаться – об электронном управлении – содержит лишь положения о защите права на доступ к информации и защите прав обладателя информации. Эти права являются важными элементами кибербезопасности, однако ни защита информации, ни обеспечение кибербезопасности не могут быть сведены лишь к правам основных участников правоотношений в цифровой среде. В связи с этим базовые положения об обеспечении кибербезопасности, в частности, о стандартизации и техническом регулировании в данной области должны быть закреплены на уровне закона.	**П**	IT-сообщество, сегодня, кроме защиты информации все больше говорит об обеспечении киберустойчивости, суть которой заключается в обеспечении бесперебойного и устойчивого функционирования информационной инфраструктуры в условиях существования постоянных рисков кибербезопасности. Тем самым основные усилия необходимо направить на проектирование систем с учетом требований обеспечения их киберустойчивости. При этом, одним из основных и важных направлений обеспечения киберустойчивости является устойчивость международных Интернет соединений. Так как, в условиях развития цифровой экономики, финансовый и бизнес секторы, при осуществлении международных транзакций и других видов международного взаимодействия, все больше используют технологические возможности Интернета. В итоге большинство международных экспертов приходят к тому, что в реалиях XXI века существует острая необходимость в движении в сторону киберустойчивости, которая подразумевает способность быстрого восстановления после киберинцидентов.

			Другой тенденцией мировой практики в области обеспечения кибербезопасности является использование подходов по обеспечению безопасности цепочки поставок (Supply chain security), суть которой заключается в обеспечении безопасности всей цепочки поставок (товаров, услуг, работ и т.д.). Сегодня цепь поставок становится транснациональной и глобальной, безопасность цепочек поставок становится все более важной. Наличие широкого круга рисков кибербезопасности, в том числе связанных с человеческим фактором, у одного участника может вызвать трудности у всех остальных партнеров, взаимосвязанных между собой информационно-коммуникационными технологиями. Кроме вышеназванных тенденций в области обеспечения кибербезопасности многие страны начали обращать особое внимание на вопросы обеспечения безопасности критической информационной инфраструктуры (далее – КИИ). В мировой практике существует различные подходы в регулировании безопасности КИИ. По результатам сравнительно-правового анализа таких подходов в качестве обобщения можно выделить две основные модели регулирования безопасности КИИ в зависимости от непосредственного предмета регулирования: «объектную» (РФ, Казахстан, Германия) и «субъектно-деятельностную» (ЕС кроме Германии, Грузия, Сингапур, Китай, Япония).

Комментарии

Информационные правоотношения в Кыргызстане складываются из отношений по распространению информации и получению доступа к ней, в том числе, в форме открытых данных. В рамках этих отношений осуществляется категоризация информация по видам, а также реализуется защита информации.

В законодательстве КР, прежде всего, в статье 12 Закона КР «Об электронном управлении» общедоступная информация рассматривается как правовой режим информации, противостоящий конфиденциальной информации. В зарубежных странах общедоступность информации является не столько элементом правового режима самой информации, сколько следствием реализации базового права человека на доступ к информации, предусмотренного

статьей 19 Всеобщей декларации прав человека и статьей 19 Пакта Международного пакта о гражданских и политических правах (Нью-Йорк, 16 декабря 1966 г.). Например, в США, по общему правилу, вся информация, находящаяся в открытом доступе, в том числе сведения персонального характера, может быть использована без ограничений, за исключением случаев, указанных в законе (принцип «разрешено по умолчанию, если иное не установлено законом»). Это основано на Первой поправке к Конституции США о защите свободы слова. Открытый характер сети Интернет подчеркнут в решениях Верховного суда США. Такой подход, с одной стороны, способствует максимально широкому использованию информации в обществе, с другой, не создает условий для нарушения прав обладателей информации, которые могут ограничить доступ к информации, если им на то предоставлено право законом.

Закон КР об электронном управлении устанавливает, что конфиденциальной признается информация, доступ к которой ограничен в соответствии с законом или решением обладателя информации. Законами Кыргызской Республики доступ к информации ограничивается только в целях защиты национальной безопасности, общественного порядка, охраны здоровья и нравственности населения, защиты прав и свобод физических и юридических лиц. Вводимые ограничения должны быть соразмерными указанным целям. К конфиденциальной информации относятся сведения:

1) о частной жизни человека;

2) о содержании переписки, телефонных и иных переговоров, почтовых, телеграфных, электронных и иных сообщений;

3) составляющие коммерческую тайну;

4) о материалах предварительного расследования, иные сведения, доступ к которым ограничивается в соответствии с процессуальным законодательством;

5) составляющие налоговую, банковскую, медицинскую, адвокатскую, журналистскую тайну, тайну усыновления и тайну страхования, иную профессиональную тайну;

6) иные сведения в соответствии с законодательством Кыргызской Республики.

В законодательстве Кыргызстана (в иных законодательных актах, кроме закона об электронном управлении) режим доступа к информации плохо структурирован и не систематизирован, что приводит к значительным наложениям и нестыковкам между режимами разных тайн, значительно затрудняющим использование соответствующей информации, в том числе такое использование, которое не может нарушать права лиц, к которым относится та или иная тайна.

В целях унификации правовых режимов охраняемых законом тайн в действующем законодательстве необходимо, в соответствии с положениями Конституции, ограничить их применение только к следующим видам данных:

- данным, составляющим государственную тайну;
- данным, составляющим коммерческую тайну;
- данным, представляющим собою профессиональную или процессуальную тайну;
- данным о частной жизни гражданина.

При построении данного законодательного института следует ориентироваться на опыт США и Европы, где сложилась система тайн, выстроенных как по отраслевому (банковская тайна, тайна связи) признаку, так и по предметному (коммерческая тайна, тайна частной жизни), при этом государственные секреты (государственная тайна) выделены в отдельный институт. Данные правовые режимы имеют значительную историю своего развития и направлены на защиту важнейших интересов тех лиц, к которым они относятся. Основанием для установления режима тайны во всех случаях является то, что разглашение информации, составляющей ту или иную тайну, способно причинить вред тому лицу, к которому относится тайна («принципалу тайны»). В качестве общего правила в отношении каждого охраняемой законом тайны в рамках специальных законов должны быть определены:

- перечень данных, доступ к которым ограничен, либо порядок отнесения конкретных данных к тайне уполномоченными лицами;

- перечень мер правового, организационного и технического характера, принимаемых для ограничения доступа к данным;
- исчерпывающий перечень оснований ответственности за нарушение установленных законодательством ограничений доступа к данным.

В Кыргызстане есть необходимые условия, чтобы активным образом продвинуться вперед в отношении инициативы открытых данных. Действующая законодательная база содержит достаточно правовых оснований для размещения государственными органами и органами местного самоуправления имеющейся в их распоряжении информации в формате открытых данных.

Нормативно-правовое регулирование охватывает:

- понятие и принципы открытых данных;
- порядок ограничения доступа к информации;
- порядок распространения и использования общедоступной информации;
- обязанность государственных органов и органов местного самоуправления, а также организаций, финансируемых из республиканского и местных бюджетов, обеспечивать доступ к информации, находящейся в их ведении;
- перечень категорий информации, которую государственные органы и органы местного самоуправления обязаны обнародовать ежегодно и в доступной форме;
- периодичность размещения информации в сети Интернет в форме открытых данных;
- право на защиту в установленном порядке в случае нарушения прав на доступ к информации и т.д.

В целях предоставления наиболее полного перечня общедоступной информации о деятельности органов государственной власти и органов местного самоуправления в 2019 году запущен Портал открытых данных, состоящий из совокупности программных и аппаратных средств, обеспечивающих взаимодействие между оператором Портала, поставщиками открытых данных и пользователями при публикации и использовании открытых данных.

Следует отметить и наличие пробелов в действующем законодательстве КР.

Так, нормативно-правовыми актами не установлены процедуры публикации данных и требования к технологическим, программным и лингвистическим средствам, необходимым для размещения информации государственными органами и органами местного самоуправления в сети Интернет в форме открытых данных. Не закреплены правовые основания для использования открытых программных продуктов (Open Source) и открытого API (Application Programming Interface) – программного интерфейс-приложения, состоящего из определенного набора технических протоколов и методов, благодаря которым программы могут обмениваться информацией. Проще говоря, открытые API позволят свободно интегрировать "части" одной программы внутрь другой или внутрь стороннего сайта.

Сегодня открытый API – двери в цифровую среду. Обязанность использования открытого API государственными органами при публикации открытых данных позволит разработчикам получать доступ к базам данных. Открытый интерфейс даст возможность сторонним разработчикам и другим бизнесам создавать инструменты доступа к данным, а также приложения для клиентов. Это позволит не только образовывать новые, но и совершенствовать старые сервисы и продукты. Таким образом, размещение интерфейсов в открытом доступе дает толчок развитию инноваций.

На сегодняшний день требуют законодательного закрепления нормы о порядке публикации открытых данных Кыргызской Республики, которые содержали бы:

- практические рекомендации по публикации открытых данных, в том числе и на Портале открытых данных,
- требования к технологическим, программным и лингвистическим средствам, необходимым для размещения информации государственными органами и органами местного самоуправления в сети Интернет в форме открытых данных,
- право на использование программных продуктов с открытым исходным кодом (Open Source) и открытого API.

Открытие государственных данных является общемировым трендом. Компанией Open Data Watch проводится ежегодная оценка охвата и открытости данных, представленных на веб-сайтах национальных статистических управлений и на любом официальном правительственном веб-сайте. Составляемый на данных исследованиях Реестр открытых данных помогает выявлять критические пробелы, продвигать политику открытых данных, улучшать доступ к данным и поощряет диалог между национальными статистическими управлениями и пользователями данных.

Так, по оценке на конец июля 2021 года, проведенной по 187 странам мира, лидируют Сингапур, Польша и Финляндия. Лидирующие позиции также у Дании, Швеции, Нидерландов, Словении, Норвегии, Монголии, Словакии, Германии, Ирландии, Канады, ОАЭ, Литвы, Филиппинов, Молдовы и Палестины.

Крупнейшее государство Евросоюза – **Федеративная республика Германия** в декабре 2014 года опубликовала Национальный план действий федерального правительства по реализации Хартии открытых данных G8. По этому плану действий федеральное правительство взяло на себя обязательства:

- обеспечить публикацию столь многих данных сколь возможно через разработку нормативных документов и других инструментов;
- опубликовать столько существующих государственных массивов данных сколько только возможно;
- GovData будет центральным порталом для федеральных, региональных и местных органов власти;
- проведение регулярного диалога с гражданским обществом, бизнесом, журналистами и исследовательским сообществом.

Также, Германия уникальна в том, что в государстве создана библиотека проектов, основанных на открытых данных. Библиотека Datalook представляет собой подборку лучших проектов, основанных на использовании разного типа данных. С помощью сервиса можно найти существующие проекты и приложения для решения любого рода задач. Кроме того, пользователи могут обсуждать существующие и добавлять свои собственные общественно значимые проекты, связываться с авторами проектов.

Соединенные Штаты Америки стали одной из первых стран, запустивших портал открытых государственных данных. Федеральный портал Data.gov был запущен в 2009 году для сбора и публикации данных различных госведомств с целью дальнейшего использования.

Законодательство США в сфере открытых данных, представлено Законом о свободе информации, который был принят в 1967 году. Закон требует полного или частичного раскрытия ранее не опубликованной информации и документов, держателем которых является Правительство США. Развитие информационных технологий привело к лучшему пониманию значения правительственной информации для надзора, анализа и ее использования. В 2013 году Администрация Барака Обамы приняла Указ об открытых данных, Руководство по политике открытых данных для агентств, которые стали политикой раскрытия открытых данных с использованием стандартизированных машиночитаемых форматов данных. В 2019 году в США вступил в силу Закон об открытых, общедоступных, электронных и необходимых правительственных данных (OPEN), который уже обязует федеральные агентства публиковать информацию в сети Интернет в виде открытых данных, с использованием стандартизированных машиночитаемых форматов данных, а их метаданные должны быть включены в каталог Data.gov.

Также ресурсом, отражающим открытость органов власти, является сайт – congressspeaks.com, анализирующий публичные заявления конгрессменов (какие термины используют в речи, как голосуют и т.д.). На портале представлена активность политических деятелей из различных партий и штатов, и все это упаковано в привлекательную анимацию сайта, что обуславливает высокую посещаемость ресурса среди населения.

Великобритания также входит в число стран-лидеров по уровню открытости правительственных данных. Имеющееся законодательство является достойным примером для

подражания другими странами опыта перехода к политике открытых данных. Акт о свободе информации (Freedom of Information Act 2000) устанавливает:

- право любого лица на доступ к информации, принадлежащей органам публичной власти;
- право быть информированным о наличии у органа публичной власти соответствующей информации;
- право на получение указанной информации по запросу лица;
- право на повторное использование наборов данных.

В 2011 году Правительством Великобритании был опубликован документ «Принципы информации», которым должны следовать все органы власти в информационной сфере.

Положение о повторном использовании информации, находящейся в распоряжении публичных органов власти (принятый в 2015 г.) регулирует право частных субъектов на повторное использование информации в коммерческих и некоммерческих целях. Акт уточняет требования к запросу на повторное использование, а также определяет обязанность публичных органов публиковать перечни данных для повторного использования и условия доступа к таковым.

Подходы к правовому регулированию унификации форматов представления информации и технологий информационного обмена в государственных информационных системах регулируют Принципы открытых стандартов (Open Standards Principles 2018), соедржащие следующие критерии выбора стандартов, которые должны:

– соответствовать потребностям пользователя,
– обеспечивать равный доступ поставщиков к гос. контрактам,
– быть гибкими и способными к изменениям,
– быть обоснованными,
– быть транспарентными.

Принципы гарантируют, что будущие технологии будут доступными, безопасными и инновационными. Они описывают, как правительство будет определять и выбирать открытые стандарты и как эти стандарты могут быть внедрены в программное обеспечение с открытым исходным кодом и проприетарное программное обеспечение. Все государственные ведомства и агентства должны использовать эти принципы.

Так, Компания Tesco является ритейлером №1 в Великобритании и №3 в мире, которая управляет около 2700 торговыми центрами по продаже продовольствия и промышленных товаров с помощью портала открытых данных, а именно данных, предоставляемых метеорологическими службами, создала почасовую модель спроса потребителей.

Приложение GP Ratings оценивает медицинские клиники Англии, используя открытые данные о клиниках, отображает рейтинговую информацию на основе множества параметров, позволяя пользователям располагать, сравнивать и идентифицировать клиники в соответствии с пользовательскими требованиями. Приложение доступно в iTunes, исходный код в Github, поэтому все желающие могут создавать такие приложения как Рейтинги школ, рейтинги госпиталей и много других.

Республика Молдова является одной из первых стран в Европе, которая начала электронное преобразование правительства. Проблемы, над решением которых, многие страны начали задумываться только сейчас, Молдова начала решать уже более 10 лет назад. По оценке 2021 года Молдова заняла 19-е место из 187-и в глобальном рейтинге по охвату и открытости данных. Законодательство Молдовы содержит специальный Закон «О повторном использовании информации публичного сектора»[11], который обязывает государственные органы и учреждения публиковать на Едином правительственном портале открытых данных, всю информацию, которая накапливается и собирается государственными органами и учреждениями, в формате, позволяющем осуществлять автоматическую обработку документов и метаданных. В целях реализации данного Закона, было принято Постановление

[11] http://lex.justice.md/viewdoc.php?action=view&view=doc&id=347200&lang=2

Правительства Республики Молдова «Об утверждении Методологии опубликования открытых правительственных данных»[12], в котором описывается тип информации, которая будет открыта и опубликована, порядок ее составления и опубликования, порядок доступа к этой информации, использование API (интерфейсы для программирования приложений) и другие вопросы, связанные с взаимодействием с Единым порталом государственных данных государственных органов и учреждений. Также, есть утвержденная «Концепция о принципах открытых данных»[13], в которой раскрыты основные проблемы реализации данного Закона и способы их решений в краткосрочной и долгосрочной перспективе. В целом, Республика Молдова обладает большим опытом, отталкиваясь от которого, можно повторить успехи и избежать ошибок, при внедрении инициативы открытых правительственных данных. Правительственный портал данных date.gov.md включает в настоящее время 3 основных модуля:

- открытые дата-сеты министерств и учреждений центральной государственной администрации, обнародованные в считываемых с компьютера форматах. На основе открытых правительственных данных, представленных в виде первичных данных непосредственно от источника, юридические лица (частные и государственные) и физические лица могут разрабатывать приложения, имеющие значительное социальное воздействие для граждан и деловой среды, а также осуществлять анализ и исследования в представляющих интерес областях и пр. (Open Government Data).
- модуль «Поиск в открытых данных», позволяющий искать, извлекать, просто и удобно просматривать открытые данные в различных регистрах, базах данных и пр., держателями которых являются государственные органы и которые обнародованы для быстрой и простой визуализации;
- модуль доступа к данным, представляющим общественный интерес, в том числе к персональным данным из государственных регистров и информационных систем, для категорий пользователей, которые – на основе законной цели и на законном основании – имеют право и возможность открывать их после электронной аутентификации и подтверждения законного основания (авторизованный доступ).

На основе сведений, опубликованных на Портале открытых правительственных данных, Expert-Grup (независимый аналитический центр из Кишинева) запустил BudgetStories.md - веб-сайт открытого бюджета, который включает в себя инфографику, визуализацию бюджетных данных и анализ использования государственных денег в Молдове в таких секторах, как государственное управление, сельское хозяйство, образование и здравоохранение. В последние годы правительство Молдовы стало более прозрачным в отношении бюджетных данных, а также других типов данных. Министерство финансов использовало инструмент BOOST Всемирного банка для выпуска подробных и дезагрегированных данных о государственных расходах. На данный момент на Правительственном портале открытых данных Молдовы опубликовано 1126 наборов данных и 10488 файлов, которые были скачаны около 5,5 миллионов раз.

В **Украине** действует Закон «О доступе к публичной информации»[14], который определяет публичную информацию в форме открытых данных как публичную информацию в формате, позволяющем ее автоматизированную обработку электронными средствами, свободный и бесплатный доступ к ней, а также ее дальнейшее использование. Распорядители информации обязаны предоставлять публичную информацию в форме открытых данных на запрос, обнародовать и регулярно обновлять ее на едином государственном веб-портале открытых данных и на своих веб-сайтах.

Постановлением кабинета министров Украины[15] утверждено «Положение о наборе данных, подлежащих опубликования в форме открытых данных» и «Порядок ежегодной

[12] http://lex.justice.md/viewdoc.php?action=view&view=doc&id=354534&lang=2
[13] http://lex.justice.md/viewdoc.php?action=view&view=doc&id=354533&lang=2
[14] https://zakon.rada.gov.ua/laws/show/2939-17#Text
[15] https://zakon.rada.gov.ua/laws/show/835-2015-%D0%BF#n12

оценки состояния обнародования и обновления открытых данных распорядителями информации на Едином государственном веб-портале открытых данных.».

Бизнес в Украине начал активно использовать любые данные, которые можно монетизировать. Ажиотажный спрос на open data привел к появлению множества стартапов, продуктов и сервисов. Открытые данные стали ресурсом, который открывает новые пути для развития. Открытие публичных данных уже оказало огромное влияние на экономику Украины, работу государственных структур и на общество в целом.

Так, публикация данных Министерством экологии Украины привела к появлению онлайн-сервиса «Чиста вода». Это карта, на которой отмечено 400 пунктов контроля воды. Уровень загрязнения в конкретном пункте или регионе отслеживается по 16 параметрам. Используя сервис Cost Ukraine, можно промониторить состояние дорог, узнать, где проходит ремонт. Открытые данные от Министерства здравоохранения способствовали появлению проекта «Донор.UA». Его цель — мониторинг запасов донорской крови, а также привлечение желающих к сдаче крови.

Среди наиболее известных украинских стартапов, которые используют открытые данные для бизнеса, — Agri Eye (выходец из инкубатора 1991 Open Data Incubator). Команда разработала систему аналитики полей, использующую Deep Learning. Над полями запускают дроны, которые генерируют данные. На основе собранных показателей строится прогноз урожайности культур. Финансовый сектор тоже не отстает. OTP Bank совместно с Open Data Incubator запустили проект Open Banking Lab. На основе открытых банковских данных разрабатывают продукты для автоматизации процессов и принятия решений в финансовой сфере. YouScore – скоринговая система, в которой используются разные реестры открытых данных. Её задача — оценить финансовую благонадежность физлица или предприятия по заданным критериям.

Распространение государственных данных в открытых форматах позволит получить экономический и социально-культурный эффект для страны, такой как повышение прозрачности деятельности государственных органов и органов местного самоуправления, укрепление доверия граждан к государству, развитие инновационной среды, рынка приложений и сервисов, полезных для граждан, в том числе и экономию бюджетных расходов при разработке общественно полезных сервисов и т.п. При этом необходимо учитывать важную роль использования открытых стандартов - одного из самых мощных инструментов, которые есть для открытия правительства. Они позволяют самому маленькому бизнесу конкурировать с самым крупным. Они делают данные открытыми для проверки любым гражданином. Они раскрывают преобразующую силу программного обеспечения с открытым исходным кодом.

В законодательстве КР отсутствуют базовые положения о защите информации и обеспечении кибербезопасности. Профильный закон, в котором такого рода положения должны содержаться – об электронном управлении – содержит лишь положения о защите права на доступ к информации и защите прав обладателя информации. Эти права являются важными элементами кибербезопасности, однако ни защита информации, ни обеспечение кибербезопасности не могут быть сведены лишь к правам основных участников правоотношений в цифровой среде. В связи с этим базовые положения об обеспечении кибербезопасности, в частности, о стандартизации и техническом регулировании в данной области должны быть закреплены на уровне закона.

Кыргызстан значительно отстает от мировых тенденций в области кибербезопасности. Сегодня парадигма обеспечения информационной безопасности начала меняться и все больше государств и компаний приходят к понимаю, что построение защиты, которую нельзя сломать, - утопично по своей сути. Еще несколько лет назад информационные технологии расценивались, в большей степени, как средства облегчения документооборота и автоматизации бизнес-процессов. В связи с этим наблюдался рост востребованности высокоинтеллектуальных средств защиты, позволяющих решать задачи по своевременному выявлению атак и инцидентов. (системы класса security information and event management (SIEM), network traffic analysis (NTA), комплексных antiAPT решениях). В таких условиях

главной задачей любой системы безопасности было максимально быстро обнаружить атаку и атакующего в системе, сократить окно его возможностей настолько, чтобы он не успел нанести непоправимый вред. Достаточно было создать необходимый периметр безопасности, которая будет нацелена на поиск и обнаружение нарушителя периметра безопасности. Однако в условиях, когда процессы выходят за пределы периметра безопасности, непрерывного развития технологий, когда субъекты становятся более мобильными размываются конкретные периметры безопасности. При таком стечении обстоятельств становится сложным найти точку применения вышеуказанных инструментов безопасности. В связи с этими рисками мы должны принять их и понимать, что предотвратить киберпреступления практически невозможно.

Учитывая данные обстоятельства IT-сообщество, сегодня, кроме защиты информации все больше говорит об обеспечении **киберустойчивости**, суть которой заключается в обеспечении бесперебойного и устойчивого функционирования информационной инфраструктуры в условиях существования постоянных рисков кибербезопасности. Тем самым основные усилия необходимо направить на проектирование систем с учетом требований обеспечения их киберустойчивости. При этом, одним из основных и важных направлений обеспечения киберустойчивости является устойчивость международных Интернет соединений. Так как, в условиях развития цифровой экономики, финансовый и бизнес секторы, при осуществлении международных транзакций и других видов международного взаимодействия, все больше используют технологические возможности Интернета. В итоге большинство международных экспертов приходят к тому, что в реалиях XXI века существует острая необходимость в движении в сторону киберустойчивости, которая подразумевает способность быстрого восстановления после киберинцидентов.

Другой тенденцией мировой практики в области обеспечения кибербезопасности является использование подходов по обеспечению **безопасности цепочки поставок (Supply chain security)**, суть которой заключается в обеспечении безопасности всей цепочки поставок (товаров, услуг, работ и т.д.). Сегодня цепь поставок становится транснациональной и глобальной, безопасность цепочек поставок становится все более важной. Наличие широкого круга рисков кибербезопасности, в том числе связанных с человеческим фактором, у одного участника может вызвать трудности у всех остальных партнеров, взаимосвязанных между собой информационно-коммуникационными технологиями. В большинстве случаев мы сталкиваемся с проблемами, когда поставляемое информационно-телекоммуникационное оборудование или программные продукты намеренно или неосознанно поставляется с нелицензированным программным обеспечением или уже с установленными вредоносными программами. То есть, из-за взаимосвязанности цепочек поставок слабая безопасность одного звена может поставить под угрозу функциональность всей цепочки поставок. Атака на цепочку поставок может произойти в любой отрасли, как в финансовом, так и в государственном или частном секторе.

Кроме вышеназванных тенденций в области обеспечения кибербезопасности многие страны начали обращать особое внимание на вопросы **обеспечения безопасности критической информационной инфраструктуры** (далее – КИИ). В мировой практике существует различные подходы в регулировании безопасности КИИ. По результатам сравнительно-правового анализа таких подходов в качестве обобщения можно выделить две основные модели регулирования безопасности КИИ в зависимости от непосредственного предмета регулирования: «объектную» (РФ, Казахстан, Германия) и «субъектно-деятельностную» (ЕС кроме Германии, Грузия, Сингапур, Китай, Япония).

Раздел 7. Персональные данные

Содержание

- принципы и основания обработки
- категории данных
- права субъекта
- обязанности оператора
- трансграничная передача
- контроль и надзор

Текущее регулирование (действующее законодательство):

1. Закон Кыргызской Республики «Об информации персонального характера» от 14 апреля 2008 года № 58
2. Закон Кыргызской Республики «О биометрической регистрации граждан Кыргызской Республики» от 14 июля 2014 года №136
3. Постановление Правительства Кыргызской Республики «Об утверждении Порядка получения согласия субъекта персональных данных на сбор и обработку его персональных данных, порядка и формы уведомления субъектов персональных данных о передаче их персональных данных третьей стороне» от 21 ноября 2017 года № 759
4. Постановление Правительства Кыргызской Республики «Об утверждении Требований к обеспечению безопасности и защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных» от 21 ноября 2017 года № 760
5. Постановление Кабинета Министров Кыргызской Республики «О Государственном агентстве по защите персональных данных при Кабинете Министров Кыргызской Республики» от 22 декабря 2021 года № 325

Краткое описание выявленных недостатков и ориентиров из мировой практики

№	Описание недостатка	Тип[16]	Лучшая практика
7.1	Отсутствуют определения: - биометрических персональных данных - псевдонимизация; - профилирование Требуются дополнения в статью 3 Закона Термины и определения	**П**	Определения приводятся в Регламенте Европейского Парламента и Совета Европейского Союза 2016/679 от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных) (General Data Protection Regulation) (GDPR)
7.2	Биометрические персональные данные не отнесены к особо чувствительным/специальной категории ПД	**П**	Биометрические данные относятся к специальным категориям персональных данных как в GDPR (Статья 9), так и в обновленной Конвенции Совета Европы о защите физических лиц при

[16] В таблице приводятся следующие типы недостатков регулирования:
(П) пробел в регулировании (регулирование требуется, но его нет)
(У) устаревшая норма (норма есть, но её нужно менять)
(Н) неработающая норма (норма есть, но в силу описанных причин она не работает)
(Б) действующая норма является необоснованным препятствием для осуществления деятельности

	Решением Конституционной палаты от 14 сентября 2015 года N 11-р указано, что «Биометрические данные являются особо чувствительной категорией персональных данных, незаконное использование которых создает угрозу и может нанести существенный вред правам и законным интересам субъектов этих данных.»		автоматизированной обработке персональных данных
7.3.	Круг оснований для обработки особо чувствительных (специальных категорий) данных не охватывает все необходимые случаи (в действующем законе указано только 2 исключения – наличие согласия, и когда обработка необходима для защиты здоровья и безопасности)	**П**	Статья 9 GDPR содержит, как минимум, 10 оснований для обработки специальных категорий персональных данных, каждое из которых служит определенной цели в цифровом обществе
7.4.	Наличие в законе требования о подписании электронной подписью согласия на обработку персональных данных в форме электронного документа является устаревшей нормой – с момента принятия Закона «Об информации персонального характера» прошло более 10 лет, за это время произошли глобальные технологические изменения, внедряются новые информационные и коммуникационные технологии. Тем не менее, действующий закон пока не признает выражение лицом своей воли с помощью электронных или иных технических средств (например, путем передачи сигнала, при заполнении формы в сети Интернет, в информационной системе, в том числе в приложении, установленном в смартфоне, при нажатии клавиши ОК) для полноценного юридически значимого волеизъявления на обработку своих персональных данных, наряду с электронной подписью.	**У**	Статья 4 (11) GDPR: «Согласие» субъекта данных — это добровольное, конкретное, информированное и однозначное волеизъявление, в котором субъект данных с помощью заявления или четкого утвердительного действия дает согласие на обработку своих персональных данных; Статья 7 GDPR. Условия согласия 1. Если обработка производится на основе согласия, контролёр должен быть в состоянии продемонстрировать, что субъект данных дал согласие на обработку своих персональных данных. 2. Если согласие субъекта данных дается в письменной декларации, которая также касается и других вопросов, запрос согласия должен быть представлен ему таким образом, чтобы запрос четко отличался от других вопросов, был в понятной и доступной форме, использовал ясный и простой язык. Любая часть такой декларации, которая представляет собой нарушение настоящего Регламента, не является обязательной.

			Руководство по согласию в соответствии с Регламентом 2016/679 (Guidelines on consent under Regulation 2016/679) 79. Без ущерба для существующего (национального) договорного права, согласие может быть получено посредством записанного устного заявления, хотя необходимо должным образом учитывать информацию, доступную субъекту данных, до указания согласия. Использование предварительно отмеченных полей недействительно в рамках GDPR. При этом молчание или бездействие со стороны субъекта данных, а также простое обращение к услуге не могут рассматриваться как активное указание выбора
7.5.	Закон не предусматривает возможность отзыва согласия в любое время и в том же порядке/форме, что и выражение согласия.	**П**	Статья 7 GDPR. Условия согласия 3. Субъект данных имеет право в любое время отозвать свое согласие. Отзыв согласия не влияет на законность обработки, которая была основана на согласии до его отзыва. Субъект данных должен быть проинформирован об этом перед тем, как он выразил согласие. Отзыв согласия должен быть столь же прост, как и его выражение.
7.6.	Круг оснований для обработки персональных данных в законе КР не соответствует потребностям цифровой экономики и международным стандартам, в частности, не указано, что обработка персональных данных может быть необходима для исполнения договора. Это является пробелом в действующем законодательстве, приводит к тому, что банки, операторы связи, или компании для заключения трудового договора, или любые поставщики услуг – вынуждены отбирать согласие на обработку ПД, что нивелирует саму суть института согласия как свободного волеизъявления, которое тем самым ставится под условие получения или неполучения	**П**	Статья 6 GDPR. Законность обработки 1. Обработка является законной только в тех случаях, когда — и в той степени, в которой — выполнено по меньшей мере одно из следующих условий: (a) субъект персональных данных дал согласие на обработку своих персональных данных для одной или нескольких конкретных целей; (b) обработка необходима для исполнения договора, в котором субъект данных является стороной, или для реализации по поручению субъекта данных шагов, предшествующих заключению договора;

	определенной услуги (банковской, услуги связи и т.п.).		(c) обработка необходима для выполнения правового обязательства, возложенного на контролёра; (d) обработка необходима для защиты жизненно важных интересов субъекта данных или другого лица; (e) обработка необходима для выполнения задачи в публичном интересе или в рамках осуществления государственной власти, доверенной контролёру; (f) обработка необходима для целей, вытекающих из легитимных интересов, преследуемых контролёром или третьим лицом, за исключением случаев, когда преимущество над такими интересами имеют интересы или фундаментальные права и свободы субъекта данных, требующие защиты персональных данных, в частности, когда субъектом данных является ребенок. Пункт (f) первого подпараграфа не применяется к обработке, которую осуществляют государственные органы при выполнении ими своих задач.
7.7.	Закон не учитывает в полном объеме все права субъектов персональных данных, содержащихся в международных стандартах, что влияет на возможности их защиты. Такие как: - Право на удаление данных ("право быть забытым"); (Всякое применение «право на забвение» должно быть строго ограничено, поскольку необходимо обеспечить соблюдение определенных минимальных требований, чтобы такое право не противоречило праву на свободу выражения мнений, как в смысле содержания, так и в процессуальном смысле. В частности, субъектами «права на забвение» должны быть	**П**	Статьи 15-22, 34 GDPR Guidelines Information Commissioner’s Office, Right of Access (2020). EDPB, Guidelines 8/2020 on the targeting of social media users (2020). EDPB, Guidelines 3/2019 on Processing of Personal Data through Video Devices (2020). EDPB, Guidelines 02/2021 on Virtual Voice Assistants (2021). EDPB, Guidelines 01/2022on data subject rights — Right of access (2022).

	частные лица, «право на забвение» должно применяться только к поисковым системам (в качестве операторов персональных данных), а не к хостинговым сервисам и контент-провайдерам. Всякие меры правовой защиты должны прямо ссылаться на свободу выражения мнений как основополагающее право, с которым такие меры защиты должны быть уравновешены) - Обязанность уведомления относительно изменения или уничтожения персональных данных или ограничения обработки; - Право на переносимость данных; - Право на возражение (против профилирования, прямого маркетинга); - право не подвергаться решению, которое может включать в себя конкретные меры, оценивающему характеристики личности, основанному исключительно на автоматизированной обработке и влекущему правовые последствия (как, например, автоматический отказ в онлайн-форме заявки на кредит или онлайн-рекрутинга без какого-либо человеческого посредничества; подобная обработка должна подлежать соответствующим мерам защиты, которые должны включать в себя специфическую информацию о субъекте данных и право требовать людского вмешательства, для выражения своей точки зрения, требования объяснения решения, принятого в результате такой оценки, и для изменения решения. Данная мера не должна относиться к ребенку); - право на получение информации о нарушении безопасности ПД (обязанность уведомления субъекта данных о нарушении безопасности персональных данных)		Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679; European Commission, Commission Guidance on the application of Union data protection law in the electoral context, A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September (2018). EDPB, Guidelines 8/2020 on the targeting of social media users (2020). European Commission, Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection Brussels (2020). ICO, Data sharing: a code of practice (2020). Spanish Data Protection Agency (AEPD), Guide on use of cookies (2021). Article 29 Working Party, Guidelines on the Implementation of the Court of Justice of the European Union Judgment on Google Spain Inc. v. Agencia Española de protección de datos (AEPD) and Mario Costeja González C-131/12 (2014). EDPB, Guidelines 5/2019 on the Criteria of the Right to be Forgotten in the Search Engines Cases under the GDPR (part 1) (2019). EDPB, Guidelines 02/2021 on Virtual Voice Assistants (2021). Article 29 Working Party, Guidelines on the Right to Data Portability (2017). Information Commissioner's Office, Right of Access (2020). EDPB, Guidelines 02/2021 on Virtual Voice Assistants (2021).

			Article 29 Working Party, Opinion 03/2014 on «Personal Data Breach Notification (2014). Article 29 Working Party, Guidelines on Personal data breach notification under Regulation 2016/679 (2018). EDPB, Guidelines 1/2021 on Examples regarding Data Breach Notification (2021). DPC (Ireland), Guidance for Individuals who Accidentally Receive Personal data (2020).
7.8.	Закон не стимулирует использование таких перспективных практик, как «проектируемая защита» и «защита по умолчанию» (Data protection by design and by default)	**П**	Статья 25 GDPR Принимая во внимание текущий уровень научно-технического прогресса, затраты на внедрение, характер, масштаб, контекст и цель обработки, а также риски, связанные с той или иной вероятностью и серьезностью нарушения прав и свобод физических лиц, вызванные обработкой, контролёр, как во время определения средств обработки, так и во время самой обработки, внедряет надлежащие технические и организационные меры, например, псевдонимизацию, предназначенные для эффективного внедрения принципов защиты персональных данных, таких как минимизация данных, а также для интеграции необходимых гарантий в обработку с целью соблюдения требований настоящего Регламента и защиты прав субъектов данных WP29, Opinion 05/2014 on Anonymisation Techniques (2014). WP29, Opinion on data processing at work (2017). Spanish Data Protection Agency (AEPD), A Guide to Privacy by Design (2019). EDPB, Guidelines 4/2019 on Article 25 – Data Protection by Design and by Default (2020):

			Защита данных по замыслу (проектируемая защита) должна быть реализована как во время определения средств обработки, так и во время самой обработки. Именно во время определения средств обработки контролеры должны внедрять меры и гарантии, направленные на эффективную реализацию принципов защиты данных. Чтобы обеспечить эффективную защиту данных во время обработки, контролер должен регулярно проверять эффективность выбранных мер и гарантий. EDPB, Guidelines on the use of location data and contact tracing tools in the context of the COVID-19 outbreak (2020). EDPB, Guidelines 3/2019 on Processing of Personal Data through Video Devices (2020). Spanish Data Protection Agency (AEPD), Guidelines for DataProtection by Default (2020). Information Commissioner's Office, Right of Access (2020). EDPB, Guidelines 01/2021 on Examples regarding Data Breach Notification (2021). EDPB, Guidelines 02/2021 on Virtual Voice Assistants (2021).
7.9.	Устаревшей нормой, а также коррупционным барьером, возможностью для применения карательных санкций также является наличие в ст. 30 Закона обязанности по обязательной регистрации массивов персональных данных и держателей (обладатели) этих массивов, и функций уполномоченного органа по ведению реестра держателей (обладателей) массива персональных данных. Существует риск применения карательных санкций в отношении любых юридических лиц за	**Б** **У**	Согласно ст. 36 GDPR. Предварительная консультация, Контролёр должен проконсультироваться с надзорным органом перед обработкой, если оценка воздействия на защиту персональных данных согласно Статье 35 указывает на то, что обработка может привести к возникновению высокой степени риска при отсутствии мер, принятых контролёром для снижения риска.

	формальное несоблюдение этого требования (не постановка на учет в качестве держателя). При этом закон не устанавливает процедур, например, максимально простой уведомительной онлайн регистрации держателей персданных только в целях их учета и понимания целей обработки персональных данных.		
7.10	Функции и полномочия уполномоченного государственного органа не соответствуют стандартам самостоятельности, независимости, компетенциям, задачам и полномочиям надзорных органов, которые являются существенным и необходимым компонентом защиты физических лиц, в отношении обработки их персональных данных	**П**	Статьи 51-59 GDPR
7.11	Требования к обеспечению безопасности и защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных: Не разработаны предусмотренные указанными требованиями: - Типовой перечень угроз безопасности персональных данных, содержащий все виды и типы предполагаемых угроз; - методика определения угроз безопасности в информационных системах персональных данных; - а также отраслевые перечни угроз безопасности персональных данных при осуществлении соответствующих видов деятельности Норма о том, что такие документы должны быть разработаны есть, но она не исполнена, документы не разработаны	**П**	Данный пробел вызван особенностями законодательства Кыргызской Республики
7.12	Не предусмотрено опубликование документа, определяющего политику держателя (обладателя) массива персональных данных в	**П**	Статья 12 GDPR Контролёр принимает соответствующие меры для предоставления субъекту данных

	отношении обработки персональных данных; (предусмотрено только доведение содержания данного документа до работников и контрагентов держателя (обладателя) массива персональных данных)		любой информации, указанной в статьях 13 и 14, и для осуществления коммуникации с субъектом касательно обработки данных в соответствии со статьями 15-22 и 34 в краткой, прозрачной, понятной и легко доступной форме, с использованием ясного и простого языка, — особенно, когда информация адресована ребенку. Информация должна быть представлена в письменной форме, или с помощью других средств, в том числе, в случае необходимости, электронными средствами. Преамбула 58 Эта информация может предоставляться в электронной форме, например, если она адресована общественности, на интернет-сайте
7.13	Положение о Государственном агентстве по защите персональных данных при Кабинете Министров Кыргызской Республики: Функции и полномочия уполномоченного государственного органа не соответствуют стандартам самостоятельности, независимости, компетенциям, задачам и полномочиям надзорных органов, которые являются существенным и необходимым компонентом защиты физических лиц, в отношении обработки их персональных данных	**П**	Статьи 51-59 GDPR
7.14	Не определены меры ответственности за многие правонарушения и преступления с персональными данными (необходимы дополнения в кодексы). Определяющими факторами при этом должны стать вопросы не столько наказаний за допущенные нарушения, сколько восстановления нарушенных прав субъектов и восстановлением причиненного им незаконными действиями вреда.	**П**	GDPR, статьи 83-84

Комментарии

Закон Кыргызской Республики «Об информации персонального характера» был принят 2008 году (далее – Закон), изменения в него внесены в 2017 году (в связи с принятием Закона Кыргызской Республики «Об электронном управлении» и Закона Кыргызской Республики «Об электронной подписи»).

В 2017 году в Закон об информации персонального характера были внесены изменения, согласно которым:

- установлена компетенция Правительства Кыргызской Республики по изданию нормативных правовых актов, регулирующих сферу персональных данных, включая вопросы безопасности;

- детализированы вопросы, касающиеся формы согласия субъекта на обработку его персональных данных, установлена возможность получения согласия в форме электронного документа;

- введена отдельная статья, касающаяся статуса и функций уполномоченного органа по защите персональных данных.

Указанные изменения позволили принять (в ноябре 2017 года) ряд нормативах правовых актов на уровне Правительства Кыргызской Республики, уточняющих вопросы защиты персональных данных в информационных системах

Закон Кыргызской Республики «Об информации персонального характера» направлен на правовое регулирование работы с персональными данными на основе общепринятых международных принципов в целях обеспечения защиты прав и свобод человека и гражданина, связанных со сбором, обработкой и использованием персональных данных.

В целом Закон отвечает основным международным стандартам защиты персональных данных, в том числе (Страсбургской) Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (ETS N 108) от 28 января 1981 г., однако не учитывает изменения, внесенные в эту Конвенцию протоколом ETS N 223.

Однако существуют ряд недостатков и пробелов, поскольку Закон принимался в «до-технологическую» эпоху, не учитывает сегодняшние реалии и проблемы, в том числе связанные с реагированием на вызовы, появившиеся в связи с пандемией COVID-19.

Подходы к правовому регулированию телекоммуникационной сферы, которые демонстрирует Евросоюз, имеют в настоящее время большое практическое значение для многих государств. Динамичное развитие регулирования отношений в сфере персональных данных в Евросоюзе свидетельствует о последовательном, системном и комплексном формировании, развитии и совершенствовании соответствующих нормативных и институциональных основ в их органической взаимосвязи.

В связи с чем, в качестве ориентира лучшей международной практики предлагается рассматривать Европейского Парламента и Совета Европейского Союза 2016/679 от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных) (General Data Protection Regulation) (GDPR).

Ситуация с защитой персональных данных усугубляется **устаревшим законодательством** – с момента принятия Закона «Об информации персонального характера» прошло более 10 лет, за это время произошли глобальные технологические изменения, внедряются новые информационные и коммуникационные технологии. Изменился не только подход к сбору личной информации, но и отношение общества к этой проблематике. В связи с чем, назрела необходимость зафиксировать современный уровень развития информационных и иных технологий, дать ответ на актуальные вызовы и угрозы, обусловленные постоянно расширяющимися возможностями обработки и трансграничной передачи данных личного характера.

Одно из таких глобальных изменений в международных стандартах защиты персональных данных - определение новых прав, предоставляемых гражданам, для управления своими персональными данными при их обработке, в том числе на основе

математических алгоритмов, искусственного интеллекта; обязанность держателей персональных данных уведомлять уполномоченный орган и граждан об утечках персданных.

Еще одним недостатком действующего закона об информации персонального характера является требование к форме согласия на обработку персональных данных – в письменной (офлайн) или в электронной (онлайн) форме, подписанное электронной подписью. Действующий закон не признает выражение лицом своей воли с помощью электронных или иных технических средств (например, путем передачи сигнала, при заполнении формы в сети Интернет, в информационной системе, в том числе в приложении, установленном в смартфоне, при нажатии клавиши ОК) для полноценного юридически значимого волеизъявления на обработку своих персональных данных. Остро стоит вопрос создания общегосударственной онлайн платформы управления полученными/выраженными согласиями граждан на обработку данных.

Не ясна ситуация с правовыми основаниями для обработки персональных данных. В законе не установлены все признаваемые международными актами юридические основания для работы с персданными (например, наличие договора), не ясны исключения на получение согласия для законной обработки данных, например, для школ, которые не являются государственными органами, имеющими исключение на получение согласия при исполнении своих функций.

В общем контексте современных подходов к защите прав граждан на неприкосновенность частной жизни является право на получение информации о несанкционированном доступе третьих лиц к их персональным данным, право заявить о своем несогласии, независимо от места жительства получать квалифицированную защиту, в том числе и от уполномоченного органа. Эти нормы также отсутствуют в нашем законодательстве.

В Законе также необходимо устранить пробелы, связанные с развитием цифровых технологий, дать ответ на актуальные вызовы и угрозы, обусловленные постоянно расширяющимися возможностями обработки и трансграничной передачи данных личного характера; определение новых прав, предоставляемых гражданам, для управления своими персональными данными при их обработке, в том числе на основе математических алгоритмов, искусственного интеллекта; обязанность держателей персональных данных уведомлять уполномоченный орган и граждан об утечках персданных.

В качестве мер реагирования на вызовы, появившиеся во время пандемии COVID-19, необходимо решить правовые вопросы, связанные с обработкой и передачей персональных данных в условиях чрезвычайной ситуации, трансграничной передачи персональных данных, когда невозможно получить согласие на это субъекта, вопросы доступа к чувствительным (специальной категории) медицинским данным.

Не определены меры ответственности за правонарушения и преступления с персональными данными (необходимы дополнения в кодексы – о правонарушениях[17], уголовный[18]). Определяющими факторами при этом должны стать вопросы не столько наказаний за допущенные нарушения, сколько восстановления нарушенных прав субъектов и восстановлением причиненного им незаконными действиями вреда.

На уровне процессуального законодательства не закреплены методы и средств цифровой криминалистики (компьютерной форензики), фиксации цифровых доказательств о нарушениях с персданными (и не только) в целях расследования, их исследования в суде.

[17] В Кодексе о правонарушениях от 28.10.2021 г., имеется одна статья - 228-1. Нарушение требований по защите информации персонального и коммерческого характера (Нарушение требований по организации защиты электронных документов, информации персонального и коммерческого характера, а равно неправомерное использование, обеспечение доступа и передача третьим лицам такой информации -влекут наложение штрафа на физических лиц в размере 200 расчетных показателей.).

[18] Уголовным кодексом от 28.10.2021 г., предусмотрено наказание за нарушение неприкосновенности частной жизни (ст. 190 УК), нарушение тайны переписки (ст. 193), несанкционированный доступ к компьютерной информации и электронным документам, в информационную систему или сеть электросвязи (ст. 319).

Режим трансграничных потоков данных также является вызовом в рамках интеграции Кыргызстана в Евразийском экономическом союзе, в цифровой повестке которого создание общего для ЕАЭС рынка и оборота (свободного перемещения) персональных данных граждан.

В перспективе, необходимо ставить вопрос о создании data-cert, который будет отслеживать и реагировать на факты утечки персональных данных.

До сих пор, не достаточно четко определены полномочия и компетенция уполномоченного государственного органа по защите персональных данных.

Статья 29-1 Закона об информации персонального характера, на уполномоченный государственный орган возлагает обеспечение контроля за соответствием обработки персональных данных требованиям настоящего Закона, защитой прав субъектов персональных данных. Уполномоченный государственный орган осуществляет сотрудничество с органами, уполномоченными в сфере защиты персональных данных в иностранных государствах, в частности международный обмен информацией о защите прав субъектов персональных данных. Решения уполномоченного государственного органа по защите прав субъектов персональных данных могут быть обжалованы в порядке, предусмотренном Законом Кыргызской Республики "Об основах административной деятельности и административных процедурах".

Постановлением Кабинета министров Кыргызской Республики 22 декабря 2021 года № 325 утверждено положение о Государственном агентстве по защите персональных данных при Кабинете Министров Кыргызской Республики в качестве государственного органа исполнительной власти, разрабатывающего и реализующего единую государственную политику в сфере информации персонального характера, осуществляющего функции по обеспечению защиты прав субъектов персональных данных (субъектов), регистрации держателей (обладателей) массивов персональных данных, ведению Реестра держателей массивов персональных данных. В соответствии с положением, целью деятельности Агентства является обеспечение защиты прав и свобод человека и гражданина, связанных со сбором, обработкой и использованием персональных данных, независимо от применяемых средств обработки этой информации, включая использование информационных технологий.

Задачами Агентства являются: 1) обеспечение контроля за соответствием обработки персональных данных требованиям законодательства Кыргызской Республики в сфере информации персонального характера государственными органами, органами местного самоуправления, государственными и муниципальными учреждениями и предприятиями, а также юридическими и физическими лицами независимо от формы собственности; 2) защита прав субъектов персональных данных; 3) предоставление общественности информации о ситуации с защитой персональных данных в Кыргызской Республике; 4) реализация иных задач, возложенных на Агентство, в соответствии с законодательством Кыргызской Республики.

В числе его функций - осуществление контроля путем проведения проверок за соблюдением требований законодательства Кыргызской Республики по защите персональных данных и прав субъектов персональных данных; ведение учета и регистрации массивов персональных данных и их держателей (обладателей); формирование и ведение Реестра держателей (обладателей) массивов персональных данных; согласование перечней персональных данных держателей (обладателей) массивов персональных данных; дача рекомендаций по спорным вопросам, возникающим между участниками информационного взаимодействия при обработке, хранении и передаче персональных данных, оказание содействия субъектам персональных данных в реализации и защите их прав; рассмотрение обращений субъектов персональных данных о нарушениях законодательства в сфере персональных данных и вынесение заключений; направление в правоохранительные органы материалов, связанных с нарушением прав субъектов персональных данных, предусмотренных законодательством Кыргызской Республики в сфере персональных данных, для принятия соответствующих мер по исполнению законодательства Кыргызской Республики; осуществление методической помощи по организации защиты персональных данных.

При этом, функции в сфере регулирования, координации, надзора и контроля не распространяются на персональные данные, полученные в результате деятельности органов прокуратуры Кыргызской Республики, правоохранительных органов и органов, осуществляющих оперативно-розыскную, разведывательную и контрразведывательную деятельность, производство официальной статистики19. Указанное является существенным и необоснованным ограничением в предмете надзора в сфере защиты персональных данных и не согласуется со статусом уполномоченных органов в других странах. В целом, функции и полномочия уполномоченного государственного органа не соответствуют стандартам самостоятельности, независимости, компетенциям, задачам и полномочиям надзорных органов в этой сфере согласно общепринятым международным стандартам20, которые являются существенным и необходимым компонентом защиты физических лиц, в отношении обработки их персональных данных

Несоблюдение принципов независимости и самостоятельности при создании института уполномоченного по защите персональных данных, в отсутствие установленных в законе полномочий такого органа и утвержденных и опубликованных стандартов его работы, чревато негативными последствиями для соблюдения прав человека в процессе такой реформы, созданием очередной правительственной структуры с полицейскими/карательными функциями, что особенно тревожно на фоне громких журналистских расследований о коррупции, утечек персональных данных с камер «Безопасного города», установка и использование камер с функцией распознавание лиц, , что сделано в отсутствие необходимой правовой базы и общественных обсуждений с экспертным сообществом, применение методов цифровой слежки по данным о геолокации, обработки цифрового фото и видео изображения, передачи телеметрических данных о состоянии здоровья по каналам связи, перевода государственных услуг в цифровой формат с требованием однозначной идентификации/подтверждения личности с получением и хранением персональных данных, включая биометрические, в цифровой среде.

Возможностью для коррупции и применения карательных санкций также является наличие в Законе Кыргызской Республики «Об информации персонального характера» функций уполномоченного органа по ведению реестра держателей (обладателей) массива персональных данных, существует риск применения карательных санкций в отношении любых юридических лиц за формальное несоблюдение этого требования (не постановка на учет в качестве держателя).

При этом закон не устанавливает процедур, например, максимально простой уведомительной онлайн регистрации держателей персданных только в целях их учета и понимания целей обработки персональных данных.

Другим пробелом в надлежащем регулировании сферы персональных данных, эксперты рассматривают наличие еще одного специального Закона – «**О биометрической регистрации граждан Кыргызской Республики**» от 14 июля 2014 года.

Указанный Закон самостоятельно, отличными от Закона об информации персонального характера способами, регулирует отношения, возникающие при осуществлении деятельности по сбору, обработке, хранению и использованию биометрических данных граждан Кыргызской Республики (далее - биометрические данные), актуализации и защите базы биометрических данных.

Согласно статье 4 Закона Сбор, обработка, хранение и использование биометрических данных осуществляются на принципах обязательной биометрической регистрации, а каждый гражданин Кыргызской Республики обязан пройти биометрическую регистрацию в соответствии с настоящим Законом.

Как видно из приведенных в Законе формулировок, биометрические данные выведены из-под регулирования закона об информации персонального характера, хотя по сути являются

[19] П.10 Положения

[20] В качестве главного ориентира в этой сфере предлагается рассматривать Общий регламент защиты персональных данных (GDPR) Европейского союза; стандарты деятельности надзорных органов предусмотрены статьями 51-59 GDPR.

чувствительными персональными данными – специальной категорией персональных данных согласно ст. 8 Закона об информации персонального характера.

Процедуры в отношении биометрических данных, указанные в Законе о биометрической регистрации, не синхронизированы с процедурами, предусмотренными Законом об информации персонального характера, не соответствуют европейским стандартам защиты сенситивных данных.

Для обязательной биометрической регистрации в Законе не делается никаких исключений, в том числе, для малолетних граждан, граждан, страдающих психическими расстройствами, граждан, постоянно проживающих за границей, лиц, чьи убеждения не позволяют им предоставлять биометрические данные. С обязательностью регистрации связаны основные трудности Закона: как в части противоречия его актам высшей юридической силы, так и в части реализации положений Закона.

Установление обязательной биометрической регистрации требует, во-первых, крайне конкретного определения целей, в которых используются собранные биометрические данные, во-вторых, наличия обоснованного перечня исключений из обязательной регистрации. Законом ни того, ни другого не предусмотрено: цели использования собранной биометрической информации определены крайне расплывчато (ст.2 и ст.7), а перечня исключений вообще не предусмотрено.

Указанные обстоятельства были предметом рассмотрения Конституционной палаты Верховного суда Кыргызской Республики, которая п ходатайству экспертов рассмотрела соответствие указанного Закона нормам Конституции.

Решением Конституционной палаты от 14 сентября 2015 года N 11-р положения рассматриваемого Закона признаны не противоречащими Конституции.

Также в решении указано, что при создании государственных информационных систем должны соблюдаться следующие условия: фиксирование биометрических данных граждан без унижения достоинства личности и причинения вреда здоровью; исключение возможности незаконного воспроизведения, использования и распространения биометрических данных граждан; обеспечение конфиденциальности и безопасности информации, содержащейся в государственной информационной системе, и ограничение этой информации только теми сведениями, которые необходимы для проверки подлинности идентификационных документов нового поколения.

Согласно Решению Конституционной палаты, Жогорку Кенешу Кыргызской Республики внести в Закон Кыргызской Республики "О биометрической регистрации граждан Кыргызской Республики" соответствующие изменения и дополнения, вытекающие из мотивировочной части настоящего Решения[21].

В 2017 году постановлением Правительства Кыргызской Республики от 21 ноября 2017 года № 760 утверждены «**Требования к обеспечению безопасности и защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных**».

До сих пор не разработаны Типовой перечень угроз безопасности персональных данных, содержащий все виды и типы предполагаемых угроз; методика определения угроз безопасности в информационных системах персональных данных; а также отраслевые перечни угроз безопасности персональных данных при осуществлении соответствующих видов деятельности.

Также пробелом является отсутствие требований об обязательном опубликовании (в том числе на сайте) документа, определяющего политику держателя (обладателя) массива персональных данных в отношении обработки персональных данных; (предусмотрено только доведение содержания данного документа до работников и контрагентов держателя (обладателя) массива персональных данных).

[21] Только сейчас Жогорку Кенешем Кыргызской Республики рассматриваются соответствующие изменения в данный Закон, подготовленные Кабинетом министров Кыргызской Республики для исполнения решения Конституционной палаты.

Кроме того, при поддержке ОБСЕ, ОФ «ГИИП» были разработаны Методические рекомендации по организации безопасности персональных данных в соответствии с требованиями Закона КР №58 «Об информации персонального характера», которые Государственным комитетом информационных технологий и связи (ныне – ГСЦР) рекомендованы держателям ПД. Методические рекомендации составлены с учётом предстоящих нормативно-правовых новелл и должны послужить руководством к действию для широкого круга граждан, экспертов, ИТ-аудиторов, специалистов и руководителей, так или иначе вовлечённых в процесс обеспечения безопасности персональных данных. Также ОФ ГИИП проведены тренинги по применению указанных Методических рекомендаций для различных держателей ПД.

Одним из серьезных вызовов праву на неприкосновенность частной жизни и законности обработки персональных данных стала пандемия коронавируса COVID-19.

Власти многих стран прибегают к беспрецедентным мерам, которые имеют потенциальные риски нарушения гражданских прав с опасностью продолжения вмешательства в частную жизнь и после конца пандемии. Для борьбы с вирусом правительства предпринимают разные меры, в том числе используя интернет-технологии. Среди них – слежение за зараженными или нарушившими карантин людьми – распознавание лиц, отслеживание мобильного трафика и геолокации пользователей и много других способов вмешательства в личную жизнь людей.

Поэтому мониторинг ограничений цифровых прав и свобод граждан, связанных с глобальной пандемией 2020 года, законности применение технологий цифровой слежки, сегодня особенно актуальны.

Правительства используют массовое наблюдение с помощью городских камер наблюдения и устройств видеофиксации, для того, чтобы выявлять тех, кто нарушает карантин. Отслеживание передвижения граждан, с помощью сетей мобильной связи, GPS, фиксирование локализации транзакций по картам и счетам. Государственные службы и ведомства получают безграничный доступ практически ко всему объему персональных данных людей.

Вводятся различные технологические элементы слежки, контроля за коммуникациями, цензуры публикаций, оправдывая свои действия борьбой с коронавирусом. Тем самым создаются предпосылки нарушения права на частную жизнь, свободу слова, тайну связи.

Зачастую эти меры носят избыточный либо непрозрачный для общественного контроля характер, либо вызывают много вопросов у специалистов по эффективности таких мер с учетом баланса интересов общества и государственного контроля.

Кроме того, есть большие риски, что все данные введённые жёсткие меры могут остаться и после пандемии. Декларируется, что ограничения эти временные и будут оперативно сняты после того, как кризис минует. Однако у правозащитников есть объективные сомнения на этот счет.

Поэтому мониторинг ограничений цифровых прав и свобод граждан, связанных с глобальной пандемией 2020 года, законности применение технологий цифровой слежки, сегодня особенно актуальны.

Важно, чтобы технологии поддерживали свободу, справедливость и инновации для граждан.

Несмотря на в целом прогрессивный характер законодательства в сфере защиты персональных данных, его (в целом) соответствие существующим международным стандартам в сфере прайвеси и защиты персональных данных, Закон «Об информации персонального характера», принятый в до-технологическую эпоху в 2008 году, устарел и нуждается в обновлении с учетом новых вызовов и угроз, связанных с автоматизированной, с помощью цифровых технологий, сбором и обработкой персональных данных, в целях его большего соответствия европейскому стандарту в сфере защиты персональных данных, поскольку защита физических лиц в отношении обработки персональных данных является фундаментальным правом.

С учетом изложенного, на основе правового анализа законодательства в сфере защиты персональных данных, **отмечаем наличие следующих пробелов и недостатков** в правовом регулировании данной сферы:

1. Отсутствуют определения:

- биометрических персональных данных
- псевдонимизация;
- профилирование

Требуются дополнения в статью 3 Закона Термины и определения.

2. Биометрические персональные данные не отнесены к особо чувствительным/специальной категории ПД.

Решением Конституционной палаты от 14 сентября 2015 года N 11-р указано, что «Биометрические данные являются особо чувствительной категорией персональных данных, незаконное использование которых создает угрозу и может нанести существенный вред правам и законным интересам субъектов этих данных.».

3. В законе не учтены все случаи исключений – когда обработка особо чувствительных (специальных категорий) данных допускается.

Например:

- обработка необходима в целях исполнения обязательств и определенных прав контролёра или субъекта данных в сфере трудового права, права социального обеспечения и социальной защиты;
- обработка касается персональных данных, которые субъект данных явным образом сделал публичными;
- обработка необходима для заявления, исполнения или защиты законных требований или в рамках осуществления правосудия судами;
- обработка необходима в целях профилактической или профессиональной медицины, для оценки трудоспособности работника, для диагностики медицинского состояния, предоставления медицинской или социальной помощи, или лечения;
- обработка необходима по причинам публичного интереса в области общественного здравоохранения, например, защиты от серьезных трансграничных угроз здоровью.

4. Наличие в законе требования о подписании электронной подписью согласия на обработку персональных данных в форме электронного документа

Эта норма является устаревшей – с момента принятия Закона «Об информации персонального характера» прошло более 10 лет, за это время произошли глобальные технологические изменения, внедряются новые информационные и коммуникационные технологии. Тем не менее, действующий закон пока не признает выражение лицом своей воли с помощью электронных или иных технических средств (например, путем передачи сигнала, при заполнении формы в сети Интернет, в информационной системе, в том числе в приложении, установленном в смартфоне, при нажатии клавиши ОК) для полноценного юридически значимого волеизъявления на обработку своих персональных данных, наряду с электронной подписью.

Вариант решения:

Письменная форма согласия считается соблюденной также в случае волеизъявления субъекта путем применения информационных технологий и совершения лицом действий с помощью электронных либо иных технических средств, позволяющих воспроизвести на материальном носителе в неизменном виде содержание согласия, при этом требование о наличии подписи считается выполненным, если использован любой способ, позволяющий достоверно определить лицо, выразившее волю. Нормативными правовыми актами Кабинета министров Кыргызской Республики и/или соглашением сторон может быть предусмотрен конкретный способ достоверного определения лица, выразившего согласие на обработку персональных данных.

(Например, предоставлением согласия на обработку персональных данных может являться проставление соответствующего флажка и нажатие кнопки «Отправить» при

регистрации (подаче электронного заявления) на Интернет-сайте и/или в соответствующим приложении держателя или обработчика персональных данных, установленном на устройстве субъекта персональных данных. Идентификация должна включать в себя цифровую идентификацию субъекта данных, например, посредством механизма аутентификации на основе учётных данных, которые используются субъектом данных для входа под своим логином в онлайновую службу, предоставляемую держателем/обработчиком данных. Держатель (обработчик) может использовать все приемлемые способы для того, чтобы проверить и подтвердить личность субъекта данных, который запрашивает доступ, в частности, в контексте онлайновых служб и онлайновых идентификаторов.).

5. Закон не предусматривает возможность отзыва согласия в любое время и в том же порядке/форме, что и выражение согласия.

Субъект данных имеет право в любое время отозвать свое согласие. Отзыв согласия не влияет на законность обработки, которая была основана на согласии до его отзыва. Субъект данных должен быть проинформирован об этом перед тем, как он выразил согласие. Отзыв согласия должен быть столь же прост, как и его выражение.

6. Отсутствие в качестве правового основания для обработки персональных данных договора – когда обработка персональных данных необходима для исполнения договора.

Дополнить ст. 5 новым правовым основание:

- если обработка необходима для исполнения для исполнения договора, в котором субъект данных является стороной, или для реализации по поручению субъекта данных действий, предшествующих заключению договора.

7. Закон не учитывает в полном объеме все права субъектов персональных данных, содержащихся в международных стандартах, что влияет на возможности их защиты.

Такие как:

- Право на удаление данных ("право быть забытым");

(Всякое применение «право на забвение» должно быть строго ограничено, поскольку необходимо обеспечить соблюдение определенных минимальных требований, чтобы такое право не противоречило праву на свободу выражения мнений, как в смысле содержания, так и в процессуальном смысле. В частности, субъектами «права на забвение» должны быть частные лица, «право на забвение» должно применяться только к поисковым системам (в качестве операторов персональных данных), а не к хостинговым сервисам и контент-провайдерам. Всякие меры правовой защиты должны прямо ссылаться на свободу выражения мнений как основополагающее право, с которым такие меры защиты должны быть уравновешены)

- Обязанность уведомления относительно изменения или уничтожения персональных данных или ограничения обработки;

- Право на переносимость данных;

- Право на возражение (против профилирования, прямого маркетинга);

- право не подвергаться решению, которое может включать в себя конкретные меры, оценивающему характеристики личности, основанному исключительно на автоматизированной обработке и влекущему правовые последствия (как, например, автоматический отказ в онлайн-форме заявки на кредит или онлайн-рекрутинга без какого-либо человеческого посредничества; подобная обработка должна подлежать соответствующим мерам защиты, которые должны включать в себя специфическую информацию о субъекте данных и право требовать людского вмешательства, для выражения своей точки зрения, требования объяснения решения, принятого в результате такой оценки, и для изменения решения. Данная мера не должна относиться к ребенку);

- право на получение информации о нарушении безопасности ПД (обязанность уведомления субъекта данных о нарушении безопасности персональных данных).

8. Закон не устанавливает в качестве обязательных технических и организационных мер к защите персональных данных как «проектируемая защита» и «защита по умолчанию» (Data protection by design and by default)

(обязательство внедрять надлежащие технические и организационные меры, например, псевдонимизацию, предназначенные для эффективного внедрения принципов защиты персональных данных, таких как минимизация данных, а также для интеграции необходимых гарантий в обработку с целью соблюдения требований).

9. Устаревшей нормой, а также коррупционным барьером, возможностью для применения карательных санкций также является наличие в ст. 30 Закона обязанности по обязательной регистрации массивов персональных данных и держателей (обладатели) этих массивов, и функций уполномоченного органа по ведению реестра держателей (обладателей) массива персональных данных.

Существует риск применения карательных санкций в отношении любых юридических лиц за формальное несоблюдение этого требования (не постановка на учет в качестве держателя).

При этом закон не устанавливает процедур, например, максимально простой уведомительной онлайн регистрации держателей персданных только в целях их учета и понимания целей обработки персональных данных.

10. Функции и полномочия уполномоченного государственного органа не соответствуют стандартам самостоятельности, независимости, компетенциям, задачам и полномочиям надзорных органов, которые являются существенным и необходимым компонентом защиты физических лиц, в отношении обработки их персональных данных.

11. Не разработаны предусмотренные указанными Требованиями к обеспечению безопасности и защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных:

- Типовой перечень угроз безопасности персональных данных, содержащий все виды и типы предполагаемых угроз;
- методика определения угроз безопасности в информационных системах персональных данных;
- а также отраслевые перечни угроз безопасности персональных данных при осуществлении соответствующих видов деятельности.

12. Не предусмотрено опубликование документа, определяющего политику держателя (обладателя) массива персональных данных в отношении обработки персональных данных;

(предусмотрено только доведение содержания данного документа до работников и контрагентов держателя (обладателя) массива персональных данных).

13. Не определены меры ответственности за многие правонарушения и преступления с персональными данными (необходимы дополнения в кодексы).

Определяющими факторами при этом должны стать вопросы не столько наказаний за допущенные нарушения, сколько восстановления нарушенных прав субъектов и восстановлением причиненного им незаконными действиями вреда.

Раздел 8. Большие данные

Содержание

- принципалы, операторы и пользователи данных
- переносимость данных
- локализация данных
- искусственный интеллект и нейросети

Текущее регулирование (действующее законодательство):

1. Закон Кыргызской Республики «Об инновационной деятельности»
2. Указ Президента Кыргызской Республики «О Национальной программе развития Кыргызской Республики до 2026 года» от 12 октября 2021 года УП №435
3. Постановление Правительства Кыргызской Республики «Об утверждении Плана мероприятий Кабинета Министров Кыргызской Республики по реализации Национальной программы развития Кыргызской Республики до 2026 года» от 25 декабря 2021 года №352

Краткое описание выявленных недостатков и ориентиров из мировой практики

№	Описание недостатка	Тип[22]	Лучшая практика
8.1	**Законодательство регулирующее использование технологий больших данных и искусственного интеллекта отсутствует.** Также отсутствуют: терминологический аппарат, принципы регулирования, права и обязанности субъектов, требования о локализации, возможность использования государственных данных, требования и ограничения к системам ИИ, меры по поддержке инноваций, уполномоченные органы, этический кодекс ИИ	**П**	Передовые страны и объединения, осознавая важность и актуальность технологий больших данных и искусственного интеллекта внедряют попытки нормативного регулирования данных технологий, а также принимают стратегические документы (программы, концепции, стратегии), направленные на их поддержку и развитие. **В 2020 году Европейский союз** принял Европейскую стратегию в области данных, которая направлена на создание общего европейского пространства данных для функционирования единого рынка данных. Регламент ЕС 2018/1807 «О системе свободного потока неличных данных в Европейском Союзе» от 14 ноября 2018 года, закрепил основные принципы свободного оборота данных, путем установления правил, касающихся требований к локализации данных, доступности данных для компетентных органов и переноса данных для профессиональных пользователей.

[22] В таблице приводятся следующие типы недостатков регулирования:
(П) пробел в регулировании (регулирование требуется, но его нет)
(У) устаревшая норма (норма есть, но её нужно менять)
(Н) неработающая норма (норма есть, но в силу описанных причин она не работает)
(Б) действующая норма является необоснованным препятствием для осуществления деятельности

			В рамках реализации Стратегии в области искусственного интеллекта, Европейская комиссия 7 декабря 2018 года представила Согласованный с государствами-членами план по искусственному интеллекту. План предлагает совместные действия для более тесного и более эффективного сотрудничества между государствами-членами. В 2019 году группа экспертов по ИИ при Еврокомиссии представила Рекомендации по политике и инвестициям для надежного ИИ и Руководство по этике для надежного искусственного интеллекта. В 2021 году Европейской комиссией был разработан и предложен документ «О принятии согласованных правил об искусственном интеллекте (Закон Об искусственном интеллекте)». Данный документ пока еще не имеет юридической силы, однако, в случае принятия, станет первым в своем роде, масштабным актом, регулирующим ИИ. **В 2014 году в США** была утверждена Национальная стратегия работы с большими данными, в которой были зафиксированы основные положения государственной политики США по развитию и использованию больших данных граждан, бизнеса и государства, прежде всего для достижения экономических и социальных эффектов. В 2015 NIST принял серию стандартов в сфере терминологии, архитектуры больших данных, конфиденциальности и безопасности персональных данных при использовании технологий больших данных. В 2018 и 2019 годах стандарты были пересмотрены и дополнены. В 2020 году была принята новая Федеральная стратегия «Использование данных как стратегического актива». В 2016 году был принят Национальный стратегический план исследований и разработок в области искусственного интеллекта, который содержит стратегический план

			исследований и разработок, финансируемых федеральным правительством в области ИИ (в 2019 был обновлен). В 2019 года был подписан указ «О сохранении лидерства США в области искусственного интеллекта», целью которого является установление федеральных принципов и стратегий для укрепления потенциала страны в области искусственного интеллекта для продвижения научных открытий, экономической конкурентоспособности и национальной безопасности. 1 января 2021 года вступила в силу «Национальная инициатива по искусственному интеллекту», которая предусматривает скоординированную программу всего федерального правительства по ускорению исследований и применения ИИ для экономического процветания страны и национальной безопасности, разъясняет понятие искусственного интеллекта. **В Российской Федерации** в 2019 году был принят «Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федерации», который, выделил развитие технологий больших данных, как одно из главных направлений способствующего развитию цифровой экономики. Также, 12 декабря 2019 года, был подписан «Кодекс этики использования данных», крупнейшими российскими компаниями, а также Аналитическим центром при Правительстве РФ, в целях закрепления основных принципов взаимодействия заинтересованных лиц – государства, граждан и бизнеса, создания базы для последующих регуляторных инициатив в области данных, а также формирования универсальных правил, определяющих границы допустимого поведения для всего профессионального сообщества. В

			2021 году был утвержден ГОСТ Р ИСО/МЭК 20546-2021 «Информационные технологии. Большие данные. Обзор и словарь», который закрепил основные термины, связанные с технологиями больших данных. Регулирование технологий искусственного интеллекта было положено Указом Президента РФ "О развитии искусственного интеллекта в Российской Федерации" от 10 октября 2019 г. № 490 с утверждением «Национальной стратегии развития искусственного интеллекта на период до 2030 года», в целях обеспечения ускоренного развития искусственного интеллекта, проведения научных исследований в области искусственного интеллекта, повышения доступности информации и вычислительных ресурсов для пользователей, а также совершенствования системы подготовки кадров в этой области. В рамках программы по поддержке разработчиков ИИ-систем, ожидается, что к 2024 году около 1200 компаний получат в общей сложности более 17 млрд рублей на развитие технологий ИИ. В 2020 году был запущен пятилетний эксперимент по внедрению технологий искусственного интеллекта на территории Москвы в рамках Национальной программы "Цифровая экономика Российской Федерации" (Федеральный закон от 24 апреля 2020 г. № 123-ФЗ "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"). Также Распоряжением Правительства Российской Федерации от 19 августа 2020 года №2129-р была утверждена

			«Концепция развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники на период до 2024 года», целью которой является определение основных подходов к трансформации системы нормативного правового регулирования для обеспечения возможности создания и применения технологий искусственного интеллекта и робототехники в различных сферах экономики с соблюдением прав граждан и обеспечением безопасности личности, общества и государства, одновременно с этим преследуются цели: создания предпосылок для формирования основ правового регулирования новых общественных отношений, складывающихся в связи с разработкой и применением технологий искусственного интеллекта и робототехники и систем на их основе, а также определение правовых барьеров, препятствующих разработке и применения указанных систем. В 2020 году были утверждены 2 стандарта в сфере ИИ: ГОСТ Р 59276-2020 «Системы искусственного интеллекта. Способы обеспечения доверия. Общие положения» и ГОСТ Р 59277-2020 «Системы искусственного интеллекта. Классификация систем искусственного интеллекта». Альянсом в сфере искусственного интеллекта, Аналитическим центром при Правительстве Российской Федерации, а также Министерством экономического развития Российской Федерации был разработан и подписан (26.10.2021) «Кодекс этики искусственного интеллекта», который установил общие этические принципы и стандарты поведения, которыми следует руководствоваться участникам отношений в сфере искусственного интеллекта, в своей деятельности

Комментарии

В Кыргызской Республике отсутствует нормативное правовое регулирование технологий больших данных и искусственного интеллекта, а также не закреплен понятийный аппарат указанных технологий.

Вопрос правового регулирования сбора, обработки и использования больших данных является достаточно сложным и комплексным. Сложность регулирования затрудняет разграничение режимов благоприятствования и ограничения использования больших данных. Выгоды использования больших данных представляются привлекательными и для экономической сферы, и для сферы государственного управления. Однако, вместе с тем использование больших данных ставит под угрозу неприкосновенность частной жизни, равенство граждан, посредством навязывания агрессивной политики сбора персональных данных потребителей (условием доступа к продуктам и сервисам является соблюдение правил пользования, которые зачастую представляют собой просто средство получения персональных данных потребителя); обработки открытой информации в социальных сетях о клиентах банка, для приоритетного права получения кредитов на основе собранной информации; получение бесплатных услуг, в обмен на предоставление персональных данных и т.д. К тому же, правовое регулирование не способно в настоящее время в достаточной мере разрешить все вопросы. Жесткие правовые рамки существенно ограничат возможные выгоды, в то время как отсутствие правового поля создает риск появления «серой» зоны оборота и использования больших данных.

Развитие технологий искусственного интеллекта ставит серьезные вызовы перед правовой системой, системой государственного управления и обществом в целом. Они обусловлены определенной степенью автономности действий систем искусственного интеллекта в решении поставленных задач и их неспособностью воспринимать этические и правовые нормы, учитывать их при осуществлении каких-либо действий. В настоящее время стремительно развивается коммерциализация искусственного интеллекта, такого как распознавание лиц, технологии распознавания изображений, распознавание речи, понимание естественного языка, портреты пользователей и т. д., благодаря чему технологии искусственного интеллекта станут новой движущей силой, ведущей к социально-экономическому развитию. Вследствие чего, для развития технологий искусственного интеллекта необходимо создание регуляторной среды, комфортной для безопасного развития и внедрения, основанной на балансе интересов человека, общества, государства, компаний - разработчиков систем искусственного интеллекта, а также потребителей их товаров, работ, услуг.

Тем не менее, Указ Президента Кыргызской Республики «О Национальной программе развития Кыргызской Республики до 2026 года» от 12 октября 2021 года УП №435, предусматривает реформу управления, которая включает в себя полную автоматизацию процессов управления, посредством внедрения концепции «Управление на основе данных», согласно которой все решения должны основываться на аналитике «Больших данных» («Big data»), накапливаемых государственными и частными системами, а также запуск проекта «Искусственный интеллект как база Больших данных», а утвержденный Постановлением Правительства Кыргызской Республики «План мероприятий Кабинета Министров Кыргызской Республики по реализации Национальной программы развития Кыргызской Республики до 2026 года» от 25 декабря 2021 года №352, закрепляет ответственных за реализацию задач, сроки выполнения и средства которые будут выделены на реализацию указанные мероприятий.

В то же время, обзор успешных практик и подходов правового регулирования данных технологий показал, что в мировой практике существуют различные практики и подходы, каждый из которых имеет свои положительные и отрицательные стороны. Принимая их во внимание, представляется наиболее перспективным реализация метода, основывающегося на совмещении опыта различных стран, в части внедрения наилучших практик каждого изученного подхода, что позволит создать необходимые условия для развития цифровой экономики в Кыргызской Республике.

Таким образом, правовое регулирование технологий больших данных и искусственного интеллекта должно в себя включать, но не ограничиваясь, следующие элементы:

- терминологический аппарат, согласно лучшим международным стандартам (ISO/IEC, NIST);
- основополагающие принципы регулирования (свободный режим перемещения для данных, доступность и переносимость данных и т.д.);
- права и обязанности субъектов (принципалы, операторы и пользователи больших данных; разработчики, пользователи и операторы ИИ);
- требования о локализации отдельных видов данных (финансовые, медицинские и биометрические данные) или трансграничная передача с согласия субъекта (альтернатива - передача указанного перечня данных после проведения анонимизации (процесс, посредством которого данные необратимо изменяются таким образом, что субъект данных больше не может быть идентифицирован прямо или косвенно);
- расширение возможностей использования государственных данных для исследований и разработок с обеспечением защищенности и конфиденциальности таких данных;
- требования и ограничения предъявляемые к системам ИИ (требования к системам ИИ использование которых может нанести вред, требования об уведомлении физических лиц о взаимодействии с системами ИИ, ограничения к системам ИИ использование которых может быть небезопасно для людей);
- меры по поддержке инноваций в сфере ИИ (создание регулятивных песочниц, приоритетный доступ МСБ и стартапам к регулятивным песочницам);
- определение уполномоченного органа в области ИИ;
- разработка этических кодексов и иных механизмов этического регулирования процесса разработки, внедрения и использования технологий ИИ.

Раздел 9. Национальная инфраструктура пространственных данных

Содержание

- инфраструктура пространственных данных
- пространственные метаданные
- принципы, правила использования инфраструктуры пространственных данных

Текущее регулирование (действующее законодательство):

1. Уголовный кодекс Кыргызской Республики;
2. Кодекс Кыргызской Республики об административных правонарушениях;
3. Закон Кыргызской Республики «О геодезии и картографии» от 20 марта 2002 года N 43;
4. Указ Президента Кыргызской Республики «О Национальной программе развития Кыргызской Республики до 2026 года» от 12 октября 2021 года УП №435;
5. Постановление Правительства Кыргызской Республики «О Министерстве сельского хозяйства Кыргызской Республики» от 9 марта 2021 года №83;
6. Постановление Кабинета Министров Кыргызской Республики «О подведомственных подразделениях и организациях Министерства сельского, водного хозяйства и развития регионов Кыргызской Республики от 6 августа 2021 года №116;
7. Постановление Правительства Кыргызской Республики «Об утверждении Инструкции по определению и обеспечению секретности топографо-геодезических, картографических, гравиметрических, аэрофотосъемочных материалов и материалов космических съемок на территории Кыргызской Республики» от 11 ноября 2013 года N 622;
8. Постановление Правительства Кыргызской Республики «Об утверждении Положения о правилах написания и применения единиц величин в Кыргызской Республике» от 6 марта 2013 года N 119;
9. Постановление Правительства Кыргызской Республики «О межведомственной комиссии по рассмотрению вопросов административно-территориального устройства и географических названий при Кабинете Министров Кыргызской Республики» от 19 августа 2008 года N 467;
10. Постановление Правительства Кыргызской Республики «Об установлении единой государственной системы координат (Kyrg-06)» от 7 октября 2010 года № 235;
11. Распоряжение Кабинета министров Кыргызской Республики от 12 января 2022 года №2-р утвержден План мероприятий по цифровизации управления и развития цифровой инфраструктуры в Кыргызской Республике на 2022-2023 годы.

№	Описание недостатка	Тип[23]	Лучшая практика
9.1	Закон Кыргызской Республики «О геодезии и картографии» является устаревшим и не удовлетворяет существующие потребности по обеспечению правового регулирования пространственных данных. Закон не содержит достаточных условий для создания и развития национальной инфраструктуры	**У**	Законодательство Кореи и ЮАР содержат комплексный подход к правовому регулированию создания и развития НИПД. В этих странах законодательно закреплены понятия НИППД, метаданных, прав и обязанности субъектов НИПД, полномочия координирующего органа по НИПД. В законодательстве этих стран достаточно подробно описаны вопросы стандартов пространственных данных, сбора, хранения, защиты, учета пространственных данных, требования к базам данных. В части развития НИПД законодательство Республики Корея предусматривает вопросы ведения анализа потребностей заинтересованных сторон в пространственных данных.
9.2.	Полностью отсутствует понятийный аппарат по вопросам связанным с НИПД	**П**	Общие определения НИПД, метаданных, геопортала и иных терминов содержаться в законодательствах практически всех стран где имеется адекватное регулирование НИПД (США, ЮАР, Корея). Даже в Казахстане и РФ законодательно закреплены базовые понятия. Разрабатываемый проект модельного кодекса СНГ о ИПД содержит наиболее полный перечень терминов и определений и может быть взят за основу при разработке нового нормативного правового регулирования.
9.3	Законодательство Кыргызской Республики не регламентирует вопросы пространственных метаданных	**П**	Закон ЮАР о НИПД от 28 января 2004 года (SPATIAL DATA INFRASTRUCTURE ACT 54 OF 2003) дает определение метаданных и устанавливает общие вопросы их регулирования. Порядок сбора и публикация метаданных закрепляются на уровне подзаконных актов. В Российской Федерации действует ГОСТ Р 52573-2006 «Метаданные»

[23] В таблице приводятся следующие типы недостатков регулирования:
(П) пробел в регулировании (регулирование требуется, но его нет)
(У) устаревшая норма (норма есть, но её нужно менять)
(Н) неработающая норма (норма есть, но в силу описанных причин она не работает)
(Б) действующая норма является необоснованным препятствием для осуществления деятельности

			который устанавливает методологию формирования метаданных и определяет: - базовый набор метаданных, необходимый и достаточный для основных операций, таких как поиск данных, определение соответствия данных выдвигаемым требованиям, доступ к данным и их использование; - обязательные и условные пакеты метаданных, сущности и элементы метаданных; - дополнительные (необязательные) элементы метаданных, позволяющие при необходимости использовать их расширенное описание.
9.4	Отсутствуют принципы создания и развития инфраструктуры пространственных данных	**П**	Проект модельного закона по НИПД в рамках ЕАЭК устанавливает следующие принципы формирования НИПД: -обязательность использования органами государственной власти, органами местного управления и самоуправления и другими субъектами регламентированных систем координат и существующих базовых пространственных данных при создании государственных информационных ресурсов и новых базовых пространственных данных; - подчиненность процессов создания и развития ИПД решению приоритетных задач социально-экономического развития страны, охраны окружающей природной среды, экологической безопасности, государственного управления, обеспечения обороноспособности и национальной безопасности страны; - обязательность координатного описания пространственных объектов при создании государственных информационных ресурсов; актуальность, достоверность, полнота, целостность и установленная точность пространственных данных; - совместимость пространственных данных на основе использования единого банка базовых пространственных данных, регламентированных систем

			координат, единых технических регламентов и стандартов; -приоритетного использования пространственных объектов с координатными данными, имеющими наибольшую установленную точность, полноту описания, достоверность и юридическую значимость; - интероперабельность геосервисов, базовых пространственных данных, их метаданных; гармонизация технических регламентов, национальных стандартов ИПД с соответствующими международными стандартами; - этапность в создании и развитии ИПД как сложной организационно-технической системы, характеризующейся бессрочностью функционирования, развития и постоянного совершенствования на основе комплексного и программного подходов; - открытость и доступность базовых пространственных данных, их метаданных для всех заинтересованных субъектов; -планирование последовательности создания и обновления наборов базовых пространственных данных; -государственная поддержка создания и обновления наборов базовых пространственных данных.
9.5	Вопросы сбора, хранения, обработки, распространения, защиты, пользования пространственными данными никак не регламентированы действующими нормативными правовыми актами Кыргызской Республики	**П**	Законодательство Республики Корея и ЮАР содержат детальные правила и порядок сбора, хранения, публикации пространственных данных. При этом в Корее данный порядок предусматривает функции каждого ответственного органа на каждом этапе процесса сбора, хранения пространственных данных
9.6.	Отсутствует правовое регулирование вопросов стандартизации пространственных данных	**П**	На практике ГУ "Госкартография" при Службе земельных ресурсов при Министерстве сельского хозяйства Кыргызской Республики осуществляются попытки применения единых стандартов, создания единой базы геоданных и обеспечения использования единых стандартов различными субъектами

			при создании пространственных данных. При этом решение данных вопросов требует закрепления нормативных правовых механизмов стандартизации пространственных данных.

Комментарии

Обзор и анализ действующей нормативной правовой базы Кыргызской Республики и анализ практик зарубежных стран показывает, что имеющаяся нормативная правовая база Кыргызской Республики является устаревшей и не удовлетворяет существующие потребности по обеспечению правового регулирования пространственных данных. Многие развитые страны начали создавать и развивать свои национальные инфраструктуры пространственных данных (НИПД) около 20 лет назад и более в Кыргызской Республике был принят в 2002 году Закон «О геодезии и картографии», который если сравнивать с нормативными правовыми актами Республики Корея, США и ЮАР выглядел уже тогда весьма архаичным и не имел даже намека на внедрении и применение новых технологий в сфере геодезии и картографии. Более того, данный Закон не содержит достаточных условий для создания и развития национальной инфраструктуры пространственных данных тем самым ставит под угрозу реализацию положений национальных стратегических документов. Указанный Закон, являющийся основным законом в данной сфере, не соответствует современным трендам развития и требует, как минимум, пересмотра большей части его положений, а возможно потребуется разработка и принятие нового Закона. На подзаконном уровне, попытки обеспечения правового регулирования носят фрагментарный характер. На законодательном уровне элементарно не закреплены понятия пространственных данных, объектов пространственных данных, прстранственных метаданных, не говоря уже о порядках и правилах хранения, обработки, использования, предоставления доступа, обмена данными, обновления, стандартов, защиты пространственных данных.

Исходя из обзора и анализа существующей нормативной праововой базы, в целом создание и развитие НИПД в правовом и институциональном аспекте характеризуется следующими проблемами.

1. В настоящее время отсутствует уполномоченный орган по координации деятельности государственных органов, органов местного самоуправления, коммерческих и научных организаций в области создания и развития НИПД.
2. Действующие нормативные правовые акты недостаточно четко закрепляют полномочия государственных органов, задействованных в создании и развитии пространственных данных.
3. Отсутствуют порядок взаимодействия субъектов пространственных данных;
4. Не регламентированы вопросы обмена пространственными данными, правила и порядок их обновления, доступа к пространственным данным;
5. Отсутствует правовое регулирование вопросов стандартизации пространственных данных.

В этой связи для обеспечения адекватного регулирования создания и развития НИПД требуется существенный пересмотр Закона Кыргызской Республики «О геодезической и картографической деятельности». С учетом необходимого количества изменений возможно потребуется разработка нового проекта Закона о пространственных данных по опыту правового регулирования Республики Корея.

Разработка новых нормативных правовых актов включая подзаконные нормативные правовые акты в первую очередь должна быть направлена на:

- пересмотр понятийного аппарата действующих нормативных правовых актов в сфере геодезической и картографической деятельности;
- внедрение принципов создания и развития НИПД;

- определение организационной структуры НИПД;
- установление и закрепление полномочий и ответственности всех сторон за создание и функционирование НИПД;
- утверждение в установленном порядке регламентов взаимодействия (включая межведомственное взаимодействие) и форматов обмена пространственными данными между разработчиками, правообладателями и пользователями НИПД;
- утверждение в установленном порядке стандартов, регулирующих функционирование НИПД;
- соблюдение прав собственности при создании и пользовании данными НИПД;
- решение вопросов сбора, хранения, обработки, распространения и защиты НИПД;
- установление ответсвенности за нарушение законодательства в сфере НИПД

Раздел 10. Электронное сообщение, запись, документ

Содержание

- правовой режим электронных сообщений
- правовой режим цифровой записи, создание и использование цифровых записей
- электронные документы: правовой режим документов, копий и оригиналов, перенос между носителями и т.п.

Текущее регулирование (действующее законодательство):

1. Гражданский процессуальный кодекс Кыргызской Республики
2. Уголовно-процессуальный кодекс Кыргызской Республики
3. Закон Кыргызской Республики «Об электронном управлении»
4. Закон Кыргызской Республики «Об электронной подписи»
5. Закон Кыргызской Республики «Об инновационной деятельности»
6. Закон Кыргызской Республики «О виртуальных активах»
7. Закон Кыргызской Республики «Об электронной торговле»
8. Закон Кыргызской Республики «Об электрической и почтовой связи»
9. Закон Кыргызской Республики «О биометрической регистрации граждан Кыргызской Республики»
10. Постановление Правительства Кыргызской Республики «О некоторых вопросах, связанных с использованием электронной подписи» от 31 декабря 2019 года № 742
11. Постановление Правительства Кыргызской Республики «Об утверждении Положения о государственной системе электронных сообщений и правилах ее использования» от 31 декабря 2019 года № 745
12. Постановление Правительства Кыргызской Республики «Об утверждении Положения об автоматизированной информационной системе «Государственная система электронного документооборота» от 30 октября 2020 года № 526
13. Постановление Правительства Кыргызской Республики «О Типовой инструкции по делопроизводству в Кыргызской Республике от 3 марта 2020 года № 120

Краткое описание выявленных недостатков и ориентиров из мировой практики

№	Описание недостатка	Тип[24]	Лучшая практика
10.1	Действующее законодательство Кыргызской Республики (законы КР «Об электронной подписи», «Об электронном управлении») являются устаревшими, поскольку регулируют электронный документооборот в сфере управления как вспомогательный, альтернативный по отношению к бумажному либо содержат существенные переходные механизмы, позволяющие сохранять бумажный документооборот там, где в этом нет необходимости. Вместо этого в законодательстве необходимо закрепить механизмы,	**У**	В законодательстве США уже более 20 лет предусматривается полное устранение бумажного документооборота на основании Закона об устранении правительственного бумажного документооборота (GPEA). Он требует, чтобы, когда это практически осуществимо, федеральные агентства использовали электронные формы, электронную регистрацию и электронные подписи для ведения официальных дел с общественностью. Закон установил, чтобы агентства к 21 октября 2003 года разрешили

[24] В таблице приводятся следующие типы недостатков регулирования:
(П) пробел в регулировании (регулирование требуется, но его нет)
(У) устаревшая норма (норма есть, но её нужно менять)
(Н) неработающая норма (норма есть, но в силу описанных причин она не работает)
(Б) действующая норма является необоснованным препятствием для осуществления деятельности

	стимулирующие переходить на исключительно цифровое взаимодействие в различных сферах и предусматривающие устранение бумажного документооборота		физическим или юридическим лицам, имеющим дело с агентствами, предоставлять информацию или заключать сделки с агентством в электронном виде, когда это практически осуществимо, и вести записи в электронном виде, когда это практически осуществимо. В Законе конкретно говорится, что электронным записям и связанным с ними электронным подписям не должно быть отказано в юридической силе, действительности или исковой силе только потому, что они представлены в электронной форме, и поощряется использование федеральным правительством ряда альтернатив подписи.
10.2	В Кыргызской Республике полноценно не развернута инфраструктура электронных подписей или иных, более современных способов управления идентичностью, а применимые стандарты являются коммерческими, и разрабатываются Российской Федерацией и Республикой Казахстан, что ставит внутренний рынок Кыргызской Республики в зависимое положение. Необходимо внедрение на национальном уровне требований, правил и стандартов по генерации электронных подписей в соответствии с международными требованиями, одновременно с принятием единых требований к сертификатам электронных подписей на уровне Евразийского экономического союза	**Н**	Наиболее актуальная практика на мировом уровне обобщена и представлена в виде юридического текста в Проекте типового закона ЮНСИТРАЛ об использовании и трансграничном признании управления идентификационными данными и удостоверительных услуг, и Руководства по имплементации данного Типового закона. Несмотря на разнообразие видов электронных подписей и правовых моделей, опосредующих их использование, подходы к правовому регулированию использования электронных подписей можно систематизировать, разбив на три типа. Первый подход — «минималистский» — направлен на признание правового значения электронных подписей и электронных документов и создание правовых условий для их использования путем устранения из существующего законодательства норм, препятствующих использованию электронных подписей. Новые правовые механизмы при этом не создаются; исключение составляет только массив норм, закрепляющих «технологическую нейтральность», т.е. отсутствие привязки законодательства к какой-либо из

			технологий формирования электронных подписей. Подобный подход реализуется, например, в США на основании E-SIGN Act 2000. Второй подход основывается на признании по преимуществу только электронных цифровых подписей; таким образом, он привязывается к одной технологии — технологии открытого ключа. Электронные цифровые подписи и подписанные ими документы признаются законодательством, однако к ним устанавливаются особые требования, отличные от требований к «бумажным» документам и собственноручным подписям. Использование электронных цифровых подписей подчинено «инфраструктуре открытых ключей», которую образуют удостоверяющие центры, выступающие посредниками между обладателями цифровых подписей и получателями заверенных подписями документов. Третий подход представляет собой гибрид первых двух. С одной стороны, он не оставляет за рамками регулирования большую часть электронных подписей, как это происходит при реализации второго подхода. Законодательством признаются все виды электронных подписей, как уже используемых, так и могущих возникнуть в будущем. С другой стороны, законодательство гарантирует определенный уровень надежности документов, подписанных электронными подписями, путем выделения «усиленных» электронных подписей; как правило, усиленными считаются подписи, использующие технологию открытого ключа
10.3	Органы судебной системы в настоящее время не признают цифровые доказательства в судебных разбирательствах из-за отсутствия компетенций и непонимания цифрового законодательства	**H**	В Великобритании и США всё делопроизводство в судах электронное в своей основе, что, помимо удобства и скорости работы с документами, позволяет всем участникам дела, включая судью, получить доступ к одному и тому же набору доказательств, существующему в электронном виде.

			Это не только снижает коррупционные риски, но и практически устраняет возможность любой дискриминации при доступе к правосудию
10.4	Отсутствует порядок хранения электронных документов, записей (информации) в цифровой форме, законодательство о цифровом (электронном) архиве	**П**	В **Эстонии** проблемы долговременного хранения документов, изначально созданных в электронном виде, начинают решаться на уровне ведомства (организации). С этой целью создана специальная компьютерная программа Универсальный модуль архивирования (Universal Archiving Module, UAM), доступная на сайте Национального архива Эстонии, предназначенная для архивистов организации и позволяющая осуществлять экспорт данных из системы управления электронными документами (СУЭД) в архив организации. Основные функции UAM отвечают всем техническим и архивным требованиям успешной подготовки документов и их метаданных для передачи из учреждения в государственный архив. UAM по своей сути всего лишь промежуточное устройство, необходимое в период между экспортом документов из СУЭД до их размещения на постоянное место хранения. UAM применяется на практике с 2010 г. для передачи документов в цифровой архив. Национальный архив находится в постоянном контакте со всеми министерствами и помогает им завершить передачу (импорт) документов с помощью UAM. Таким образом, благодаря данному программному модулю реализован единый универсальный инструмент, позволяющий передать электронные документы из сферы оперативного управления в государственный архив.

Комментарии

Базовые комментарии относительно развития современных концепций цифрового взаимодействия и перехода от электронного документооборота к управлению, основанному на данных, представленных в качестве записей в информационных системах, и информационных ресурсах как базовых источниках информации, представлены

применительно к Разделу 3 настоящего анализа. В настоящем разделе рассмотрены недостатки законодательства, связанные с использованием электронных документов и переходом к электронному документообороту.

Действующее законодательство Кыргызской Республики (законы КР «Об электронной подписи», «Об электронном управлении») являются устаревшими, поскольку регулируют электронный документооборот в сфере управления как вспомогательный, альтернативный по отношению к бумажному либо содержат существенные переходные механизмы, позволяющие сохранять бумажный документооборот там, где в этом нет необходимости. Вместо этого в законодательстве необходимо закрепить механизмы, стимулирующие переходить на исключительно цифровое взаимодействие в различных сферах и предусматривающие устранение бумажного документооборота. В мире уже почти 20 лет ориентиром в данной сфере является Закон США об устранении правительственного бумажного документооборота (GPEA), который требует, чтобы, когда это практически осуществимо, федеральные агентства перешли на электронные формы, электронную регистрацию и электронные подписи для ведения официальных дел с общественностью к 2003 году. Закон требует, чтобы агентства разрешили физическим или юридическим лицам, имеющим дело с агентствами, предоставлять информацию или заключать сделки с агентством в электронном виде, когда это практически осуществимо, и вести записи в электронном виде, когда это практически осуществимо. В Законе конкретно говорится, что электронным записям и связанным с ними электронным подписям не должно быть отказано в юридической силе, действительности или исковой силе только потому, что они представлены в электронной форме, и поощряется использование федеральным правительством ряда альтернатив подписи.

Закон направлен на то, чтобы "помешать агентствам или судам систематически относиться к электронным документам и подписям менее благосклонно, чем к их бумажным аналогам", чтобы граждане могли взаимодействовать с федеральным правительством в электронном виде. В Законе также рассматривается вопрос о том, могут ли частные работодатели использовать электронные средства для хранения и передачи в федеральные агентства информации, касающейся их сотрудников. GPEA заявляет, что электронным записям и связанным с ними электронным подписям не следует отказывать в юридической силе, действительности или исковой силе только потому, что они представлены в электронной форме. Он также поощряет использование федеральным правительством целого ряда альтернатив подписи.

Закон является технологически нейтральным, что означает, что закон не требует от правительства использовать одну технологию вместо другой. Такой подход имеет как преимущества, так и недостатки. Оставаясь нейтральным, это позволяет каждому правительственному учреждению решать, какая технология соответствует его конкретным потребностям. Это также означает, что правительство не ограничивается использованием старых технологий, поскольку становятся доступными новые и более совершенные системы. В качестве недостатка некоторые могут спорить о том, какой метод захвата подписи является лучшим, и такие разногласия могут замедлить процесс внедрения.

Несмотря на разнообразие видов электронных подписей и правовых моделей, опосредующих их использование, **подходы к правовому регулированию использования электронных подписей** можно систематизировать, разбив на три типа[25].

Первый подход — «минималистский» — направлен на признание правового значения электронных подписей и электронных документов и создание правовых условий для их использования путем устранения из существующего законодательства норм, препятствующих использованию электронных подписей. Новые правовые механизмы при этом не создаются; исключение составляет только массив норм, закрепляющих «технологическую нейтральность», т.е. отсутствие привязки законодательства к какой-либо из технологий

[25] См.: Spyrelli, Christina. Electronic Signatures: A Transatlantic Bridge? An EU and US Legal Approach Towards Electronic Authentication // The Journal of Information, Law and Technology (JILT) 2002(2).

формирования электронных подписей. Подобный подход реализуется, например, в США на основании *E-SIGN Act 2000*[26].

Второй подход основывается на признании по преимуществу только электронных цифровых подписей; таким образом, он привязывается к одной технологии — технологии открытого ключа. Электронные цифровые подписи и подписанные ими документы признаются законодательством, однако к ним устанавливаются особые требования, отличные от требований к «бумажным» документам и собственноручным подписям. Использование электронных цифровых подписей подчинено особому механизму, так называемой «инфраструктуре открытых ключей», которую образуют удостоверяющие центры, выступающие посредниками между обладателями цифровых подписей и получателями заверенных подписями документов. В обязанности таких центров входит выдача ключей цифровых подписей, ведение реестра этих ключей и аутентификация (подтверждение соответствия) заверенных подписями документов. К *удостоверяющим* центрам устанавливаются определенные требования, включающие, как правило, минимальные финансовые гарантии возмещения ущерба в тех случаях, когда такой ущерб возник по вине сбоя в его работе (несвоевременной либо ошибочной аутентификации подписи).

Третий подход, назовем его «двухуровневым», представляет собой гибрид первых двух. С одной стороны, он не оставляет за рамками регулирования большую часть электронных подписей, как это происходит при реализации второго подхода. Законодательством признаются все виды электронных подписей, как уже используемых, так и могущих возникнуть в будущем. С другой стороны, законодательство гарантирует определенный уровень надежности документов, подписанных электронными подписями, путем выделения «усиленных» электронных подписей; как правило, усиленными считаются подписи, использующие технологию открытого ключа. Требование об использовании именно усиленных электронных подписей устанавливается применительно к некоторым разновидностям правоотношений, требующих большей, чем обычно, формальности (взаимоотношения с государственными органами, внешнеторговые сделки и некоторые другие). Данный подход позволяет, с одной стороны, создать более универсальную законодательную модель, способную адаптироваться к тем изменениям в технологиях формирования подписей, которые могут произойти в будущем, с другой — позволяет гарантировать необходимую надежность документов, заверенных электронной подписью, в случаях, когда это достаточно важно. Двухуровневый подход предусмотрен в ряде актов международного уровня, таких как *MLES*[27] и Регламент *eIDAS*[28].

Из трех описанных выше подходов наиболее эффективным с точки зрения идентификации и аутентификации в международном обороте признается «минималистский»: хотя он и не предоставляет, в отличие от двух других, сколько-нибудь серьезных гарантий надежности и достоверности подписанных электронной подписью документов, он в то же время и не ограничивает признание самых различных электронных подписей, сформированных в рамках разных национальных моделей правового регулирования использования электронных подписей. Поскольку данный подход основывается больше на функциях электронных подписей, нежели на технологиях их формирования, а также на методах воплощения этих функций в конкретные технологии обмена информацией, он позволяет достичь значительных успехов и в сфере гармонизации законодательства разных стран, касающегося использования электронных подписей[29].

Еще в 1990-е годы в ЕС было принято две директивы, регулирующих вопросы применения электронных подписей: 1999/93/ЕС об электронных подписях и 2000/31/ЕС об электронной коммерции. Директива по электронным подписям по содержанию во многом напоминает *MLES*, однако структура их несколько отличается. Если в *MLES* основное

[26] Закон США об электронных подписях в глобальной и национальной торговле (Electronic Signatures in Global and National Commerce Act 2000).

[27] Типовой закон ЮНСИТРАЛ об электронных подписях 2001 г. // https://base.garant.ru/2567278/.

[28] Regulation (EU) № 910/2014 of the European Parliament and of the Council.

[29] См.: Spyrelli, Christina. Op. cit. P. 7.

внимание обращается на проблемы действительности подписи и права и обязанности сторон, то Директива стремится прежде всего создать организационный аппарат по работе с электронными подписями, и установить рамки для его работы. В 2014 г. структура регулирования электронных подписей в ЕС была изменена и вместо директив был принят регламент *(eIDAS)*, охватывающий помимо электронных подписей иные сервисы идентификации и доверенные сервисы. Регламент *eIDAS*, в свою очередь, является одним из элементов стратегии Цифрового единого рынка ЕС *(Digital Single Market)*. Поэтому главным принципом регулирования, обозначенным в самом его начале (ст. 4) является принцип внутреннего рынка. В соответствии с ним должно разрешаться свободное обращение на внутреннем рынке продуктов и удостоверяющих сервисов, соответствующих требованиям Регламента, и не должно быть никаких ограничений для предоставления удостоверительных сервисов на территории одного государства — члена ЕС поставщиком удостоверяющих сервисов, учрежденным в другом государстве — члене ЕС.

В отношении электронных подписей в Регламенте реализован двухуровневый подход. Любая электронная подпись не может считаться не имеющей юридических последствий или признаваться недопустимым доказательством в судебном разбирательстве только на том основании, что она имеет электронную форму или не соответствует требованиям квалифицированной подписи. В то же время только квалифицированная электронная подпись имеет такие же юридические последствия, что и собственноручная подпись. Квалифицированная электронная подпись, основанная на квалифицированном сертификате, который был выдан в одном государстве — члене ЕС, признается квалифицированной электронной подписью во всех государствах — членах ЕС.

Усиленная электронная подпись, согласно Регламенту, должна соответствовать следующим требованиям:

(a) быть уникальным образом связана с подписантом;

(b) давать возможность идентифицировать подписанта;

(c) должна быть создана с использованием данных создания электронной подписи, которые подписант с высоким уровнем уверенности использует под единоличным контролем;

(d) должна быть связана с данными, в отношении которых она проставляется, таким образом, чтобы изменение таких данных после проставления подписи можно было обнаружить.

Процесс проверки подлинности электронной подписи должен подтверждать действительность электронной подписи при условии, что:

(a) сертификат, на основании которого используется подпись, является на момент подписания квалифицированным сертификатом для электронной подписи и соответствует предъявляемым требованиям;

(b) квалифицированный сертификат был выдан квалифицированным поставщиком удостоверяющих сервисов и являлся действительным на момент подписания;

(c) данные проверки подлинности подписи совпадают с данными, предоставленными полагающейся стороне;

(d) уникальный набор данных, характеризующих подписанта в сертификате, был корректно представлен полагающейся стороне;

(e) полагающейся стороне однозначно сообщается об использовании псевдонима, если во время подписания использовался какой-либо псевдоним;

(f) электронная подпись была создана специальным программно-аппаратным комплексом создания квалифицированных электронных подписей;

(g) целостность данных, заверенных подписью, не была скомпрометирована;

(h) система, использующаяся для проверки электронной подписи, должна предоставлять полагающейся стороне корректные результаты процесса проверки, а также позволять полагающейся стороне выявлять любые важные для информационной безопасности аспекты.

Если сравнить два документа двух международных организаций — *MLES UNCITRAL* и Регламент *eIDAS* ЕС, можно обнаружить разницу в подходах к регулированию электронной

подписи. Они одинаково определяют понятие электронной подписи, создают одинаковую структуру правоотношений «отправитель — получатель — удостоверяющий центр». Но при этом подход Регламента более точный и более жесткий. Устанавливаются права, обязанности, ответственность сторон, критерии признания подписи обретают характер замкнутого перечня, делается упор на сертификацию. Это ведет к унификации внутри Сообщества, но осложняет взаимодействие с другими государствами. Приняв сначала директиву об использовании электронных подписей, а потом и регламент о сервисах идентификации, ЕС не смог решить задачу включения своего информационно-правового пространства в общемировое. Согласно ст. 14 Регламента сервисы идентификации, получаемые из третьей страны, признаются только в соответствии с международным договором между ЕС и такой третьей страной или международной организацией.

В Соединенных Штатах на федеральном уровне было принято два документа. Первым стал Модельный закон об электронных сделках *(Uniform Electronic Transactions Act,* 1999 — *UETA).* Вторым — Акт о применении электронных подписей в международной и внутренней коммерции *(Electronic Signatures in Global and National Commerce Act,* 2000 — *E-sign Act)*[30]. Они стали базой для законов об электронных подписях, принятых в настоящее время в 49 штатах.

UETA изначально создавался не как кодекс, т.е. некий всеобъемлющий акт, касающийся всех возможных случаев применения электронных подписей, а как модель закона, приспосабливающего существующее законодательство к новому виду деятельности. В официальном комментарии к *UETA* это особо подчеркивается: «…Целью *UETA* является преодоление существующих препятствий для электронной коммерции путем придания юридической силы электронным документам и электронным подписям. *UETA* не является статутом, кодифицирующим договорное право — основные нормы договорного права остаются неизменными. Также это не статут об электронных цифровых подписях. *UETA* призван лишь дополнять и поддерживать то законодательство об ЭЦП, которое уже есть в штатах».

Акт также не уделяет особого внимания технической стороне вопроса. Определение электронной подписи здесь охватывает собой фактически любой способ подписания (ЭЦП, отпечаток пальца, сканирование сетчатки глаз, образец голоса), главное — намерение лица, совершающего подпись, подписать документ — в том смысле, в котором это употребляется в бумажном документообороте. В акте нет упоминания и про обязательную сертификацию подписей, это вопрос *bona fide* сторон либо экспертизы в рамках судебного разбирательства.

В целом, согласно *UETA*, электронным документам и электронным подписям (в основном в коммерческом обороте, так как это составляет основной предмет регулирования Акта) будет придано юридическое значение, аналогичное бумажным документам («форма представления договора, иного документа или подписи — электронная или бумажная — сама по себе не влечет различий в его юридическом признании»). Акт, впрочем, устанавливает ряд исключений из этого правила, это, например, сделки с недвижимостью, траст, завещания. Перечень исключений, предлагаемых актом, не очень четкий, но вполне очевидный; в различных штатах он не очень сильно отличается.

*E-Sign Act урегулировал в*опрос электронных подписей непосредственно на федеральном уровне. Он повторяет правило *UETA* о равном признании электронной и бумажной подписи, электронного и бумажного документа. При этом особо подчеркивается, что подписанный документ может повлечь как положительные, так и отрицательные последствия, например, в случае мошенничества, подписания без законных на то полномочий, а также в других случаях, предусмотренных гражданским законодательством (нормы о пороках воли и волеизъявления).

E-Sign Act рассматривает также некоторые специальные случаи использования электронных подписей. Например, электронная подпись может быть нотариально заверена (тоже электронным путем). Сфера применения электронных подписей ограничивается в вопросах наследования, семейного права, вынесения судебных решений, иных отношений

[30] Тексты доступны на http://www.law.upenn.edu/bll/ulc/ulc_final.htm

с участием государственных органов, а также при передаче предметов, опасных для жизни и здоровья людей. Особое внимание уделяется применению электронных подписей в отношениях с участием потребителей: здесь оговаривается право потребителей на получение всей необходимой информации, связанной с использованием электронной подписи, рассматривается возможность потребителя отозвать свою подпись и последствия такого отзыва.

В акте реализован «минималистский» подход к признанию иностранных электронных подписей. Положение п. (1) ст. 301 раздела «Содействие международной электронной коммерции», где содержится своего рода преамбула ко всему разделу, возлагает на федерального министра торговли (который является государственным органом, ответственным за реализацию *E-Sign Act)* обязанность «предпринимать все меры… необходимые для устранения или сокращения в максимально возможной степени препятствий торговле при использовании электронных подписей в целях облегчения развития торговли между штатами и внешней торговли».

В целях максимального устранения всех препятствий на пути международной торговли механизм признания иностранных подписей включает в себя всего несколько принципов.

(A) *A.* «Устранение зависящих от использования бумажного документа препятствий для электронных сделок путем утверждения соответствующих принципов *MLEC* 1996 г.». Принцип направлен на устранение препятствий к использованию электронных документов, основанных только на том, что такие документы не были выполнены в «бумажном» виде, и в полной мере реализован в самом *E-Sign Act*.

(B) *B.* «Разрешение сторонам сделки устанавливать приемлемые технологии подтверждения подлинности в своих сделках с гарантией того, что такие технологии и модели применения будут признаваться и подлежать принудительному обеспечению». Принцип воплощает общие условия *диспозитивности* (свободы сторон по собственному усмотрению определять технологии, которые будут использоваться в качестве электронной подписи, определять модели использования электронных подписей) и *правовой защиты* (трансакции, совершенные на основании соглашения сторон об использовании электронных подписей, наделяются полной юридической силой, как если бы они были совершены в «бумажном» виде). Однако стоит еще раз отметить, что использование электронных подписей на основании соглашения сторон таит в себе определенные проблемы.

(C) *C.* «Разрешение сторонам сделки иметь возможность доказывать в суде или при ином производстве, что их подходы к подтверждению подлинности и их сделки являются действительными». Этот принцип фактически содержит в себе указание на возможность обращения в суд в целях подтверждения действительности соглашения об использовании электронных подписей и действительности заключенных на его основе сделок. Хотя материальных норм, касающихся признания таких сделок действительными, *E-Sign Act* не устанавливает, процессуальные гарантии являются крайне важными: они позволяют преодолеть трудности с заключением соглашения об использовании электронных подписей, о котором говорилось в предыдущем пункте.

D. «Принятие недискриминационного подхода к электронным подписям и способам подтверждения подлинности в других юрисдикциях». Несмотря на неопределенность и возможность двоякого толкования данного положения, оно (даже в самом общем виде) принципиально важно: иностранные подписи в США должны признаваться наравне с подписями, сформированными в США. Следовательно, это позволяет распространить на иностранные подписи все те требования, касающиеся действительности электронных подписей, которые установлены *E-Sign Act* для национальных электронных подписей.

Подобный «минималистский» подход к признанию электронных подписей является следствием «минималистского» подхода к регулированию использования электронных

подписей в целом. В целом же законодательства США и ЕС демонстрируют два разных подхода к международно-правовым аспектам идентификации на основе электронных подписей. Первый предполагает автоматическое признание иностранных электронных подписей, если они соответствуют условиям действительности подписей, установленным в национальном законодательстве. В рамках второго подхода необходимо, чтобы подпись или ее сертификат были гарантированы в рамках национальной правовой системы государства, где требуется признание подписи прежде всего на основании соответствующего международного договора.

Вопросы признания и использования электронных документов и электронных записей имеют значение с точки зрения доказывания в суде. В США система подачи обращений "Управление делами / Электронный Архив дел" (Case Management / Electronic Case Files - CM/ECF) оказалась очень успешной и уже в 2005 году она была внедрена во все федеральные суды страны. С того времени система постоянно совершенствуется и активно используется, поскольку в США установлена обязанность сторон подавать документы в электронном виде с помощью CM/ECF. Сегодня в США подача документов в суд в бумажном виде осуществляется в виде исключения в случае особой необходимости. Тогда стороне следует писать заявление "О несоблюдении обязательства подачи документа в электронной форме". Чтобы помочь пользователям в работе с системой, в каждом суде доступно обучение.

Система "Управление делами / Электронный Архив дел" позволяет судам принимать заявления и предоставляет доступ к поданным документам онлайн. Чтобы подать документы в суд в системе CM/ECF, необходимы логин и пароль, выданные соответствующим судом. Электронные документы с помощью системы CM/ECF подаются только в формате PDF. Таким образом, система "Управление делами / Электронный Архив дел" (CM/ECF) обеспечивает поступление документов в электронном виде, а Система открытого доступа к судебным документам в электронном виде (PACER) обеспечивает предоставление публичного доступа к судебным материалам. Управление обеими системами осуществляется, однако доступ к файлам дел осуществляется централизованно через общую систему доступа.

В федеральных судах США вопросы представления доказательств регулируются отдельным правовым актом - "Федеральными правилами о доказательствах" (Federal Rules of Evidence). В декабре 2017 года в Федеральные правила о доказательствах были внесены изменения, упрощающие проверку подлинности данных из электронных источников. Изменения описывают процесс аутентификации предоставляемых документов, таких как распечатка с интернет-страницы или документ, извлеченный из файлов, хранящихся на персональном компьютере. Они также предусматривают использование процесса цифровой идентификации (хэш-значения) для аутентификации подлинности электронных данных.

В Великобритании также активно внедряются элементы электронного правосудия. Основными направлениями реформирования судебной системы Великобритании являются:

- переход к электронному документообороту на всех этапах судопроизводства, в том числе формирование информации о судебном деле в электронном виде;

- рассмотрение в режиме онлайн мелких административных правонарушений и уголовно-наказуемых деяний невысокой степени общественной опасности, наказание за которые не предусматривает лишения свободы, а также гражданских споров (с ценой иска до 25 тысяч фунтов);

- рассмотрение большинства гражданских споров с помощью удаленного интернет-доступа к суду к 2022 году.

В Великобритании электронная подача документов, а также публичный доступ к электронному судебному делу возможны с помощью Программы электронного документооборота (Electronic Working Pilot Scheme). Система действует в специализированных судах отделения Королевской скамьи и Канцлерского отделения Высокого суда.

С 2017 года исковые заявления в специализированные подразделения Высокого суда Англии и Уэльса, рассматривающие споры с участием предпринимателей, подаются исключительно в электронном виде с помощью Системы судебных электронных дел (Courts

Electronic Filing system - CE-File). Помимо этого, существует интернет-портал CaseLines, с помощью которого можно подавать исковые заявления, жалобы и доказательства в электронном виде, а также функционирует Онлайн суд Ее Величества (Her Majesty's Online Court - HMOC), который позволяет рассматривать дела в режиме онлайн.

Одной из основных проблем перевода в настоящее время становится законодательство в сфере архива, где предусматривается хранение документов, которые подходят хранению бумажных документов. Отсутствует порядок хранения электронных документов и электронной информации.

В Стратегическом плане Национального архива **США (НАРА)** на период 2014–2018 гг. прием, хранение электронных документов и обеспечение их доступности рассматриваются как один из вызовов современной цифровой эпохи, как одно из основных условий успешной деятельности архива. Проблема управления документами и государственного делопроизводства в целом была в очередной раз поднята на высшем государственном уровне в США в 2011 г., когда был издан специальный Меморандум «Управление государственными документами», выдвинувший задачу всем федеральным агентствам к 2019 г. перейти в максимальной степени на электронный документооборот, в том числе и для документов с постоянным сроком хранения. Для этого НАРА необходимо пересмотреть свое руководство по передаче на архивное хранение электронных документов постоянного срока хранения и регулярно обновлять требования к его реализации. Сегодня национальный архив США содержит около семисот терабайт (Тб) электронных документов, из которых за время президентского срока Буша было получено 79 Тб, а за время Обамы – 250 Тб, что свидетельствует о значительной интенсификации процесса передачи в архив электронных документов.

В **Великобритании** для реализации задач хранения электронных документов разработан стратегический план «Архивы вдохновляют: планы и приоритеты Национального архива Великобритании на 2015–2019 гг.». План состоит из пяти основных направлений, первое из которых посвящено проведению экспертной оценки документов и исследований, необходимых для ведения и совершенствования делопроизводства в правительственных учреждениях. В январе 2017 г. Национальные архивы Великобритании опубликовали свою новую «Электронную стратегию», где обозначили цель стать инновационным электронным архивом, фундаментально переосмысливающим архивную практику, начиная с основополагающих принципов. Такой архив должен обеспечить долговременную сохранность созданных государственными органами электронных документов любых видов, а не только тех, что были созданы в нескольких широко распространенных форматах.

На идеологию этого плана повлияла модель континуума документов, рассматривающая их как архивные с момента создания. Именно поэтому Национальный архив Великобритании позиционирует себя активным участником обсуждения новых информационных систем, чтобы о проблемах сохранности электронных документов начинали задумываться как можно раньше.

Вопросами передачи на постоянное хранение электронных документов занимаются и **в Евросоюзе**. Проект E-ARK (European Archival Records and Knowledge Preservation) разработан и финансируется Европейской комиссией в рамках Программы поддержки информационных и коммуникационных технологий, включенной в Программу по конкурентоспособности и инновациям. Цель проекта – обеспечение эффективного делопроизводства, связанного с тремя основными видами архивной деятельности, а именно – комплектованием, хранением и возможностью повторного использования архивной информации. Проект E-ARK – это трехлетняя многонациональная научно- исследовательская работа, осуществление которой запланировано на период с 1 февраля 2014 г. по 31 января 2017 г. Помимо архивов в него вошли университеты, министерства, фонды, государственные учреждения.

Приоритетной задачей проекта является создание общеевропейской методологии архивного хранения электронных документов на основе существующей национальной и международной практики в области обеспечения подлинности и возможности повторного использования цифровых материалов в течение длительного периода времени.

Помимо указанного проекта отдельные европейские государства достаточно эффективно реализуют задачи архивного хранения электронных документов. Причем наиболее активно в этом участвуют страны Северной Европы.

В **Эстонии** проблемы долговременного хранения документов, изначально созданных в электронном виде, начинают решаться на уровне ведомства (организации). С этой целью создана специальная компьютерная программа Универсальный модуль архивирования (Universal Archiving Module, UAM), доступная на сайте Национального архива Эстонии, предназначенная для архивистов организации и позволяющая осуществлять экспорт данных из системы управления электронными документами (СУЭД) в архив организации. Основные функции UAM отвечают всем техническим и архивным требованиям успешной подготовки документов и их метаданных для передачи из учреждения в государственный архив. UAM по своей сути всего лишь промежуточное устройство, необходимое в период между экспортом документов из СУЭД до их размещения на постоянное место хранения.

UAM применяется на практике с 2010 г. для передачи документов в цифровой архив. Национальный архив находится в постоянном контакте со всеми министерствами и помогает им завершить передачу (импорт) документов с помощью UAM. Таким образом, благодаря данному программному модулю реализован единый универсальный инструмент, позволяющий передать электронные документы из сферы оперативного управления в государственный архив.

В **Нидерландах** с 2013 г. проводится работа по созданию единого национального хранилища электронных документов. К этому периоду была сформирована его концепция, регламентированы необходимые процессы, создана информационная архитектура, сконструирована модель метаданных для всех государственных структур, являющихся источниками комплектования голландских архивов и др. Одновременно, Национальный архив разработал прототип цифрового хранилища для документов центрального правительства, которое соответствует модели построения систем хранения данных в электронной форме OAIS (Open Archival Information System). В 2014–2016 гг. удалось создать необходимую инфраструктуру, а в 2017 г. планировалось передать в хранилище все оцифрованные и изначально созданные в электронном виде документы.

В связи с этим архивы Нидерландов начали реализацию пилотных проектов по приему документов из систем электронного документооборота органов власти и управления. Голландский закон «Об официальных документах» (Public Records Act) предписывает передачу в архив правительственных документов постоянного хранения через 20 лет после создания, однако национальное электронное хранилище позволяет принимать документы и до истечения этого срока.

В **Финляндии** Службой Национального архива разработаны стандарты для финских систем управления электронными документами (известны как Sähke, Sähke2), определяющие метаданные и функции, необходимые для работы в этих системах. Требования Sähke были впервые опубликованы в 2005 г. и усовершенствованы в 2008 г. Если государственные и муниципальные учреждения пожелают оставить документы постоянного срока хранения только в электронной форме, то им следует выполнить требования, предусмотренные Sähke, получить разрешение Службы Национального архива на хранение документов в электронном виде. Кроме того, в стандарте также уточняются способы передачи электронных документов на постоянное хранение из учреждения в Национальный архив.

В последние годы Национальный архив Финляндии получил на хранение базы данных и реестры из различных государственных органов. Основная стратегия Национальных архивов предусматривает сохранение только данных, а не функциональных возможностей, правил обработки данных или алгоритмов. Данные извлекаются из системы управления базами данных (СУБД) и отделяются от структур базы данных. Национальные архивы не устанавливают строгих правил в отношении форматов файлов данных. Вместо этого ключевые требования связаны с обязательными элементами метаданных. Описание данных и их передача в Национальные архивы осуществляются с помощью стандартизированных структур сдаточных информационных ZIP-папок и метаданных. Дополнительная

документация, касающаяся контекста, происхождения данных, системы управления базами данных (СУБД), моделей данных, правил обработки и рекомендаций по удобству использования, также сохраняется в формате PDF. Вопрос о том, какую документацию следует включать в ZIP-папку, решается для каждого случая отдельно.

Национальные архивы разработали в рамках Sähke2 структуру ZIP-папок с целью обеспечить передачу в единой структуре документов из различных электронных систем управления документами в свою службу обеспечения долговременной сохранности. Sähke2-структура также используется при передаче баз данных и данных реестров. Такой подход обеспечивает передачу всех материалов в Национальные архивы Финляндии, в единой структуре с однотипными метаданными.

В **ФРГ** стремительный рост количества электронных документов приводит к тому, что в федеральных организациях на серверах и в системах управления документами находится огромное количество данных, которые активно не используются. Согласно требованиям федеральных организаций, вышедшие из активного употребления документы должны храниться в организации от пяти до тридцати лет. Таким образом, от федеральных организаций требуется обеспечение надежного хранения своих материалов, которые можно будет использовать через 30 лет. В то же время Федеральный архив не в состоянии одновременно обрабатывать такое количество электронных документов и форматов по истечении 30 лет.

По этой причине в ФРГ для федеральных организаций создается Цифровой промежуточный архив. Внеофисное хранение документов, потерявших оперативное значение, освобождает административные системы по управлению электронными документами от вышедших из активного употребления документов и способствует более эффективной работе этой системы. Федеральные организации создают Пакет представления информации (ZIP), включая основные данные в сжатом файле и метаданные в файле на языке XML. Этот пакет посылается через безопасную сеть в Интерфейс доступа цифрового промежуточного архива. Затем Пакет представления информации преобразуется в пакет XAIP и метаданные извлекаются в базу данных для проведения исследований. После проверок и легализации пакет XAIP сохраняется, и федеральная организация получает его идентификацию. В 2015 г. было запланировано начало первой передачи данных и тестирование.

Во **Франции** в 2011 г. был запущен проект межведомственной системы архивного хранения электронных документов VITAM (Valeurs Immatérielles Transférées aux Archives pour Mémoire – Нематериальные ценности, переданные в архивы для сохранения памяти). VITAM нацелен на развитие модульной программной платформы хранения документов в министерствах, адаптированной к их потребностям и специфике. Она будет также служить базой для развития программного обеспечения для постоянного хранения электронных документов в научных целях в Национальном архиве и в архивах министерств обороны и иностранных дел.

В 2015 г. было заметно некоторое торможение в реализации проекта VITAM. В публикациях 2016 г. уже не говорится о создании «суперплатформы для краткосрочного, промежуточного и постоянного хранения электронных архивов центральных учреждений Франции», а лишь о разработке программного обеспечения «электронный архив», которое три пилотных министерства, а затем и другие заинтересованные учреждения смогут использовать. Пилотными министерствами, внедряющими VITAM, являются в настоящее время Министерство культуры (проект AD-Essor), МИД (проект Saphir) и Министерство обороны Франции (проект GardeV2-Archipel).

В **Польше** в рамках достижения цели Улучшение цифровой эффективности учреждений реализуется проект по применению системы EZD (Электронное управление документацией) на уровне государственной администрации – воеводских управлений. В первом квартале 2012 г. были начаты подготовительные работы по пилотному внедрению системы EZD в нескольких учреждениях объединенной администрации двух воеводств. Таким образом, местная государственная администрация оснащается единой и совместно развиваемой системой для электронного управления документацией, что позволит обеспечить

электронное взаимодействие между учреждениями с помощью платформы e-PUAP (электронная Платформа услуг публичной администрации).

Рассматривая решения разных стран в части обеспечения долговременной сохранности электронных документов, можно выявить некоторые общие тенденции, которые, очевидно, могут быть реализованы и в Кыргызской Республике.

Во-первых, для обеспечения хранения электронных документов в соответствии с установленными сроками в информационных системах организаций, где эти документы создаются и/или используются в оперативных целях, должны быть реализованы некоторые функции, позволяющие произвести отбор документов по срокам хранения. А также эти системы должны гарантировать подготовку документов для передачи в информационную систему архива в соответствии с требованиями последнего, т. е. архивные требования закладываются в системы оперативной работы с документами.

Во-вторых, очевидно, необходимо говорить о новом организационном решении долговременного хранения электронных документов. Модель, в соответствии с которой документы из оперативного делопроизводства передаются в архив своей организации, а затем в государственный архив, может оказаться неэффективной. Более целесообразным признается вариант, когда электронные документы из различных организаций (органов власти) передаются в единый архив электронных документов, обладающий соответствующим программно-техническим обеспечением.

В-третьих, практика показывает, что в условиях постоянно совершенствующихся информационных технологий, изменений программно-аппаратной среды и быстрого устаревания всех известных электронных носителей сохранить электронные документы без проведения процедур конвертации и миграции невозможно. Необходимо найти решения для обеспечения их аутентичности, целостности, достоверности и пригодности для использования в условиях долговременного хранения.

Раздел 11. Цифровая идентификация

Содержание

- способы идентификации (коды, токены, подписи, биометрическая идентификация)
- средства идентификации
- системы идентификации

Текущее регулирование (действующее законодательство):

1. Конституционный закон Кыргызской Республики «О выборах Президента Кыргызской Республики и депутатов Жогорку Кенеша Кыргызской Республики» от 2 июля 2011 года № 68 (в части идентификации избирателей).
2. Конституционный закон Кыргызской Республики «О референдуме Кыргызской Республики» от 31 октября 2016 года № 173 (в части идентификации избирателей).
3. Закон Кыргызской Республики «Об электронном управлении» от 19 июля 2017 года № 127 (в части установления правовых основ единой системы идентификации).
4. Закон Кыргызской Республики «Об электронной подписи» от 19 июля 2017 года № 128.
5. Закон Кыргызской Республики «О биометрической регистрации граждан» от 14 июля 2014 года № 136 (в части сбора и обработки биометрических данных).
6. Закон Кыргызской Республики «О виртуальных активах» от 21 января 2022 года № 12 (правовые основы токена как средства удостоверения имущественных и (или) неимущественных прав, в том числе прав требования на другие объекты гражданских прав).
7. Закон Кыргызской Республики «О платежной системе Кыргызской Республики» от 21 января 2015 года № 21 (в части идентификации клиентов).
8. Закон Кыргызской Республики «О противодействии финансированию террористической деятельности и легализации (отмыванию) преступных доходов» от 6 августа 2018 года № 87.
9. Закон Кыргызской Республики «О выборах депутатов местных кенешей» от 14 июля 2011 года № 98 (в части идентификации избирателей).
10. Указ Президента Кыргызской Республики «О неотложных мерах по активизации внедрения цифровых технологий в государственное управление Кыргызской Республики» от 17 декабря 2020 года УП № 64.
11. Постановление Правительства Кыргызской Республики «Об идентификационной карте - паспорте гражданина Кыргызской Республики образца 2017 года (ID-карта)» от 3 апреля 2017 года № 197, в том числе:
    a. Положение об идентификационной карте - паспорте гражданина Кыргызской Республики образца 2017 года (ID-карта) (приложение).
12. Постановление Правительства Кыргызской Республики «О некоторых вопросах, связанных с использованием электронной подписи» от 31 декабря 2019 года № 742.
13. Постановление Правительства Кыргызской Республики «О некоторых вопросах, связанных с государственными информационными системами» от 31 декабря 2019 года № 744, в том числе:
    a. Требования к защите информации, содержащейся в базах данных государственных информационных систем (приложение) (в части идентификации пользователей).
14. Постановление Правительства Кыргызской Республики «Об отдельных вопросах осуществления электронного управления в Кыргызской Республике» от 31 декабря 2019 года № 748, в том числе:

a. Положение о Единой системе идентификации Кыргызской Республики (приложение 1);

b. Требования к реквизитам и форме (формату) представления информации в электронных документах государственных органов, органов местного самоуправления, а также в электронных документах, являющихся обращениями граждан в государственные органы и органы местного самоуправления (приложение 2).

15. Постановление Правления Национального банка Кыргызской Республики «Об утверждении Положения «О минимальных требованиях по предоставлению удаленного/дистанционного обслуживания в Кыргызской Республике» от 15 апреля 2015 года № 22/3, в том числе:
    a. Положение о минимальных требованиях по предоставлению удаленного/дистанционного обслуживания в Кыргызской Республике (приложение).
16. Постановление Правления Национального банка Кыргызской Республики «Об утверждении Положения «О требованиях по обеспечению информационной безопасности в коммерческих банках Кыргызской Республики» от 26 мая 2010 года № 36/7, в том числе:
    a. Положение «Об основных требованиях к деятельности коммерческих банков при заключении агентского договора по предоставлению банковских розничных услуг» (приложение).
17. Постановление Правления Национального банка Кыргызской Республики «Об утверждении Положения «О требованиях по обеспечению информационной безопасности в коммерческих банках Кыргызской Республики» от 22 декабря 2021 года № 2021-П-20/72-8-(НПА), в том числе:
    a. Положение о требованиях по обеспечению информационной безопасности в коммерческих банках Кыргызской Республики (приложение).
18. Постановление Правления Национального банка Кыргызской Республики «Об утверждении Концепции развития цифровых платежных технологий в Кыргызской Республике на 2020-2022 годы» от 27 марта 2020 года № 2020-П-14/17-4-(ПС), в том числе:
    a. Концепция развития цифровых платежных технологий в Кыргызской Республике на 2020-2022 годы (приложение).
19. Постановление Правления Национального банка Кыргызской Республики О порядке идентификации и верификации клиентов в удаленном режиме» от 13 мая 2020 года № 2020-П-12/27-1-(НПА), в том числе:
    a. Порядок идентификации и верификации клиентов в удаленном режиме (приложение).

Краткое описание выявленных недостатков и ориентиров из мировой практики

№	Описание недостатка	Тип[31]	Лучшая практика
11.1	Законодательство, регулирующее использование идентификационной карты – паспорта гражданина (ID-карты), не позволяют широко использовать возможности данного инструмента.	**Н**	В **Европейском союзе** получили распространение идентификационные карты в качестве средства идентификации. Использование электронной идентификационной карты в соответствии с Директивами

[31] В таблице приводятся следующие типы недостатков регулирования:
(П) пробел в регулировании (регулирование требуется, но его нет)
(У) устаревшая норма (норма есть, но её нужно менять)
(Н) неработающая норма (норма есть, но в силу описанных причин она не работает)
(Б) действующая норма является необоснованным препятствием для осуществления деятельности

	В электронном чипе ID-карты содержатся необходимые биометрические данные (цветное изображение лица, графическое строение папиллярных узоров пальцев обеих рук, собственноручная подпись владельца) и ключ ЭЦП. Однако законодательство не содержит правовых возможностей использовать ID-карту для цифровой (электронной) идентификации. Так, например, при идентификации на избирательных участках используются технологии биометрической идентификации, а не ID-карта		2002/21/EC, 2009/140/EC, 2002/20/EC, 2009/140/EC, позволяет реализовать двухфакторный процесс верификации: сначала проверяются данные пользователя, затем для каждого шага в процессе выполнения электронной транзакции требуется простановка цифровой подписи, что гарантирует осознанное, явное подтверждение авторизации на выполнение конкретного действия. Например, в **Великобритании** действует система предоставления государственных услуг на основе системы единой идентификации/аутентификации. В **Голландии** реализована инфраструктура авторизации и делегирования прав (CARF), позволяющая гражданам и юридическим лицам делегировать свои права по выполнению транзакций и получению государственных услуг от своего имени. Идентификация и аутентификация лиц осуществляется при оказании государственных услуг, финансовых услуг, в коммерческих отношениях, в том числе в электронной торговле. В **Сингапуре** всем резидентам выдаётся Национальная регистрационная карта (NRIC), являющаяся обязательным элементом для идентификации и аутентификации пользователей практически для всех государственных, финансовых и телекоммуникационных услуг.
11.2	Законодательные возможности цифровой идентификации ограничены средствами ЭЦП и биометрической идентификацией. Отсутствуют возможности использования иных средств, таких как токены, коды, идентификация по sms, видеоидентификация	**У**	В **Европейском союзе** высоко развито предоставление услуг на основе идентификации пользователей на основе информации, содержащейся в базах данных операторов связи. В **Эстонии** реализована технология Mobil-ID (запись в sim-карту идентификационного приложения ЭЦП). Указанная технология позволяет пользователю идентифицировать себя с

			использованием мобильного телефона без использования считывающего устройства для ID-карты. В **Сингапуре** разработана Национальная платформа для аутентификации, позволяющая осуществлять двухфакторную аутентификацию. Пользователями данной платформы являются государственные органы и учреждения, службы, банки, крупные финансовые учреждения государства. Аутентификация осуществляется по идентификационному номеру, а также посредством направления пароля по sms. Двухфакторная идентификация используется при предоставлении широкого спектра государственных и финансовых услуг. Аутентификация путем отправки sms на номер сингапурского мобильного оператора может использоваться для подтверждения операций с цифровой подписью – для осуществления транзакций, подтверждения документов, заключения договоров и осуществления иных хозяйственных операций. В **Индии** при получении государственных и муниципальных услуг предусмотрена возможность аутентификации с помощью номера телефона и sms. Аутентификация путем отправки sms на номер мобильного оператора может использоваться для подтверждения операций с цифровой подписью – для осуществления транзакций, подтверждения документов, заключения договоров и осуществления иных хозяйственных операций.
11.3	Законодательство возможности цифровой идентификации существенно ограничены сферой государственного управления – предоставлением государственных услуг и участия избирателей в	**П**	В **Сингапуре** идентификация и аутентификация лиц осуществляется при оказании государственных услуг, финансовых услуг, в коммерческих отношениях, в том числе электронной торговле.

	выборах и референдумах. Например, не предусматриваются возможности цифровой идентификации при взаимодействии в рамках электронной коммерции		В **Европейском союзе** к сферам, при взаимодействии в которых предусмотрены правовые возможности цифровой идентификации различными способами, относятся в том числе: банковские услуги, включая осуществление переводов денежных средств по поручению физических лиц без открытия банковских счетов; привлечение денежных средств физических и юридических лиц во вклады; размещение указанных привлеченных средств; совершение юридически значимых действий.
11.4	Законодательное регулирование биометрической идентификации ограничено сферами миграционных и избирательных правоотношений. При этом законодательно предусмотрено, что биометрическая регистрации обязательна для всех граждан Кыргызской Республики, что теоретически предполагает широкие возможности использования биометрических баз данных граждан, в том числе при предоставлении государственных и муниципальных услуг, оказании банковских услугах.	**Н**	В **Соединённых Штатах Америки** сферы использования биометрической идентификации включают в себя: миграционные отношения, порядок въезда и выезда иностранных граждан; правоохранительную деятельность; национальную безопасность, борьбу с терроризмом; коммерческие услуги; здравоохранение, получение медицинских услуг; финансовые отношения, банковский сектор.
11.5	Законодательство, регулирующее правовой статус Единой системы идентификации, не предполагают возможностей её широкого использования непосредственно в целях идентификации, не предполагают подключения к ней коммерческих банков и иных организаций.	**Н**	В **Российской Федерации** законодательно закреплено разрешение доступа к Единой системы идентификации и аутентификации коммерческих организаций, компаний, занимающихся телемедициной, и удостоверяющих центров. Кроме того, широкое распространение и использование получает Единая биометрическая система.

Комментарии

Законодательство Кыргызской Республики и, особенно, подзаконные акты уполномоченных государственных органов содержит значительные предпосылки широкого использования различных инструментов цифровой идентификации. Такая идентификация, позволяющая обеспечить взаимодействие заинтересованных сторон (государства, бизнеса, личности) в удалённом формате, является одной из тенденций развития цифровизации.

При этом регулирование в сфере цифровой идентификации предполагает создание необходимых условий для их применения, в том числе за счёт повышения гибкости в

регулировании, совершенствовании инструментов защиты прав потребителей, а также установление требований по совершенствованию информационной безопасности, защите персональных данных и иных мер.

В то же время, в настоящее время законодательные механизмы, разрешающие удалённую или цифровую идентификацию, направлены в первую очередь на государственный сектор и не раскрывают всех возможностей такой идентификации в коммерческих целях, включая банковские услуги.

Международные принципы законодательного регулирования

В Великобритании действует рекомендательный документ – Принципы подтверждения идентификации содержащий подходы правительства к вопросам идентификации пользователей в сети Интернет и содержащий, в том числе следующие принципы:

– **принцип прозрачности** – идентификация пользователя может осуществляться в случае, когда пользователь полностью информирован о данном процессе и понимает цель данных действий;

– **принцип кратности** – пользователь может пользоваться услугами и выбирать любых удостоверяющих провайдеров столько раз, сколько ему будет необходимо;

– **принцип минимизации данных** – использование минимально достаточного количества данных, необходимых для достижения цели взаимодействия;

– **принцип сертификации** – пользователь должен иметь уверенность в надёжности средств идентификации, деятельность которых основывается на обязательной сертификации;

– **принцип конкуренции и технологической нейтральности** (недопущение ограничения использования конкретных программно-технических средств по признакам происхождения, способа разработки и модели лицензирования).

Анализ Рекомендаций ФАТФ позволяет выявить определенный набор принципов и требований, предъявляемых к содержанию закона, регулирующего деятельность государственных органов и финансовой сферы в данной области. Такой закон должен включать в себя:

– основные положения, содержащие, в том числе, перечень государственных институтов, обеспечивающих реализацию закона;

– действия, которые должны предприниматься финансовыми организациями в целях исполнения закона;

– признаки подозрительных сделок, которые подлежат особому контролю, и о которых должно быть направлено сообщение в соответствующий орган;

– определение органа, ответственного за получение и обработку информации о подозрительных сделках;

– определение органа, ответственного за проведение дальнейшего расследования;

– ответственность финансовых организаций за нарушение требований закона;

– осуществление международного сотрудничества.

Раздел 12. Цифровые сервисы

Содержание

- регулирование цифровых сервисов в киберпространстве

Текущее регулирование (действующее законодательство):

1. Закон Кыргызской Республики «Об электронном управлении» от 19 июля 2017 г. № 127

Краткое описание выявленных недостатков

№	Описание недостатка	Тип[32]	Лучшая практика
12.1	Обеспечить защиту прав потребителей цифровых сервисов В соответствии со статьей 33 Конституции Кыргызской Республики важно обеспечить право потребителей на доступ к необходимой информации, включая: - информацию о качестве предоставляемых услуг, продаваемых товаров, а также иных сведений, имеющих важное значение для потребителя - информацию об операторе сервиса и предоставляемых им услугах	**П**	**Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (Закон о цифровых услугах)** Статья 12: «Поставщики посреднических услуг включают в свои правила и условия информацию о любых ограничениях, которые они налагают в отношении использования своего сервиса в отношении информации, предоставляемой получателями сервиса. Эта информация должна включать информацию о любых политиках, процедурах, мерах и инструментах, используемых для целей модерации контента, включая алгоритмическое принятие решений и проверку человеком. Он должен быть изложен ясным и недвусмысленным языком и должен быть общедоступным в легкодоступном формате.» **Закон Китайской Народной Республики об электронной торговле от 01.01.2019 г.** Статья 17: «Предприятие электронной коммерции должно полностью, достоверно, точно и своевременно раскрывать информацию о товарах или услугах для защиты права потребителей на знание и право выбора. Компания

[32] В таблице приводятся следующие типы недостатков регулирования:
(П) пробел в регулировании (регулирование требуется, но его нет)
(У) устаревшая норма (норма есть, но её нужно менять)
(Н) неработающая норма (норма есть, но в силу описанных причин она не работает)
(Б) действующая норма является необоснованным препятствием для осуществления деятельности

			электронной коммерции не имеет права проводить ложное или вводящее в заблуждение коммерческое продвижение путем фабрикации транзакций, составления комментариев пользователей или любыми другими способами, чтобы обмануть или ввести в заблуждение потребителей.» Статья 15: «Предприятие электронной коммерции обязано на видном месте своей домашней страницы постоянно публиковать информацию о своей лицензии на осуществление предпринимательской деятельности, информацию об административном лицензировании, относящемся к осуществляемому им предприятию, обстоятельства, не требующие от него регистрации участника рынка, предусмотренные статьей 10 настоящего Закона, и иную информацию., или отметка о ссылке на вышеуказанную информацию.»
12.2	Закрепить принцип добросовестной рекламы В соответствии со статьей 6 Закон Кыргызской Республики от 24 декабря 1998 года № 155 «О рекламе», не допускается распространение недобросовестной рекламы. Так как цифровые сервисы являются составной частью информационного пространства, использование рекламы является их неотъемлемой частью. В целях обеспечения прав и свобод человека и гражданина необходимо установить специальные требования к рекламе, размещаемой в цифровых сервисах	**П**	**Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (Закон о цифровых услугах)** Статья 24: «Онлайн-платформы, отображающие рекламу на своих онлайн-интерфейсах, должны обеспечивать, чтобы получатели услуги могли идентифицировать каждую конкретную рекламу, отображаемую каждому отдельному получателю, ясным и недвусмысленным образом и в режиме реального времени: (a) что отображаемая информация является рекламой; (b) физическое или юридическое лицо, от имени которого отображается реклама; (в) содержательная информация об основных параметрах, используемых для определения получателя, которому показывается реклама.»

			Закон Китайской Народной Республики об электронной торговле от 01.01.2019 г. Статья 17: «При предоставлении результатов поиска товаров или услуг потребителю на основе хобби, потребительской привычки или любых других его черт бизнес электронной коммерции обязан предоставлять потребителю варианты, не ориентированные на его идентифицируемые черты, а также уважать и в равной степени защищать законные права и интересы потребителей.»
12.3	Закрепить требования, позволяющих обеспечить добросовестную конкуренцию в информационном поле Степень вовлеченности граждан в информационное пространство, коммерциализация цифровых сервисов и многие иные факторы могут влиять на уровень конкуренции на товарном рынке в силу различного рода преимуществ цифровых сервисов над нецифровыми, а также между собой	**П**	**Закон Китайской Народной Республики об электронной торговле от 01.01.2019 г.** Статья 22: «Если бизнес электронной коммерции занимает доминирующее положение на рынке из-за своего технологического преимущества, количества пользователей, контроля над соответствующей отраслью, зависимости других компаний от него в торговле или любого другого фактора, бизнес электронной коммерции не может злоупотреблять доминирующим положением на рынке, чтобы исключить или ограничить конкуренцию.»
12.4	Предусмотреть гарантии обеспечения защиты персональных данных пользователей Защита персональных данных субъектов заключается в вопросах обработки персональных данных, их анализе и передачи третьим лицам, а также получении от субъекта персональных данных согласия, возможности его отзыва в любое время	**П**	**Статья 7 GDPR. Условия согласия** 3. Субъект данных имеет право в любое время отозвать свое согласие. Отзыв согласия не влияет на законность обработки, которая была основана на согласии до его отзыва. Субъект данных должен быть проинформирован об этом перед тем, как он выразил согласие. Отзыв согласия должен быть столь же прост, как и его выражение. **Закон Китайской Народной Республики об электронной торговле от 01.01.2019 г.** Статья 24: «Предприятие электронной коммерции обязано при сборе или использовании индивидуальной информации своих пользователей соблюдать положения о защите индивидуальной информации, содержащиеся в

			соответствующих законах и административных регламентах.» Статья 25: «Бизнес электронной коммерции должен прямо указывать средства и процедуры поиска, исправления или удаления пользовательской информации и снятия пользователя с регистрации, а также не устанавливать необоснованных условий поиска, исправления или удаления пользовательской информации и снятия пользователя с регистрации. При своевременном получении заявки на поиск, исправление или удаление пользовательской информации предприятие электронной коммерции обязано после проверки личности своевременно разрешить поиск, исправление или удаление пользовательской информации. В случае снятия пользователя с регистрации предприятие электронной коммерции обязано немедленно удалить информацию пользователя; если какой-либо закон или административный регламент предусматривает или стороны оговаривают, то сохранение, закон, административный регламент или оговорка имеют преимущественную силу.»
12.5	Закрепить принцип самостоятельного обеспечение безопасности цифровых сервисов их операторами от потенциальных IT-угроз Цифровые сервисы подвержены различного рода угрозам в киберпространстве. Закрепление возможности саморегулирования в области обеспечения безопасности цифровых сервисов на ровне с государственным регулированием, будет способствовать повышению степени безопасности сервисов, что в свою очередь позволит гарантировать: - бесперебойность работы цифровых сервисов - снижение рисков киберугроз	**П**	**Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (Закон о цифровых услугах)** Статья 12 «Поставщики посреднических услуг включают в свои правила и условия информацию о любых ограничениях, которые они налагают в отношении использования своего сервиса в отношении информации, предоставляемой получателями сервиса. Эта информация должна включать информацию о любых политиках, процедурах, мерах и инструментах, используемых для

	- безопасность информации, хранящейся в цифровых сервисах - безопасность персональных данных пользователей		целей модерации контента, включая алгоритмическое принятие решений и проверку человеком. Он должен быть изложен ясным и недвусмысленным языком и должен быть общедоступным в легкодоступном формате.» Статья 26: «Очень крупные онлайн-платформы должны выявлять, анализировать и оценивать с даты подачи заявки, указанной во втором абзаце статьи 25 (4), не реже одного раза в год любые значительные системные риски, вытекающие из функционирования и использования их услуг в Союзе. Эта оценка рисков должна быть специфичной для их услуг и включать следующие системные риски: (a) распространение незаконного контента через их сервисы; (b) любые негативные последствия для осуществления основных прав на уважение частной и семейной жизни, свободу выражения мнений и информации, запрещение дискриминации и прав ребенка, закрепленных соответственно в статьях 7, 11, 21 и 24 Закона; (c) преднамеренное манипулирование их сервисом, в том числе посредством недостоверного использования или автоматизированного использования сервиса, с фактическим или прогнозируемым негативным воздействием на защиту общественного здоровья, несовершеннолетних, гражданского дискурса или фактическими, или прогнозируемыми последствиями, связанными с избирательными процессами и общественной безопасностью.» **Закон Китайской Народной Республики об электронной торговле от 01.01.2019 г.** Статья 30: «Бизнес платформы электронной коммерции должен принимать технологические меры и другие необходимые меры для

			обеспечения своей кибербезопасности и стабильной работы, предотвращения незаконной и преступной деятельности в Интернете, эффективного противодействия событиям кибербезопасности и обеспечения безопасности торговли электронной коммерцией. Бизнес-платформа электронной коммерции должна составить план действий на случай возникновения событий кибербезопасности, и когда происходит событие кибербезопасности, она должна немедленно запустить план действий на случай непредвиденных обстоятельств, принять соответствующие меры по исправлению положения и сообщить об этом соответствующим компетентным органам.»

Комментарии

Различного рода сервисы, предоставляемые гражданам как государственными структурами, так и частными компаниями, под воздействием цифровых технологий начинаются переводится в цифровой формат. Последней тенденцией является интеграция большого количества цифровых сервисов в рамках одной цифровой платформы или экосистемы. Таким образом, цифровые сервисы являются составляющим элементом цифровой платформы. Задачей цифровых сервисов является предоставление услуг, удовлетворение потребностей граждан на основе информации в цифровом виде.

Большинство цифровых платформ, в которые включены цифровые сервисы, имеют финансовые, технологические ресурсы, данные и клиенскую базу для экспансии на международные рынки, а также используют такие ресурсы для конкуренции на внутреннем рынке. Правительства многих ведущих стран (США, Китай, Великобритания, члены ЕС) обеспокоены проблемой неурегулированности деятельности цифровых платформ, а равно и цифровых сервисов.

Беспокойство обуславливается возможностью оказать серьезное влияние на товарный рынок как внутри страны, так и на международном уровне. Внутри страны имеется двоякое противостояние между цифровыми сервисами между собой и цифровыми и обычными сервисами. Очевидным является факт, что сервисы, которые не были переведены в цифровой формат, уступают конкурентам.

Конкуренция с международными аналогами может привести к повышению киберугроз, снижению уровня безопасности цифровых сервисов, утечке информации и персональных данных пользователей и к иным последствиям.

При этом важно обеспечить бесперебойность функционирования сервисов, в том числе и цифровых, на основе определенных принципов.

Предлагается закрепить следующие:

- безопасность цифровой среды;

- здоровая конкуренция между цифровыми сервисами в рамках деятельности цифровых платформ;

- прозрачность условий доступа потребителей к сервисам цифровой экосистемы и платформы, не допускающих неограниченного усмотрения собственника экосистемы;

- свобода перехода пользователей между цифровыми платформами, экосистемами;

- свобода распоряжения пользователями своими данными, хранящимися и обрабатываемыми цифровой платформой, экосистемой;

- недопущение навязывания платформами и экосистемами собственных сервисов, создания дискриминационных условий;

- недопущение ограничения выбора потребителя;

- гарантия открытости.

23 апреля 2022 года было достигнуто соглашение между Европейским парламентом и государствами-членами ЕС по предложению о Законе о цифровых услугах (Digital Services Act), который в свою очередь оценивается мировым сообществом как беспрецедентный опыт, так как Закон впервые закрепляет статус цифровых платформ и правовое регулирование их деятельности. При этом в Китае в настоящее время уже действует Закон об электронной торговле, который также содержит отдельные положения, касающиеся деятельности рассматриваемых участников рынка.

Раздел 13. Государственные и муниципальные цифровые услуги

Содержание

- обеспечение процесса цифровой трансформации государственного управления (4 стадии цифровой трансформации) – backend

- принципы предоставления государственных и муниципальных услуг в цифровой форме – frontend

- координация в сфере цифровой трансформации государственного управления (между органами, ответственными за цифровую трансформацию, органами по развитию экономики, органами, обеспечивающими госуправление).

Текущее регулирование:

1. Закон Кыргызской Республики «Об электронном управлении» от 19 июля 2017 г.№ 127
2. Закон Кыргызской Республики «О государственных и муниципальных услугах» от 17 июля 2014 г. № 139
3. Постановление Правительства Кыргызской Республики «О мерах по оптимизации системы предоставления государственных услуг физическим и юридическим лицам» от 31 марта 2011 г. №129
4. Постановление Правительства Кыргызской Республики «О Типовом стандарте государственных и муниципальных услуг» от 3 сентября 2012 г. № 603
5. Постановление Правительства Кыргызской Республики «Об утверждении стандартов государственных услуг, оказываемых физическим и юридическим лицам государственным органам, их структурными подразделениями и подведомственными учреждениями» от 3 июня 2014 г. № 303
6. Постановление Правительства Кыргызской Республики «Об утверждении Правил пользования Государственным порталом электронных услуг» от 7 октября 2019 г. № 525
7. Постановление Правительства Кыргызской Республики «О реализации пилотного проекта "Государство как платформа" по внедрению инновационных способов предоставления государственных и муниципальных услуг и сервисов» от 25 февраля 2020 г. №113
8. Постановление Правительства Кыргызской Республики «О внесении изменений в постановление Правительства Кыргызской Республики "Об утверждении Правил пользования Государственным порталом электронных услуг"» от 7 октября 2019 года № 525" от 20 ноября 2020 г. № 573

Краткое описание выявленных недостатков

№	Описание недостатка	Тип [33]	Лучшая практика
13.1	Закрепить понятие «проактивных» услуг Требуется дополнение статьи 3 «Основные понятия, используемые в настоящем Законе» Закона Проактивность предоставления государственных и муниципальных услуг предусматривает электронный	**П**	В **Российской Федерации** в настоящее время активно проводится работа по внедрению проактивных услуг и суперсервисов. Предполагается, что каждый суперсервис будет состоять из взаимосвязанных госуслуг, услуг бюджетных учреждений, а также

[33] В таблице приводятся следующие типы недостатков регулирования:
(П) пробел в регулировании (регулирование требуется, но его нет)
(У) устаревшая норма (норма есть, но её нужно менять)
(Н) неработающая норма (норма есть, но в силу описанных причин она не работает)
(Б) действующая норма является необоснованным препятствием для осуществления деятельности

	способ подачи заявлений, приоритет «реестровой» модели (приоритет юридически значимых записей в электронных реестрах), преимущество или только исключительное взаимодействие между органом при предоставлении услуги с получателем и пр.		негосударственных сервисов (банковских, страховых и пр.) Опыт **Дании**, страны-лидера рейтинга электронного правительства ООН, интересен во многом с точки зрения проактивных услуг, основанных «на взаимодействии с гражданами в особые моменты их жизни». В **Эстонии** проактивные услуги в настоящее время задействованы при борьбе с безработицей, Фонд страхования по безработице (EUIF) уже использует искусственный интеллект для предоставления соискателям необходимой работы на основе их многолетнего опыта. В планах – здравоохранение и образование.
13.2	Закрепить принцип предоставления государственных и муниципальных услуг в электронной форме Требуется дополнение статьи 4 «Основные принципы предоставления государственных и муниципальных услуг» соответственно	**П**	**Статья 4 Федерального закона от 27 июля 2010 г. № 210-ФЗ "Об организации предоставления государственных и муниципальных услуг":** **Возможность получения государственных и муниципальных услуг в электронной форме**, если это не запрещено законом, а также в иных формах, предусмотренных законодательством Российской Федерации, по выбору заявителя, за исключением случая, если на основании федерального закона предоставление государственной или муниципальной услуги осуществляется исключительно в электронной форме.
13.3	Предусмотреть возможность получения государственных и муниципальных услуг в альтернативной форме при помощи цифровой идентификации личности человека	**П**	С 2021 года в **Российской Федерации** закреплена возможность получать с помощью биометрии широкий спектр финансовых и государственных услуг посредством Единой биометрической системы и Единой системы идентификации и аутентификации. При этом, на рассмотрении в Государственной Думе Российской Федерации находится законопроект, вводящий запрет обуславливать предоставление

			услуг обработкой биометрических данных. **Эстония** занимает третье место в рейтинге электронного правительства ООН. Она имеет на сегодняшний день самую передовую национальную систему удостоверений личности в мире. Помимо легального удостоверения личности с фотографией, обязательная национальная карта обеспечивает цифровой доступ ко всем защищенным электронным услугам государства. В сотрудничестве с SK ID Solutions и Cybernetica был разработан так называемый Smart-ID – электронная идентификация нового поколения, предназначенная для удобного использования на смарт-устройствах, способная сохранять при этом высокий уровень безопасности.
13.4	Закрепить возможность внедрения «реестровой модели» предоставления государственных услуг «Реестровая модель» представляет собой конструкцию, когда результатом предоставления услуги является не выдача разрешительного документа на бумажном носителе, а запись в электронном реестре (хотя получение выписки из реестра может быть сохранено в качестве отдельного сервиса).	**П**	В настоящее время реестровая модель оказания государственных услуг успешно внедрена в ряде ведомств **Российской Федерации** - ФНС, Росреестре и Росаккредитации. В частности, в последней, она позволила отказаться от использования в обращении аттестата аккредитации на бумажном носителе, заменив его автоматически генерирующейся выпиской с QR-кодом. Реестровая модель предоставления государственных услуг применяется в **Эстонии** в настоящее время только в отдельных сферах, например, в налоговой.

Комментарии

Оптимизация государственного управления тесным образом связана с предоставлением государственных и муниципальных услуг. В свою очередь, такая оптимизация в настоящее время невозможна без повсеместного внедрения цифровых технологий в государственном и муниципальном управлении.

Первым этапом цифровизации государственных и муниципальных услуг принято считать внедрение концепции «одного окна». Также превращение обычных государственных услуг в электронный стала их платформизация.

Этап же цифровизации подразумевает перевод большинства государственных и муниципальных услуг исключительно в электронный вид с приоритетом принципа проактивности и исключением любого очного взаимодействия между получателем услуги и

органом, а также заменой бумажного документооборота электронным. Помимо проактивности, будут реализовываться также принципы доступности, омникальности, бесшовности и ряд иных. Применение реестровых моделей начато давно в иных отраслях, для управления документацией и информацией. Реализация реестровой модели в сфере предоставления услуг позволит решить несколько задач:

- сокращение очных посещений центров предоставления услуг;
- сокращение времени получения результата государственной или муниципальной услуги;
- ускорение перехода к полноценному электронному документообороту;
- иные

Наибольший опыт цифровизации государственного управления накоплен у Дании и Эстонии, которые уже продолжительное время лидируют в рейтинге электронного правительства ООН. Примечательным может быть опыт Российской Федерации, где применение цифровых технологий в сфере предоставления государственных и муниципальных услуг активно ведется либо уже готовы к внедрению.

Раздел 14. Цифровое здоровье и благополучие

Содержание

- подходы к управлению данными о состоянии человека в течение всей его жизни
- возможность установления требований к программным и аппаратным средствам для обеспечения здоровья и благополучия человека (отсылочная норма)
- применение этических норм

Текущее регулирование (действующее законодательство):

1. Закон Кыргызской Республики от 24 июля 2009 года № 248 «Об общественном здравоохранении»;
2. Закон Кыргызской Республики от 9 января 2005 года № 6 «Об охране здоровья граждан в Кыргызской Республике»;
3. Закон Кыргызской Республики от 13 августа 2004 года № 116 «Об организациях здравоохранения в Кыргызской Республике»;
4. Закон Кыргызской Республики от 18 октября 1999 года № 112 «О медицинском страховании граждан в Кыргызской Республике»;
5. Закон Кыргызской Республики от 2 августа 2017 года № 166 «Об обращении медицинских изделий»;
6. Закон Кыргызской Республики от 2 августа 2017 года № 165 «Об обращении лекарственных средств»;
7. Закон Кыргызской Республики от 30 июля 2003 года № 159 «О системе единого плательщика в финансировании здравоохранения Кыргызской Республики»;
8. Закон Кыргызской Республики от 19 июля 2017 года № 128 «Об электронной подписи»;
9. Закон Кыргызской Республики от 19 июля 2017 года № 127 «Об электронном управлении»;
10. Закон Кыргызской Республики от 14 апреля 2008 года № 58 «Об информации персонального характера»;
11. Закон Кыргызской Республики от 14 июля 2014 года № 136 «О биометрической регистрации граждан Кыргызской Республики»;
12. Соглашение о единых принципах и правилах обращения медицинских изделий (изделий медицинского назначения и медицинской техники) в рамках Евразийского экономического союза (г. Москва, от 23 декабря 2014 года, присоединение – Закон Кыргызской Республики от 14 июля 2015 года № 167).
13. Указ Президента Кыргызской Республики от 12 октября 2021 года УП № 435 «О Национальной программе развития Кыргызской Республики до 2026 года»;
14. Постановление Правительства Кыргызской Республики от 20 декабря 2018 года № 600 «О Программе Правительства Кыргызской Республики по охране здоровья населения и развитию системы здравоохранения на 2019-2030 годы «Здоровый человек - процветающая страна»;
15. Распоряжение Кабинета министров Кыргызской Республики от 12 января 2022 года № 2-р «Об утверждении Плана мероприятий по цифровизации управления и развития цифровой инфраструктуры в Кыргызской Республике на 2022-2023 годы»;
16. Приказ Министерства здравоохранения Кыргызской Республики от 15 марта 2018 года № 190 «Об утверждении Архитектуры электронной системы здравоохранения КР на 2018-2023 гг.»;

№	Описание недостатка	Тип[34]	Лучшая практика
14.1	Не закреплены основополагающие принципы развития системы электронного здравоохранения.	**П**	Предлагается определить принципы цифровой трансформации общественного здравоохранения. Лучшая практика: 8 принципов цифровой трансформации общественного здравоохранения Регионального отделения ВОЗ – Панамериканской организации здравоохранения (The Pan American Health Organization (PAHO)). Исходя из указанной практика предлагается закрепить следующие принципы: - единства электронной системы здравоохранения; - интероперабельности (совместимости) медицинских информационных систем; - инклюзивности и бесплатного доступа к электронной системе здравоохранения; безопасности персональных данных; постоянного совершенствования архитектуры электронной системы здравоохранения.
14.2	В действующем законодательстве наличествуют отдельные пробелы в части вопросов обеспечения безопасности медицинских персональных данных, например: не определен порядок выдачи и получения информированного добровольного согласия и согласия на обработку персональных данных пациента на основе конклюдентных действий при получении медицинских услуг с использованием телемедицинских технологий; не определен порядок и случаи передачи персональных медицинских данных третьей стороне;	**П**	Предлагается закрепить основы защиты медицинских персональных данных. Лучшая практика: в качестве образца для формирования основополагающих общих норм в сфере защиты персональных данных предлагается применить практику GDPR, а также Постановление о персональных данных (конфиденциальности) (The Personal Data (Privacy) Ordinance (PDPO) CAP КНР Гонконг. В качестве лучшей практики для защиты медицинских персональных данных с соответствующей апробацией предлагается рассмотреть Постановление о

[34]В таблице приводятся следующие типы недостатков регулирования:
(П) пробел в регулировании (регулирование требуется, но его нет)
(У) устаревшая норма (норма есть, но её нужно менять)
(Н) неработающая норма (норма есть, но в силу описанных причин она не работает)
(Б) действующая норма является необоснованным препятствием для осуществления деятельности

	не урегулированы отдельные вопросы обработки персональных медицинских данных в медицинских информационных системах.		персональных данных (конфиденциальности) и система обмена электронными медицинскими картами (Personal Data (Privacy) Ordinance and Electronic Health Record Sharing System (PCPD)) САР КНР Гонконг.
14.3	Не определен порядок сооплаты при получении медицинских услуг с использованием телемедицинских технологий для участия частных компаний в рамках государственно-частного партнерства.	**П**	Внести дополнения в положение о сооплате за медицинские услуги и возможно в законы о системе единого плательщика и о государственно-частном партнерстве. Лучшая практика: Федеральный закон от 13.07.2015 № 224-ФЗ «О государственно-частном партнерстве, муниципально-частном партнерстве в Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации»
14.4	Не урегулирован порядок использования устройств дистанционного мониторинга состояния здоровья и физиологических параметров домашнего применения и стационарозамещающих технологий.	**П**	Предлагается определить порядок и регулирование устройств дистанционного мониторинга состояния здоровья и физиологических параметров домашнего применения и стационарозамещающих технологий в подзаконных актах и предусмотреть соответствующие ссылочные/бланкетные нормы в части вышеуказанных устройств. Лучшая практика: Руководство по классификации медицинских изделий ЕС (MDCG 2021-24 Guidance on classification of medical devices): – раздел 10 «Активные устройства для диагностики и мониторинга или предназначенные для диагностической или терапевтической радиологии»; – раздел 11 «Программное обеспечение, предназначенное для предоставления информации для принятия решений с диагностическими или терапевтическими целями, или программное обеспечение, предназначенное для мониторинга физиологических процессов».

14.5	Не предусмотрен порядок использования со стороны пациента простой электронной подписи при получении медицинских услуг с использованием телемедицинских технологий.	**П**	Предлагается внести изменения в Закон Кыргызской Республики от 19 июля 2017 года № 128 «Об электронной подписи» и/или в соответствующие подзаконные акты, в части положений, предусматривающих использование простой цифровой подписи пациента и, в отдельных случаях необходимости оказания медицинской помощи, возможность использования систем электронного здравоохранения без процедуры идентификации и аутотентификации. Лучшая практика: Регламент ЕС по электронной идентификации и доверительным услугам для электронных сделок на Европейском едином рынке (Electronic Identification, Authentication and Trust Services (eIDAS)/

Комментарии

Общая архитектура электронного здравоохранения Кыргызской Республики состоит из прикладных приложений, компонента общесистемных и инфраструктурных сервисов, интеграционной шины единого информационного пространства здравоохранения.

Сегмент прикладных приложений (клинических) включает существующие и создаваемые информационные системы, обеспечивающие информационно-технологическую поддержку функций управления в здравоохранении, информационного взаимодействия с гражданами. Создание и совершенствование клинических приложений должно базироваться на основе всестороннего внедрения электронной медицинской карты как базового программного продукта, объединяющего информацию из различных информационных систем организаций здравоохранения различных уровней.

Электронная медицинская карта должна будет содержать исчерпывающий структурированный объем общих персональных, клинических, биометрических, социальных, экономических, финансовых, страховых и других данных о пациенте, документировать оказанные ему медицинские услуги.

Основными целями внедрения электронной медицинской карты являются обеспечение непрерывности, преемственности и качества диагностики, лечения, а также своевременной профилактики и иных мероприятий по обеспечению здоровья конкретного человека путем документирования и сохранения соответствующей медицинской информации и своевременного предоставления ее уполномоченным медицинскими работниками пациенту.

Внедрение электронной медицинской карты направлено на решение следующих задач:

- доступность информации о здоровье пациента в любой точке страны, непротиворечивой и в полном объеме;
- оперативное получение информации в удобной форме, структурированной в соответствии с принятой методикой оформления медицинских документов.

Наряду с внедрением электронной медицинской карты как базового продукта для устойчивого развития электронного здравоохранения необходимо перевести в электронный режим работу лабораторий, аптек, санитарно-эпидемиологической службы и других специализированных организаций здравоохранения.

Для обеспечения доступа к информации в сфере лекарственного обращения и улучшения прозрачности необходимо создание электронной базы данных лекарственных средств и изделий медицинского назначения, которая будет охватывать все аспекты обращения лекарственных средств, начиная с момента регистрации и заканчивая их продажей и утилизацией.

Соответствующие работы в направлении создания электронной базы данных лекарственных средств и изделий медицинского назначения проводятся в соответствии с Концепцией создания электронной базы данных лекарственных средств и изделий медицинского назначения в Кыргызской Республике, утвержденной постановлением Правительства Кыргызской Республики от 27 октября 2015 года № 743.

Международный опыт

Пример изменений в направлении цифрового здравоохранения показывает **Португалия.** В настоящее время в стране действует 60 систем информационно-коммуникационных технологий разного уровня развития. Цель состоит в том, чтобы изменить парадигму оказания медицинской помощи, поместив гражданина в центр системы. Этот переход осуществляется с помощью внедрения национальной электронной медицинской карты. Эта карта предназначена для сохранения на протяжении всей жизни человека, предоставляя ему возможность получать информацию из разных медицинских учреждений, с которыми человек взаимодействует в различные периоды жизни. Чтобы удовлетворить эту потребность, Отдел общих служб Министерства здравоохранения разрабатывает национальные системы, используя простые в применении стандарты. Информация также доступна физическим лицам через портативный «кошелек здоровья», содержащий данные лекарственных назначений, предупреждения о времени приеме лекарств и многое другое. Комплексные, взаимно совместимые системы, относящиеся к здоровью, выходят далеко за рамки собственно медицинских учреждений. Для устранения существующих пробелов необходимы меры стратегического руководства на национальном уровне, многоотраслевые взаимодействия и стратегии согласования с заинтересованными сторонами.» - указывается в одном из докладов.

Смещение акцентов на профилактику – более раннее и более целенаправленное лечение, привлечение индивидуума в качестве активного партнера, например, через сведения о результатах лечения, сообщенные пациентом. Обеспечение своевременного знания – достоверные данные об индивидууме должны быть доступны в любое время, когда это необходимо, посредством оказания координированной помощи с применением интегрированных информационных систем. Основой для этого является «Паспорт Здоровья», включающий в себя не только медицинскую информацию индивидуума, но и информацию по его образу жизни (питанию, физической активности, социальным условиям и др.) с целью комплексной оценки возможных рисков и неблагоприятных тенденций по ухудшению здоровья и своевременной поддержки через систему здравоохранения и социальной помощи;

В структуре систем здравоохранения можно выделить три основных компонента:

- высококачественная первичная медико-санитарная помощь и услуги общественного здравоохранения;
- деятельность многочисленных секторов, направленной на удовлетворение потребностей;
- активно вовлеченных сообществ с расширенными правами и возможностями.

Цифровое здравоохранение играет ключевую роль в создании мостов между этими тремя структурными компонентами.

«Медицинская модель общественного здравоохранения медленно и осторожно движется к более широкому использованию персонализированной информации, но потребители менее терпеливы: они выходят в интернет для самодиагностики. Это означает, что для определения болезненного состояния индивидуума можно использовать не только клинические данные, но и всевозможные персональные пользовательские данные, или

«социальные выбросы», иллюстрирующие цифровой ландшафт, отслеживание которого может помочь в формировании многих дополнительных представлений о проблемах здоровья.

Ориентация на данные имеет решающее значение с одним основным правилом: все собранные данные должны быть защищены, и к ним следует относиться с уважением, однако аргументы в отношении прав собственности на данные являются сложными, и в конечном счете все данные будут иметь много владельцев.

Искусственный интеллект и машинное обучение в системах здравоохранения и в предоставлении медицинских услуг

По итогам работы, проведенной Национальной службой здравоохранения **Англии**, были сформулированы три следующих принципа использования искусственного интеллекта в здравоохранении:

- создание стандартов и нормативов в поддержку использования искусственного интеллекта в системе здравоохранения имеет большое значение и требует изменения механизмов разработки и применения нормативных актов.
- следует осваивать искусство возможного, уделяя время и усилия тому, чтобы развеивать мифы и активно работать над демонстрацией практического применения искусственного интеллекта в здравоохранении.
- на этом пути никто не должен оставаться позади: необходимо обеспечивать инклюзивный подход к искусственному интеллекту в здравоохранении, который предусматривает участие медицинских работников, пациентов и общественности. Прозрачность и коммуникация в отношении инициатив и тематических исследований имеют решающее значение.

Электронный рецепт, который необходимо рассматривать не как разовое технологическое внедрение, а как модель, подвергающуюся постоянной адаптации и эволюции. В Швеции система электронных рецептов была введена в 1980-х годах, когда государству принадлежала монополия на аптеки. В 2008–2009 гг. этот рынок был либерализован. Примерно в этот период было учреждено Шведское агентство электронного здравоохранения, которое в настоящее время отвечает за все базы данных электронных рецептов, с которыми связаны 1400 аптек по всей стране. В результате – 99% рецептурных назначений проводится в электронном формате, повысились качество и уровень безопасности для пациентов, улучшилось обслуживание граждан, достигается экономия времени и средств, ужесточился контроль над системой. В Испании особо успешным оказалось создание единого плана лекарственного лечения, в котором представлен сводный обзор назначенных пациенту лекарств. Препараты сгруппированы для простоты понимания в соответствии с продолжительностью и типом лечения (длительный курс, прием препаратов при необходимости, краткий курс и др.), план содержит основные сведения о каждом препарате и инструкции о том, как его принимать.

Эффективное использование информации для принятия решений в здравоохранении. «Решающее значение имеет инновационная визуализация, представляющая информацию в наиболее простой форме. Не следует упускать из виду важность использования «успешных историй» для иллюстрации того, о чем свидетельствуют данные, и многие подходы для этого уже существуют. Основной целью является оказание медицинской помощи гражданам».

В **Ирландии** политика определяется на основе изучения информации о системе здравоохранения на макроуровне и анализа эффективности системы, борющейся с растущими расходами и длинными очередями для пациентов. Ландшафт данных здравоохранения фрагментирован, поэтому была проделана работа, чтобы выяснить, какие технологии и процессы доступны для получения более общей картины. Процесс анализа данных был направлен на минимизацию данных, необходимых для оптимальной передачи надлежащих сообщений. Был приобретен один из имеющихся на рынке аналитических инструментов, с помощью которого все существующие наборы данных были объединены в новой архитектуре (база данных MySQL) с программным обеспечением на входе и выходе, чтобы помочь

наилучшим образом использовать данные и поддерживать основные виды деятельности Министерства здравоохранения.

Цель состоит в том, чтобы создать централизованную систему управления медицинскими данными, которая объединяет инструменты в едином информационном пространстве для обращения с данными для всех задействованных субъектов, от поставщиков услуг до пациентов, в сочетании с системами поддержки принятия решений.

Раздел 15. Технологическая инфраструктура цифрового управления

Содержание

- принципы использования инфраструктуры (повторное использование, недискриминационный доступ к инфраструктуре и т. п.)
- полномочия по установлению технических требований к отдельным видам инфраструктуры.

Текущее регулирование (действующее законодательство):

1. Закон Кыргызской Республики от 19 июля 2017 года № 127 «Об электронном управлении»;
2. Закон Кыргызской Республики от 2 апреля 1998 года № 31 «Об электрической и почтовой связи»;
3. Закон Кыргызской Республики от 22 мая 2004 года № 67 «Об основах технического регулирования в Кыргызской Республике»;
4. Указ Президента Кыргызской Республики от 31 октября 2018 года № 221 «О Национальной стратегии развития Кыргызской Республики на 2018-2040 годы»;
5. Постановление Правительства Кыргызской Республики от 5 декабря 2019 года № 661 «О некоторых вопросах, связанных с государственной инфраструктурой электронного управления»;
6. Постановление Правительства Кыргызской Республики от 13 августа 2020 года № 421 «Об утверждении Правил межсетевого соединения в Кыргызской Республике»;
7. Постановление Правительства Кыргызской Республики от 31 декабря 2019 года № 747 «Об утверждении Требований к государственным центрам обработки данных и соединяющим их каналам связи»;
8. Постановление Правительства Кыргызской Республики от 21 ноября 2017 года № 762 «Об утверждении Требований к защите информации, содержащейся в базах данных государственных информационных систем»;
9. Постановление Кабинета Министров Кыргызской Республики от 25 декабря 2021 года № 352 «Об утверждении Плана мероприятий Кабинета Министров Кыргызской Республики по реализации Национальной программы развития Кыргызской Республики до 2026 года»;
10. Распоряжение Кабинета Министров Кыргызской Республики от 12 января 2022 года № 2-р «План мероприятий по цифровизации управления и развития цифровой инфраструктуры в Кыргызской Республике на 2022-2023 годы».

Краткое описание выявленных недостатков и ориентиров из мировой практики

№	Описание недостатка	Тип[35]	Лучшая практика
15.1	Отдельные правовые нормы, устанавливающие принципы развития технологической инфраструктуры цифрового (электронного) управления, в действующем законодательстве Республики Кыргызстан отсутствуют.	**П**	В силу комплексного характера задач по цифровизации государственного управления, отдельных практик, посвященных правовому регулированию именно *технологической инфраструктуры* цифрового (электронного) управления, не применяется. Все

35 В таблице приводятся следующие типы недостатков регулирования:
(П) пробел в регулировании (регулирование требуется, но его нет)
(У) устаревшая норма (норма есть, но её нужно менять)
(Н) неработающая норма (норма есть, но в силу описанных причин она не работает)
(Б) действующая норма является необоснованным препятствием для осуществления деятельности

			подобные практики имплементированы в соответствующие нормативные и ненормативные правовые акты (в том числе, документы стратегического планирования) различных уровней. Вместе с тем, в качестве одной базовой практики предлагается рассмотреть пункт 2 «Основные принципы совершенствования инфраструктуры электронного взаимодействия» раздела IV Концепции развития механизмов предоставления государственных и муниципальных услуг в электронном виде (утв. Распоряжением Правительства РФ от 25.12.2013 № 2516-р). Предлагается включить в разрабатываемый проект принципы: • недискриминационного доступа к инфраструктуре; • отчуждаемости инфраструктуры электронного взаимодействия от ее разработчиков, поставщиков и эксплуатирующих организаций; • определенности порядка использования инфраструктуры электронного взаимодействия; • взаимной совместимости информационных систем инфраструктуры электронного взаимодействия; • стабильности и преемственности характеристик инфраструктуры электронного взаимодействия; • максимального использования возможностей рынка; • обеспечения безопасности персональных данных и иной информации ограниченного доступа. Кроме того, в рамках данного раздела, предлагается предусмотреть ссылочные и (или) бланкетные нормы на соответствующие отраслевые законы и (или) подзаконные акты, регулирующие отношения в рамках инфраструктурного уровня государственной инфраструктуры электронного управления,

			образуемого государственными центрами обработки данных и соединяющими их каналами связи.
15.2	В соответствии со статьей 24 Закона Кыргызской Республики от 19 июля 2017 года № 127 «Об электронном управлении», требования к государственным центрам обработки данных и соединяющим их каналам связи, включая требования к устойчивости и защищенности, а также порядок включения центров обработки данных и соединяющих их каналов связи в состав государственной инфраструктуры электронного управления устанавливаются Правительством Кыргызской Республики. По результатам анализа соответствующих нормативных и ненормативных правовых актов, установлено, что текущее регулирование охватывает узкий перечень функциональных и технических параметров ЦОД.	**П**	Цели и задачи государственных центров обработки данных (далее – ГЦОД), их параметры, структура, требования по защищенности и устойчивости и соединяющих их каналов связи установлены постановление Правительства КР от 31 декабря 2019 года № 747 «Об утверждении Требований к государственным центрам обработки данных и соединяющим их каналам связи». Требования к системам бесперебойного функционирования технических средств серверного оборудования и к серверному помещению государственного органа, органа местного самоуправления, организации установлены постановлением Правительства КР от 21 ноября 2017 года № 762 «Об утверждении Требований к защите информации, содержащейся в базах данных государственных информационных систем». **Лучшая практика:** ГОСТ Р 58812-2020 РФ «Центры обработки данных. Инженерная инфраструктура. Операционная модель эксплуатации. Спецификация» утвержденный и введенный в действие приказом Федерального агентства по техническому регулированию и метрологии 19.02.2020 №68 СТ предусматривает более детальные условия проектирования и эксплуатации центров обработки данных. К примеру, в ГОСТ Р 58812-2020 устанавливаются требования к организационной модели эксплуатации (организационной структуре службы эксплуатации, ресурсной модели), требования к процессам эксплуатации инженерной инфраструктуры (обслуживание

			оборудования, контроль качества, гарантирования безопасности, взаимодействия). Исходя из схожих политических, социально-экономических и исторических факторов развития, российский опыт зачастую имеет более благоприятный сценарий развития в Республике Кыргызстан в отличие от практики стран дальнего зарубежья, а также не требует Таким образом, предлагается несколько вариантов обеспечения правового регулирования ГЦОД: • имплементация в систему регулирования технологической инфраструктуры цифрового управления соответствующих государственных (национальных) стандартов (как более гибких и эффективных инструментов отраслевого регулирования) путем включения соответствующих положений в текст; • разработка и принятие соответствующих государственных (национальных) стандартов, устанавливающих требования к технологической инфраструктуре цифрового управления в соответствии требованиями и стандартами, соответствующими современному уровню развития в данной отрасли.
15.3	В Законе Кыргызской Республики от 2 апреля 1998 года № 31 «Об электрической и почтовой связи» наличествуют коррупционные риски и риски злоупотребления доминирующим положением в силу следующих факторов: - установленные в Законе требования о недопустимости дискриминации носят дискретный характер; - отсутствие развития данных правовых механизмов в подзаконных актах; - отсутствует механизм контроля	**Н**	В связи с данным недостатком, предлагается установить соответствующие правила обеспечения недискриминационного доступа к сетям электросвязи и предусмотреть соответствующие положения. Примером эффективной практики является Постановление Правительства Российской Федерации от 29.11.2014 № 1284 «Об утверждении Правил недискриминационного доступа к инфраструктуре для размещения

	уполномоченных органов за соблюдением прав операторов электросвязи.		сетей электросвязи».

Раздел 16. Сети и ресурсы электросвязи (телекоммуникаций)

Текущее регулирование (основные акты действующего законодательства):

1. Закон КР об электрической и почтовой связи
2. Закон КР о почтовой связи
3. Закон КР о лицензионно-разрешительной системе
4. Закон КР об электронном управлении
5. Закон КР о естественных монополиях в Кыргызской Республике
6. Закон КР об основах технического регулирования
7. Закон КР о порядке проведения проверок субъектов предпринимательства
8. Закон КР о телевидении и радиовещании
9. Закон КР о гарантиях и свободе доступа к информации
10. Закон КР об электронной подписи
11. Налоговый Кодекс КР
12. Кодекс Кыргызской Республики о неналоговых доходах
13. Кодекс КР о правонарушениях
14. Положение о лицензировании деятельности по использованию радиочастотного спектра (ППКР №754 от 17.11.2017г.)
15. Положение о лицензировании деятельности в области электрической и почтовой связи (ППКР от 31 декабря 2019 года № 746)
16. Национальная система и план нумерации сетей электросвязи Кыргызской Республики (ППКР от 9 января 2018 года №10)
17. Правила оказания услуг подвижной радиотелефонной связи (ППКР от 17 февраля 2014г. №97)
18. Методика расчета ежегодной платы за использование номиналов и (или) полос радиочастот радиочастотного спектра (ППКР №460 от 7 июля 2015 года)

Краткое описание выявленных недостатков и ориентиров из мировой практики

№	Описание недостатка	Тип[36]	Лучшая практика
16.1	Законодательные нормы, регулирующие вопросы создания сетей связи, их эксплуатации, а также использования ресурсов электросвязи, включены в различные отраслевые законодательные акты и зачастую не согласованы между собой	**У**	Системное приведение норм, относящихся к вопросам сетей и ресурсов электросвязи (телекоммуникаций), в соответствие с отраслевым (специальным) законодательством, с возможным исключением их из иных законодательных актов в целях избежания ненужного дублирования и избыточного регулирования
16.2	В законе КР об электрической и почтовой связи исключить положения, касающиеся почтовой связи ввиду наличия отраслевого (специального) закона КР «О почтовой связи» (ст.ст.18-20 и др.)	**У**	Законодательство стран Европейского союза, как правило, выводит регулирование (демонополизируемых или остающихся во владении государства) почтовых услуг за рамки каких-либо «непрофильных» правовых актов

[36] В таблице приводятся следующие типы недостатков регулирования:
(П) пробел в регулировании (регулирование требуется, но его нет)
(У) устаревшая норма (норма есть, но её нужно менять)
(Н) неработающая норма (норма есть, но в силу описанных причин она не работает)
(Б) действующая норма является необоснованным препятствием для осуществления деятельности

16.3	Одним из принципов ст.1 закона КР об электрической связи указана «всемерная поддержка предоставления высококачественных традиционных и инновационных услуг электрической и почтовой связи». Этот принцип не конкретизирован и на практике никак не реализуется	**Н**	Требуется конкретизация указанного принципа в описании соответствующих правовых институтов (господдержки). Например, как это предусмотрено законами США и стран Евросоюза в части возмещения затрат операторам связи для достижения определенных государством целей, а также установления норм технологической нейтральности, стимулирующих переход к перспективным технологическим решениям
16.4	Ст. 2 закона КР об электриче- ской и почтовой связи «Определения»	**У**	Привести в соответствие с глоссарием Международного союза электросвязи
16.5	Ст. 9 закона КР об электриче-ской и почтовой связи «Использование радиочастотно- го спектра и орбитальных позиций спутников связи» не содержит положений, облегчаю- щих использование радиоспект- ра для оказания перспективных услуг и освоения новых технологий («интернет вещей», системы искусственного интеллекта и т.п.)	**П**	В законодательстве многих стран Европейского союза и других регионов мира содержатся прямые нормы (позитивные предписания) направленные на стимулирование использования радиоспектра в интересах оказания перспективных услуг и развития новейших технологий
16.6	Ст.13 закона КР об электрической и почтовой связи закрепляет требования к лицензии «Кыргызтелекома». Это нарушает принцип равенства хозяйствующих субъектов	**У**	В рамках общемировой тенденции к демонополизации сферы электросвязи статья подлежит исключению из закона.
16.7	В статье 26 закона КР об электрической и почтовой связи содержится неработающая норма о компенсации убытков, понесенных оператором услуг электросвязи, из-за приостановления его деятельности. То же – в следующей статье 27	**Н**	Требуется регламентация порядка соответствующей компенсации из бюджета
16.8	В статье 31 закона КР об электрической и почтовой связи содержится положение об учёте строительными и иными организациями требований операторов связи о размещении их технических средств. На практике норма не работает, так как при строительстве не учитывается потребность в сетях связи и отсутствует ответственность застройщика за неисполнение этой нормы	**Н**	Соответствующие корреспондирующие нормы должны быть внесены в градостроительное законодательство и Кодекс КР о правонарушениях

16.9	В кодексе КР о правонарушени-ях диспозиции статей не соот-ветствуют нормативным актам, действующим в области связи	**Б**	Требуется приведение в соответствие; например как это сделано в Кодексе Республики Молдовы о правонарушениях (Глава 14)
16.10	Согласно кодексу КР о неналоговых платежах «поставщики услуг электросвязи и почтовой связи вносят отчисления на развитие отрасли связи в размере 0,9 процента от выручки услуг электрической и почтовой связи». При этом на значимые проекты в области связи фактически денежные средства не выделяются	**Н**	Модельный закон об электронных коммуникациях для стран Восточного партнерства.
16.11	В Налоговом кодексе КР налогом на доход облагаются «телекоммуникационные услуги» (ст.249), но законодательством о связи не предусмотрена данная терминология	**Б**	Конкретизировать (гармонизировать) терминологию
16.12	В Налоговом кодексе КР ставка налога с продаж установлена самая высокая – 5%, в то время как для банковской системы и застройщиков ставка составляет по 2% (ст.368)	**Б**	Дополнительное налогообложение должно быть устранено
16.13	В Положении о лицензировании деятельности в области электрической и почтовой связи многие нормы потеряли актуальность, и (или) избыточны, и (или) недостаточно конкретизированы для единообразного толкования.	**Б**	Гармонизация с законодательством ЕС и сокращение избыточных требований
16.14	В Методике расчёта ежегодной платы за использование номиналов и (или) полос радиочастот радиочастотного спектра установленные коэффициенты эффективности не направлены на стимулирование расширения сети и снижения финансового бремени на оператора связи	**Б**	Аналогичная Методика, применяемая в Российской Федерации

Комментарии

Особенности развития телекоммуникационной инфраструктуры, использования сетей и ресурсов электросвязи в Кыргызской Республике в значительной степени связаны с её географическим положением. Кыргызская Республика не имеет выхода к морю. Более трёх четверти территории страны занимают скалистые горы (средняя высота над уровнем моря составляет 2750м), что обусловило преимущественное применение беспроводных технологий связи и активное использование радиочастотного ресурса. Широкое применение также нашли волоконно-оптические линии связи. Согласно данным Международного союза электросвязи

(МСЭ) по Индексу развития ИКТ по итогам 2017 года Кыргызстан на 109 месте из 176 стран мира и на 10 месте среди стран СНГ.

В январе 2022 года в Кыргызстане было 3,41 миллиона интернет-пользователей (на 6,68 млн населения). Уровень проникновения интернета в Кыргызстане составил 51,1% от общей численности населения. В Кыргызстане зафиксировано 3,60 миллиона пользователей социальных сетей (53,9% от общей численности населения). Наибольший удельный вес по объему оказываемых услуг на рынке связи занимает мобильная (сотовая) связь. По итогам 2021 года мобильная сотовая связь занимает второе место на рынке связи с показателем более чем в 41,7% по удельному весу по объему оказываемых услуг и составил 10 245,89 млн. сом, что на 15,6% больше аналогичного показателя прошлого года.

Телекоммуникационный рынок Кыргызстана отличает относительно либеральное до недавнего времени законодательство, низкая себестоимость услуг по передаче данных, высокая конкуренция между основными игроками отрасли.

Действующее в Кыргызской Республике регулирование вопросов электросвязи основано на принятом в 1997 году Законе КР «Об электрической и почтовой связи», основной задачей закона было развитие конкуренции и рост числа операторов в сфере электросвязи. При этом ограничивались полномочия исторического оператора связи ОАО «Кыргызтелеком», который в то же время был признан в качестве национального. Законом также предусматривалось разграничение прав и полномочий государственного органа, определяющего политику и органа, отвечающего за регулирование рынка (Национальное агентство связи). Орган регулирования имел полномочия разработки собственных нормативных актов, направленных на оперативное регулирование. Действие актов было направлено на обязательное исполнение всеми участниками рынка. Вместе в тем, определен орган, разрабатывающий политику в сфере использования радиочастотного спектра.

Такая структура была довольно успешной. Рынок связи начал активно развиваться, привлекая своей простотой входа на рынок и получения государственного ресурса (телефонной нумерации и радиочастотного ресурс). Заработали 4 оператора сотовой связи, Кыргызстан сумел внедрить и использовать на своей относительно не большой территории несколько стандартов мобильной связи таких как DAMPS, GSM и CDMA. Такой прорыв дал значительную возможность выбора абонентам. Кроме того, регулятор обладал функциями надзора и контроля, а также самостоятельными функциями антимонополии, что позволяло качественно исследовать и анализировать рынок, иметь четкое представление об участниках рынка и их положению, рассматривать жалобы и обращения граждан в рамках защиты прав потребителей. В дальнейшем система органов управления в сфере электросвязи неоднократно модифицировалась.

За истекшие после принятия базового закона о связи годы законодательство Кыргызской Республики значительно изменилось в сторону появления многочисленных нормативных актов, относящихся к разным отраслям и содержащих те или иные правовые нормы в сфере регулирования электросвязи, но без должной координации со специальным (отраслевым) законодательством и даже без соблюдения надлежащего терминологического единообразия. Так, фактически в области связи действуют два «конкурирующих» закона со сходными названиями и пересекающимися сферами применения – «Об электрической и почтовой связи» и «О почтовой связи».

Реформирование законодательства в сфере развития сетей связи и использования ресурсов электросвязи не может быть сведено только к «точечным» корректировкам отдельных положений отраслевых (специальных) законов и действующих в отдельных аспектах телекоммуникаций Кодексов и иных Законов Кыргызской Республики. Развитие новых экономических моделей и технологий, в том числе диверсификация услуг, оказываемых операторами связи, требует расширения ресурсной базы и возможностей более эффективного и менее затратного строительства инфраструктуры. В частности, появление технологий 5G, «интернета вещей», беспилотного транспорта (систем искусственного интеллекта), Smart City и других, с неизбежностью ставит вопрос об освоении новых частотных диапазонов, увеличении полос выделяемых операторам радиочастот, недопущении «запретительно

высокой» оплаты за предоставление таких ресурсов. Это также подтверждает, что для обеспечения реальной цифровой трансформации не только экономики, но и всей повседневной жизни страны, деятельности государственных органов Кыргызской Республики, её граждан и бизнеса инфраструктура телекоммуникаций (электросвязи) еще длительное время будет основой для разворачивания соответствующих цифровых платформ, сервисов и услуг. Что, в свою очередь, влечёт за собой необходимость обеспечения приоритетного внимания к нуждам операторов такой инфраструктуры, с изменением подходов к лицензированию их деятельности и выделению им потребных для эффективной работы частотных и иных ресурсов, а также с последовательным облегчением (упрощением) разрешительных процедур для размещения и эксплуатации необходимого оборудования электросвязи.

Международный опыт

Опыт реформирования системы регулирования в сфере электросвязи в разных странах, отличающихся по уровню экономического и технологического развития, достаточно обширен и разнообразен. Наряду с примерами законодательного регулирования сферы телекоммуникаций в соседних странах Центральной Азии, других государствах – членах интеграционных объединений с участием Кыргызской Республики (Евразийский союз, Содружество независимых государств и др.) для выбора оптимальных направлений развития законотворчества в сфере связи (сетей и ресурсов электросвязи) следует использовать опыт развития законодательства Европейского союза, а также таких стран как США, Канада и Австралия. Для гармонизации законодательства Кыргызской Республики с лучшими зарубежными практиками важно изучать и применять рекомендации Международного союза электросвязи и Всемирного банка.

Выводы и рекомендации

Признавая инфраструктуру телекоммуникаций, сетей и ресурсов электросвязи важнейшим фактором (фундаментом) цифровой трансформации Кыргызской Республики, необходимо на основании лучших зарубежных практик и рекомендаций, а также опыта развития телекоммуникационной отрасли страны, пересмотреть подходы к регулированию сферы связи, заложенные в базовый закон КР «Об электросвязи и почтовой связи» более 25 лет назад. В первую очередь необходимо добиться единообразия правовых подходов в общих и специальных законодательных актах Кыргызской Республики, с разных сторон регулирующих вопросы телекоммуникаций.

В частности, требуется:

- обеспечить единство применяемой терминологии и принципов регулирования в сфере электросвязи, создав возможности (эталонную терминологическую базу) для внесения корректирующих изменений во все иные правовые акты;
- устранить дублирование в предметной сфере регулирования разными законодательными актами, а также нормативными актами разного уровня;
- конкретизировать установленные законодательством требования и меры поддержки, направленные на стимулирование развития и внедрения новейших технологий и услуг;
- инвентаризировать и отменить при необходимости устаревшие, потерявшие актуальность или доказавшие неэффективность ограничительные меры и обременения, обращённые на операторов связи и затрудняющие их повседневную деятельность;
- предоставить операторам (организациям) связи недискриминационные условия в части налогообложения, а также доступа к инфраструктуре и ресурсам, контролируемым или предоставляемым государством;

- скорректировать подходы к лицензированию деятельности в сфере электросвязи в соответствии с международной практикой; максимально использовать альтернативные (не связанные с запрашиванием разрешений у государственных органов) способы регулирования, включая уведомительные методы и саморегулирование;
- обеспечить фактическое равенство игроков телекоммуникационного рынка, включая модель сохранения на среднесрочную перспективу национального оператора при соблюдении мер антимонопольного регулирования.

Раздел 17. Межоператорское взаимодействие, сетевая нейтральность

Текущее регулирование (действующее законодательство):

1. Закон КР об электрической и почтовой связи
2. Закон КР о лицензионно-разрешительной системе
3. Закон КР об электронном управлении
4. Закон КР о естественных монополиях в Кыргызской Республике
5. Налоговый Кодекс КР
6. Кодекс Кыргызской Республики о неналоговых доходах
7. Правила межсетевого соединения в Кыргызской Республике (ППКР от 13 августа 2020г. №421)
8. Положение о лицензировании деятельности по использованию радиочастотного спектра (ППКР №754 от 17.11.2017г.)
9. Положение о лицензировании деятельности в области электрической и почтовой связи (ППКР от 31 декабря 2019 года № 746)
10. Положение о порядке взаимодействия операторов мобильной сотовой связи с органами внутренних дел Кыргызской Республики, осуществляющими оперативно-розыскную деятельность по розыску похищенных мобильных устройств (ППКР от 25 марта 2009 г. №192)

Краткое описание выявленных недостатков и ориентиров из мировой практики

№	Описание недостатка	Тип[37]	Лучшая практика
17.1	Ст.30 закона КР об электри-ческой и почтовой связи «Межсетевое соединение (сопряжение)» адресована в основном «доминирующим» операторам, содержит неоднозначную терминологию и не даёт возможности развитию межоператорских отношений на основе равноправных соглашений между операторами, отходя от логики построения телефонных (фиксированных) сетей связи	**Б/У**	Общемировая тенденция в сфере регулирования межоператорских отношений основана на принципе технологической нейтральности при пропуске межсетевого трафика, и отказа от жёстких требований к построению иерархических сетей фиксированной связи, и на снижение тарифов на интерконнект: «операторы должны зарабатывать на своих клиентах, а не на своих конкурентах».
17.2	Правила межсетевого соединения в Кыргызской Республике (Постановление Правительства КР от 13.02.2020) сохраняют логику требований к сетям, функционирующих на основе коммутации каналов, а не маршрутизации пакетов	**Б/У**	Зарубежная практика регулирования (стран Европейского Союза, стран Северной Америки и др.) не ограничивает вопросы межсетевого взаимодействия исключительно сетями «традиционной телефонии»
17.3	Действующее законодатель-ство в сфере связи не содержит положений об устранении (или существенном	**БП/Б**	Роуминговые тарифы в Европейском Союзе фактически обнулены. Обсуждается (но пока не решается) и

[37] В таблице приводятся следующие типы недостатков регулирования:
(П) пробел в регулировании (регулирование требуется, но его нет)
(У) устаревшая норма (норма есть, но её нужно менять)
(Н) неработающая норма (норма есть, но в силу описанных причин она не работает)
(Б) действующая норма является необоснованным препятствием для осуществления деятельности

	сокращении) тарифов на интерконнект, в первую очередь при транс- граничном межоператорском взаимодействии в рамках интеграционных объединений с участием Кыргызской Республики (ЕАЭС, СНГ и др.) – вопрос о снижении (до минимального уровня) ставки интерконнекта и отмены международного роуминга		вопрос об отмене роуминга в странах-членах ЕАЭС.
17.4	Действующее законодательство Кыргызской Республики не содержит норм, обеспечивающих реализацию принципа сетевой нейтральности	**БП**	Законодательство ряда штатов США; Общие правила обеспечения равного и недискриминационного отношения к трафику при предоставлении услуг доступа в Интернет и соответствующих прав конечных пользователей Евросоюза

Комментарии

Законодательство Кыргызской Республики в части регулирования межоператорского взаимодействия (правил присоединения сетей и пропуска трафика) в целом соответствует современному этапу развития телекоммуникационных технологий. Однако оно по-прежнему исходит из «традиционно телефонных» принципов построения сетей связи и фактически не учитывает (точнее, не регулирует) вопросы взаимодействия сетей передачи данных, основанных не на коммутации каналов связи, а на маршрутизации пакетов передаваемой по сетям информации. Оно также нуждается в обеспечении терминологического единообразия по всем нормативным документам и их соответствия международной практике (рекомендациям и документам Международного союза электросвязи). В целом же должен быть осуществлён переход от директивно устанавливаемых правил присоединения сетей к двусторонним (и многосторонним) межоператорским соглашениям по типу SLA (Service Level Agreement).

Отмечается, что одним из основных барьеров развития сетей и предоставления абоненту более доступной связи является высокий тариф на пропуск межсетевого трафика. Мировая тенденция на сегодняшний день заключается в снижении тарифов на интерконнект и обеспечении технологической нейтральности при пропуска межсетевого трафика. Самой яркой иллюстрацией сложившейся ситуации является стремление абонентов «уходить» от обременительных сценариев использования инфраструктуры телекома путём использования различных мобильных и иных приложений (OTT-сервисы). Это также ставит вопрос о целесообразности урегулирования вопросов взаимодействия операторов связи и провайдеров OTT-сервисов по аналогии с межоператорским взаимодействием между лицензируемыми операторами связи.

Дальнейшим следствием урегулирования межоператорского взаимодействия на национальном уровне станет возможна отмена роуминговых платежей для абонентов в странах – участницах интеграционных объединений с участием Кыргызской Республики. Так, для создания благоприятных условий для общения и обмена информацией между гражданами государств - членов ЕАЭС, обсуждалась комплексная реформа межоператорского взаимодействия операторов-партнеров путем снижения межоператорских роуминговых ставок и ставок на услуги завершения вызова. Такое решение позволит снизить абонентские тарифы на услуги связи в роуминге до уровня, сопоставимого с условиями домашнего региона («в роуминге как дома»). Это показал и опыт Российской Федерации по отмене национального роуминга, который был признан в 2019 г. лучшей мировой практикой в сфере цифровой экономики.

Отдельной проблемой, требующей решения в рамках корректировки законодательства Кыргызской Республики о цифровой трансформации, является реализация принципа сетевой нейтральности, заключающегося, по общему правилу, в недопустимости дискриминации обслуживания клиентов в зависимости от типа передаваемого по сети трафика. Эту проблему следовало бы понимать в максимально широком смысле. Так, первоначально законодательство США о соблюдении принципов сетевой нейтральности базировалось на следующих элементах: защита прав потребителей, прозрачность, устранение избыточных требований для поощрения инвестиций в широкополосную сеть. В Европейском Союзе этот принцип нашёл своё отражение в Регламенте по открытому доступу в Интернете от 25 ноября 2015 г.№ 2120 «Общие правила обеспечения равного и недискриминационного отношения к трафику при оказании услуг доступа в Интернет и соответствующих прав конечных пользователей».

Международный опыт

Вопросы межоператорского взаимодействия достаточно детально изложены в рекомендациях Международного союза электросвязи. Кроме того, положительным примером регулирования в этой сфере является законодательство Европейского союза и входящих в него государств.

Применительно к сокращению тарифов на интерконнект и потенциальной отмены международного роуминга можно воспользоваться практикой стран Евросоюза, а также опытом Российской Федерации по устранению отмене национального роуминга. Наконец, следует проанализировать ход и причины неудач в обсуждении подобного рода вопросов на уровне Евразийского союза.

По вопросам сетевой нейтральности представляется оптимальным следовать Регламенту Евросоюза по открытому доступу в Интернет, где указывается, что «конечные пользователи имеют право получать доступ и распространять информацию и контент, использовать и предоставлять приложения и услуги, а также использовать оконечное оборудование по своему выбору, независимо от местоположения конечного пользователя или поставщика услуг или местоположения, происхождения или назначения информации, контента, приложения или услуги через свою службу доступа в Интернет». Особое значение указанный принцип имеет в условиях предстоящего внедрения технологий искусственного интеллекта (ИИ) и разработки соответствующего законодательства.

Выводы и рекомендации

Исходя из адекватного (в целом) уровня регулирования вопросов межоператорского взаимодействия в законодательстве Кыргызской Республики предлагается, помимо необходимости уточнения и обеспечения применяемого терминологического аппарата, сосредоточиться на регламентировании вопросов, в отношении которых сейчас есть пробелы в регулировании**, а именно:**

- межоператорское взаимодействие в отношении сетей (передачи данных), основанных на маршрутизации пакетов передаваемой по ним информации;
- порядок использования сетей операторов связи поставщиками OTT-сервисов;
- стимулирование снижения тарифов интерконнекта;
- создание условий для отмены международного роуминга в странах интеграционных объединений с участием Кыргызской Республики;
- последовательная реализация принципа сетевой нейтральности.

Раздел 18. Услуги электросвязи (права и обязанности пользователей и операторов; надзор и контроль)

Текущее регулирование (основные акты действующего законодательства):

1. Закон КР об электрической и почтовой связи
2. Закон КР о почтовой связи
3. Закон КР о лицензионно-разрешительной системе
4. Закон КР об электронном управлении
5. Закон КР о нормативных правовых актах Кыргызской Республики
6. Закон КР о защите прав потребителей
7. Закон КР о порядке проведения проверок субъектов предпринимательства
8. Налоговый Кодекс КР
9. Кодекс Кыргызской Республики о неналоговых доходах
10. Кодекс КР «О правонарушениях»
11. Положение о лицензировании деятельности по использованию радиочастотного спектра (ППКР №754 от 17.11.2017г.)
12. Положение о лицензировании деятельности в области электрической и почтовой связи (ППКР от 31 декабря 2019 года № 746)
13. Национальная система и план нумерации сетей электросвязи Кыргызской Республики (ППКР от 9 января 2018 года №10)
14. Правила оказания услуг подвижной радиотелефонной связи (ППКР от 17 февраля 2014г. №97)
15. Положение о порядке взаимодействия операторов мобильной сотовой связи с органами внутренних дел Кыргызской Республики, осуществляющими оперативно-розыскную деятельность по розыску похищенных мобильных устройств (ППКР от 25 марта 2009г. №192)

Краткое описание выявленных недостатков и ориентиров из мировой практики

№	Описание недостатка	Тип[38]	Лучшая практика
18.1	Статья 4 закона КР об электрической и почтовой связи содержит многочисленные полномочия органов власти, которые в реальности почти не реализованы в виде нормативных правовых актов (документов стратегического планирования)	**Н**	Типовой закон об электронных коммуникациях для стран Восточного партнёрства (ст.5) рекомендует наделить регулятора полномочиями законодательной инициативы. Такая рекомендация может быть реализована в рамках действующих конституционно-правовых механизмов КР
18.2	Статьи 5 и 6 закона КР об электрической и почтовой связи требуют внесения изменений в части приведения в соответствие с текущей системой органов власти КР	**У**	Подлежащие внесению изменения должны учитывать независимый статус регулятора в области электросвязи (см.ниже)
18.3	Статья 7 закона КР об электрической и почтовой связи «Уполномоченный	**Б/У**	Международные институты рекомендуют независимость

[38] В таблице приводятся следующие типы недостатков регулирования:
(П) пробел в регулировании (регулирование требуется, но его нет)
(У) устаревшая норма (норма есть, но её нужно менять)
(Н) неработающая норма (норма есть, но в силу описанных причин она не работает)
(Б) действующая норма является необоснованным препятствием для осуществления деятельности

	государст- венный орган по связи» не предусматривает создания независимого регулятора		регулирующих органов от политических властей. Так, Руководство по регулированию электросвязи проекта Infodev Всемирного банка и МСЭ однозначно указывает: полностью оправдано усиление степени независимости регулирующих органов по отношению к органы государственной власти. Эта независимость является гарантом нейтралитета, (…) и определенного иммунитета от политического (…) давления. Такое восприятие независимости особенно важно, когда государство сохраняет за собой в собственности государственного оператора связи.
18.4	Статья 9-3 закона КР об электрической и почтовой связи «Выбор поставщика услуг» на практике не применяется (потеряла актуальность в связи с развитием таких технологий, как интернет-мессенджеры)	**Б/У**	Исключить из закона
18.5	Статья 24 закона КР об электрической и почтовой связи «Предоставление услуг связи в сетях связи общего пользования» содержит многочисленные мелочные и малооправданные положения, не соответствующие современной практике договорного закрепления условий оказания услуг связи	**Н/У**	Подобного рода нормы должны содержаться в подзаконных актах («Правилах оказания услуг») или вообще быть исключены
18.6	Ст.26 закона КР об электрической и почтовой связи содержит устаревшие ссылки на полномочия органов власти в сфере защиты прав потребителей	**У**	Типовой закон об электронных коммуникациях для стран Восточного партнерства
18.7	Действующее законодательство Кыргызской Республики не содержит положений о реально независимом статусе регулятора в сфере электросвязи	**П/Б/У**	Международный опыт (в том числе в бывших республиках СССР) свидетельст- вует о желательности и необходимости обеспечения независимого статуса регу-лирующего органа в сфере электросвязи

Комментарии

В законодательстве Кыргызской Республики вопросы, относящиеся к регулированию услуг связи, правам и обязанностям пользователей (абонентов) и операторов (поставщиков) услуг электросвязи в целом решены на достаточно удовлетворительном уровне, без тех особенностей и неопределённости регулирования, которые в последние годы стали характерны для телекоммуникационного законодательства ряда бывших республик СССР. В то же время остаются открытыми (требующими нормативного уточнения) вопросы не сколько об объёме правомочий и обязанностей операторов связи, а о том, кто именно и по каким критериям может или должен быть отнесён к числу операторов. Это возвращает проблематику правового регулирования услуг связи к более фундаментальным вопросам – о принципах лицензионно-разрешительной деятельности в области электросвязи, о стимулировании развития и потребления новых услуг, создающих добавленную стоимость, а также о порядке взаимодействия между сетями электросвязи лицензированных операторов и техническими средствами владельцев OTT-сервисов. Вышесказанное не исключает целесообразности внесения редакционных изменений в законодательные акты, устраняющих терминологический разнобой и внутреннюю несогласованность между различными нормативными документами.

В части осуществления надзора и контроля наиболее актуальной остаётся проблема функционирования национального регулятора в области связи как независимого органа. Изначальный замысел Закона Кыргызской Республики об электросвязи и почтовой связи (1997 г.) о порядке формирования и функционирования такого регулятора (Национального агентства связи) к настоящему моменту потерял актуальность. В 2009 году структура Правительства Кыргызской Республики изменилась и Национальное агентство связи было преобразовано в Государственное агентство связи при Правительстве КР. Таким образом регулятор утратил свой независимый статус и был переведён подчинение Правительства. Кроме того, в 2009 году был принят Закон КР нормативных правовых актах Кыргызской Республики, которым устанавливалось, что нормативные правовые акты, принятые (изданные) государственными органами, не являющимися согласно данному Закону нормотворческими органами, действуют до 31 декабря 2010 года при условии их государственной регистрации в органах юстиции до вступления в силу этого Закона. Попало под запрет внесение изменений и дополнений в нормативные правовые акты, принятые (изданные) государственными органами, не являющимися нормотворческими органами. Таким образом, вся нормативная база, наработанная Национальным агентством связи, утратила силу. В результате изменений требовалась разработка или переутверждение нормативных актов, регулирующих отрасль связи. Согласно Закону об НПА государственное агентство связи не обладало полномочиями нормотворчества, в связи с чем все нормативные проекты запускались через Министерство транспорта и коммуникаций КР. Процедура принятия значимых решений замедлилась в силу специфики отрасли, которая не всегда была понятна всем государственным органам, принимающим участие в согласовании проектов НПА.

В 2016 году Функции министерства транспорта и коммуникаций в части, касающейся телекоммуникаций, были переданы вновь образованному Государственному комитету информационных технологий и связи Кыргызской Республики. Государственное агентство связи при Правительстве Кыргызской Республики потеряло еще одну ступень и было преобразовано в Государственное агентство связи при Государственном комитете информационных технологий и связи Кыргызской Республики. При этом, потеряло функции полноценного антимонопольного регулирования, надзора и контроля. В 2021 году Государственное агентство связи при Государственном комитете информационных технологий и связи Кыргызской Республики было переименовано в Службу по регулированию и надзору в отрасли связи при Министерстве цифрового развития Кыргызской Республики. При этом независимым регулятором, обладающим законодательной инициативой, полномочиями в сфере антимонопольного регулирования, эффективного надзора и контроля он не обладает.

Международный опыт

Поскольку, как уже указывалось выше, вопросы регулирования услуг связи и субъектного состава соответствующих правовых отношений урегулированы в законодательстве Кыргызской Республики достаточно адекватно, предложения в этой сфере (помимо юридико-технических и редакционных аспектов) должны быть адресованы в нормативные акты, касающиеся проблематики лицензирования в сфере связи, защиты прав потребителей и т.д. Ориентиром здесь могут служить как рекомендации Международного союза электросвязи («Справочник по цифровому регулированию») и Модельный закон об электронных коммуникациях для стран Восточного партнёрства.

Более серьёзным является вопрос об обеспечении статуса независимого регулятора в сфере электросвязи. Основываясь на опыте государств Евросоюза, а также таких стран со схожими с Кыргызской Республикой историческими традициями государственного регулирования, как Молдова, Грузия и Украина, можно сформулировать такой сценарий преобразования регулирующего органа в сфере электросвязи, который бы полностью соответствовал конституционным нормам Кыргызской Республики, и в то же время учитывал бы лучшие мировые практики в этой области. Как указано в аналитическом исследовании Восточного партнёрства (EU4 Digital, декабрь 2020 г.), для этого необходимо принять политические решения и закрепить их в нормативном документе: (1) о независимом статусе регулятора, (2) о порядке формирования его управляющего органа, (3) о порядке разрешения споров и, безусловно (4) о полномочиях в регулируемой сфере.

Выводы и рекомендации

С учётом в целом удовлетворительного уровня регулирования вопросов оказания услуг связи и правового статуса операторов электросвязи и их абонентов (пользователей) оптимизация соответствующей нормативной базы видится скорее **в уточнении перечня собственно лицензируемых видов деятельности, критериев отнесения хозяйствующих субъектов к операторам связи, а также порядка их взаимодействия с владельцами OTT-сервисов (новых интернет-услуг).** При этом нормативная база в этой сфере, тем не менее, нуждается в аккуратном обновлении, направленном на устранении терминологических неточностей и внутренней несогласованности.

Принципиальным вопросом повышения эффективности системы надзора и контроля в сфере электросвязи является внесение изменений в законодательство, направленных на **обеспечение независимости регулятора в этой сфере, в соответствии с общемировой практикой.** Независимость регулирующего органа в сфере электросвязи является важнейшим фактором повышения взаимного доверия и плодотворного взаимодействия между государственными и негосударственными организациями в области цифровой трансформации.

Раздел 19. ГЧП в условиях цифровой трансформации

Содержание

- объекты ГЧП (информсистемы, информресурсы, технологические системы и телекоммуникационные сети)
- особый порядок использования и монетизации объектов ГЧП

Текущее регулирование (действующее законодательство):

1. Бюджетный кодекс Кыргызской Республики;
2. Закон Кыргызской Республики «О государственно-частном партнерстве» от 11 августа 2021 года № 98
3. Постановление Правительства Кыргызской Республики «Об определении уполномоченных органов в сфере государственно-частного партнерства» от 14 сентября 2012 года № 616;
4. Постановление Правительства Кыргызской Республики «О финансировании подготовки проектов государственно-частного партнерства» от 17 марта 2014 года № 147;
5. Постановление Правительства Кыргызской Республики «Об образовании Совета по государственно-частному партнерству в Кыргызской Республике от 16 июня 2016 года № 328;
6. Постановление Правительства Кыргызской Республики «О некоторых вопросах в сфере государственно-частного партнерства» от 21 февраля 2020 года № 111

Краткое описание выявленных недостатков и ориентиров из мировой практики

№	Описание недостатка	Тип[39]	Лучшая практика
19.1	Закон о ГЧП не допускает включение в другие законы нормы, предметом регулирования которых является Закон о ГЧП (статья 2). При этом ни в Законе, ни в Бюджетном кодексе процедуры применения бюджетных инвестиций не предусматриваются, а устанавливаются отдельным решением в виде НПА о ГЧП в каждом случае индивидуально, что, во-первых, значительно усложняет принятие решение о каждом новом проекте ГЧП, во-вторых, подвергает большому риску использования бюджетных средств не по целевому назначению	**Н**	Закон о ГЧП не может ограничивать правовое регулирование норм, предусматривающих общественные отношения в сфере ГЧП в разных нормативных правовых актах. Соответственно предлагается не ограничивать предмет регулирования ГЧП в иных законодательных актах Кыргызской Республики. Специфика проектов ГЧП в силу социально-экономического развития Кыргызской Республики и существующих проблем, и задач в различных сферах общества исключают систематизацию нормативной правовой базы по вопросам ГЧП в один Закон.

39 В таблице приводятся следующие типы недостатков регулирования:
(П) пробел в регулировании (регулирование требуется, но его нет)
(У) устаревшая норма (норма есть, но её нужно менять)
(Н) неработающая норма (норма есть, но в силу описанных причин она не работает)
(Б) действующая норма является необоснованным препятствием для осуществления деятельности

			Законодательство зарубежных стран определяет отношения в сфере ГЧП как сотрудничество между государственным и частным инвестором в целях разработки и реализации проектов по созданию и/или модернизации, эксплуатации и содержанию инфраструктурных объектов и/или инфраструктурных услуг. Задачи, которые стоят перед ГЧП предполагают наличие законодательных норм, касающихся разных сфер инвестиционных проектов: - (повышение эффективности и качества создания инфраструктурных объектов и предоставления инфраструктурных услуг; - повышение эффективности государственных расходов на проектирование, строительство и/или модернизацию, эксплуатацию, содержание инфраструктурных объектов и предоставление инфраструктурных услуг; - привлечение инвестиций в экономику страны; вовлечение дополнительного управленческого потенциала частного сектора; - достижение оптимального соотношения цены в течение жизненного цикла активов и качества или соответствия их назначению при реализации инфраструктурных проектов; - использование инноваций и эффективности частного сектора; стимулирование роста и развития новых технологий).
19.2	В законе не описаны виды финансовой поддержки со стороны государства, а также правила распределения рисков между государственным и частным партнерами, что является обязательным условием проекта ГЧП (в целях защиты имущества, невмешательства со стороны государственного партнера, право на возмещение убытков и т.д.)	**П**	Предлагается внести дополнения в Закон, в части определения видов государственных гарантий, видов рисков, сроки, на каком этапе частный партнер может рассчитывать на компенсацию убытков и т.д. В зарубежных странах при реализации проектов ГЧП используются различные механизмы сотрудничества государства и

			частного бизнеса. В зависимости от объема и условий сотрудничества, обязательств сторон, принципов разделения рисков между партнерами, ответственности за проведение различных видов работ механизмы ГЧП меняются. Статьей 36 Закона о ГЧП Республики Беларусь установлено, что частному партнеру предоставляются гарантии прав, предусмотренные законодательством Республики Беларусь. Не допускается вмешательство в деятельность частного партнера, за исключением случаев, когда такое вмешательство предусмотрено законодательными актами в интересах национальной безопасности, общественного порядка, защиты нравственности, здоровья населения, прав и свобод других лиц; • частному партнеру гарантируется защита имущественных и иных прав, приобретенных и осуществляемых им в соответствии с соглашением о ГЧП; • после уплаты установленных законодательством Республики Беларусь налогов, сборов (пошлин) и иных обязательных платежей в бюджет иностранному частному партнеру гарантируется беспрепятственный перевод за пределы Республики Беларусь прибыли и иных правомерно полученных денежных средств, связанных с исполнением соглашения о ГЧП.
19.3	В существующем законе КР отсутствуют механизмы, обеспечивающие конкуренцию и создание равных и справедливых условия для всех участников процесса прохождения отбора конкурса, и как следствие нарушение принципов ГЧП (прозрачности деятельности, справедливости, справедливого распределения рисков) при отборе победителя конкурса	**Б**	В зарубежной практике не встречаются правила, согласно которым для проведения квалификационного отбора достаточно подачи одной заявки на участие в квалификационном отборе**.** Наибольшее распространение механизм отбора или тендеров получил в странах ЕАЭС, в которых допускается применение одноэтапных, двухэтапных, закрытых отборов

19.4	Хотя в Законе КР упоминается возможность присуждения проекта ГЧП путем прямых переговоров, сама процедура проведения прямых переговоров отсутствует	**П**	Предлагается дополнить Закон статьей об условиях прямых переговоров и перечне направлений, по которым возможно заключение соглашения о ГЧП путем прямых переговоров. Например, Закон Республики Казахстан от 31 октября 2015 года № 379-V «О государственно-частном партнерстве» предусматривает, что частный партнер определяется на основании прямых переговоров регулятором по государственному планированию, и применяется в случаях, когда: 1) проект государственно-частного партнерства инициирован потенциальным частным партнером в отношении объекта, находящегося у него на правах собственности или долгосрочной аренды; 2) проект государственно-частного партнерства неразрывно связан с реализацией исключительных прав на результаты интеллектуальной творческой деятельности, принадлежащих потенциальному частному партнеру. Определение частного партнера на основании прямых переговоров осуществляется посредством следующих последовательных стадий: 1) инициирование проекта государственно-частного партнерства потенциальным частным партнером; 2) извещение об инициировании проекта ГЧП с указанием основных технико-экономических параметров проекта ГЧП и запрашиваемых выплат из бюджета и (или) мер государственной поддержки; 3) экспертиза бизнес-плана к проекту ГЧП; 4) проведение переговоров между потенциальными сторонами договора государственно-частного партнерства об условиях договора государственно-частного партнерства; 5)заключение договора государственно-частного артнерства

Комментарии

Исходя из обзора международной практики и анализа законодательства и развития ГЧП в Кыргызской Республике, определены следующие проблемы:

1. Отсутствует четкая стратегическая программа развития ГЧП с приоритетными секторами инфраструктурных объектов и инфраструктурных услуг в Кыргызской Республике.
2. Отсутствие информированности граждан (частного сектора) и понимания механизмов ГЧП (одним из способов повышения эффективности законодательства является лучшее информирование населения о правах на получение качественных услуг, о возможностях участвовать в процессе принятия решений. Пока проект ГЧП находится еще на стадии планирования и разработки, Кабинет Министров Кыргызской Республики должен создать механизмы участия общественности и организовать группы населения, которые бы их использовали, иначе это право не будет реализованным).
3. Низкое качество и недостатки Закона Кыргызской Республики «О государственно-частном партнерстве» и других нормативных правовых актов, регулирующих сферу ГЧП, ограничивают заинтересованность потенциальных инвесторов. К основным недостаткам относятся: противоречия нормативных правовых актов, внутренние коллизии, пробелы нормативных правовых актов; наличие дискреционных полномочий в нормах Закона; нарушение принципов ГЧП - прозрачности, конкуренции, справедливости при отборе победителя (участие одного конкурсного предложения и его же отбор); высокая степень коррупциогенности норм Закона.

Таким образом, в первоочередном порядке необходимо привести в соответствие все законы и нормативные правовые акты, регулирующие вопросы ГЧП, поскольку несовершенство правового регулирования вопросов ГЧП не позволит полноценно инициировать проекты ГЧП со стороны иностранных инвесторов.

Для потенциального инвестора требуется предсказуемая и надежная нормативно-правовая база, т.е. меньшее количество, простота и качество норм. Кроме того, нормативно-правовая база должна учитывать интересы получателей услуг (частных партнеров) и давать им возможность участвовать в юридических процедурах, защищающих их права и гарантирующих им доступ к процессу принятия решений.

В большинстве случаев, инвесторы предпочитают работать в тех странах, где достаточно опираться на общее законодательство, а не на акты, регулирующие отношения в определенном секторе, при реализации проектов, например, в области транспорта или образования, поскольку общим законодательством затрагиваются интересы большего числа участников и меньше вероятность возникновения проблем в результате изменения законов.

Практика показывает, что гораздо проще вносить изменения в руководства, инструкции и другие регулирующие акты, нежели в законы, поскольку один документ, регулирующий ГЧП может быть более гибким и лояльным. В то время как отраслевое регулирование может быть противоречивым и затрудняющим деятельность инвесторов, поскольку внесение поправок в законы очень длительный процесс.

Однако, специфика проектов ГЧП в силу социально-экономического развития нашей страны и существующих проблем и задач в различных сферах общества исключают систематизацию нормативной правовой базы по вопросам ГЧП в один Закон.

Учитывая, что для создания основ цифровой экономики в Кыргызской Республике, в части определения объектов ГЧП направленных на цифровую трансформацию информационных систем, информационных ресурсов, технологических систем и телекоммуникационных сетей, необходимо принимать во внимание особенности сферы ИКТ. Специфика развития информационных технологий и постоянно растущего объёма элементов базы данных не может быть предметом соглашения о ГЧП финансируемого за счет государственного бюджета (при отсутствии бюджетных средств), поскольку необходимо

постоянное непрерывное совершенствование и модернизация ИКТ систем, и возможности этого процесса могут быть объектом долгосрочной поддержки частных инвестиций нежели государства. И в этой связи, предлагается разработать эффективный Закон о ГЧП в сфере ИКТ и предусмотреть его отдельным нормативным правовым актом.

Данный нормативный акт должен создать новую платформу взаимодействия между государством и частным сектором, для построения «умного партнерства», результатом которого станет повсеместное внедрение проектов ГЧП с новейшими цифровыми решениями и инновациями в стране.

Международный опыт

Популярность ГЧП в конкретной стране зависит от моделей взаимодействия государства с частными инвесторами. Основное условие взаимодействия — это доброжелательное законодательство по отношению к бизнесу. Наибольшее распространение механизм партнерства получил в странах англосаксонской правовой системы, которая допускает применение ГЧП в малых и средних проектах.

В зависимости от уровня социально-экономического развития страны использование ГЧП по странам отличается друг от друга. В странах «Большой семерки» на первом месте — здравоохранение, на втором — образование, на третьем — автомобильные дороги. Например, в США наиболее приоритетной отраслью являются автодороги, в Великобритании — здравоохранение и образование, в Германии — образование, в Италии, Канаде и Франции — здравоохранение.

Лидирующей отраслью по использованию успешно завершенных проектов ГЧП- по таким странам как Австрия, Бельгия, Дания, Австралия, Израиль, а также Ирландия, Финляндия, Испания, Португалия, Греция, Южная Корея, Сингапур и др., является строительство дорог и только потом — образование и здравоохранение. Такая закономерность использования проектов ГЧП по отраслям прослеживается и в странах с переходной экономикой, и в развивающихся странах: чем дальше страна находится по уровню своего развития от уровня стран «Большой семерки», тем больше проектов ГЧП реализуется по строительству дорог, тоннелей и мостов, аэропортов и тюрем.

Таким образом, в развивающихся странах и странах с переходной экономикой ГЧП в отраслях здравоохранения и образования (в отличие от автодорог) не будут приоритетными. Учитывая более низкий уровень экономического развития в этих странах, на первое место по приоритетности привлечения инвестиций с помощью ГЧП должна выйти транспортная инфраструктура. В таких странах, как Центральная и Восточная Европа (Болгария, Чехия, Венгрия, Хорватия, Польша, Румыния), Балтии (Латвия) и СНГ (Украина) по применению ГЧП лидируют автодороги, строительство мостов и тоннелей, легкого наземного метро, аэропортов.

В Индии, Бразилии, Чили, Гонконге, Мексике, Саудовской Аравии, Объединенных Арабских Эмиратах, как и в вышеперечисленных странах на первом месте по количеству проектов ГЧП стоят автодороги, на втором месте — аэропорты, тюрьмы и водоочистные сооружения.

При изучении опыта отдельных государств установлено, что неоспоримым лидером в области применения механизмов ГЧП на протяжении долгого временного периода считалась Великобритания, поскольку именно это государство лидирует и по общему числу проектов, и по охвату ГЧП различных сфер и отраслей.

Британское правительство активно использует на практике концепцию взаимодействия и партнерства между частным бизнесом и государством в виде ГЧП – для привлечения частных инвестиций в обеспечение развития инфраструктуры и предоставление услуг, что влечет за собой снижение финансовой нагрузки на бюджет государства. ГЧП применяется в тех случаях, когда частные компании могут выполнять государственные задачи, причем также хорошо, а порой и лучше, чем само государство.

Такое повышение эффективности достигается путем распределения рисков и задач, применения принципа жизненного цикла, улучшения инструментов стимулирования.

В **Германии** одной из основных сфер применения ГЧП являются информационно-коммуникационные технологии (далее - ИКТ), которой придается большая роль в процессе трансформирования национальной экономики из индустриальной в информационную. Роли участников ГЧП распределяются следующим образом: правительство создает условия для развития ИКТ путем принятия рамочного законодательства и проведения стимулирующей экономической политики, а частный сектор обеспечивает инвестирование в научно-исследовательские и опытно-конструкторские работы (далее - НИОКР) в области ИКТ, внедрение ИКТ в отраслях внутреннего хозяйства и во внешнеторговых операциях.

В **Дании** финансирование проектов по строительству социального жилья осуществляется на принципах ГЧП: местные власти предоставляют застройщику государственный беспроцентный заем, который возвращается им в течение 50 лет.

В **КНР** сфера ГЧП является в настоящее время достаточно широко распространенной практикой, но применяемой преимущественно в сфере развития инфраструктуры (строительство дорог и скоростных магистралей, мостов, учебных заведений и т.д.). При этом механизмы ГЧП реализуются с использованием таких организационно-проектных форм, как контракты и концессии.

Примером практики цифрового ГЧП является проект «ГЧП пятого поколения» в Европе. Государство создает необходимую физическую инфраструктуру методом государственного заказа, а затем передает право пользования инфраструктурой в формате концессии. Следует отметить, что если в традиционной концессии на объект может претендовать только один концессионер, то в случае «цифрового ГЧП» количество концессионеров ограничено только пропускной возможностью сети.

Если говорить о странах СНГ, **то в Российский Федерации** (далее-РФ) зарождение института ГЧП начинается с 2004 года и связано оно с инфраструктурными проектами.

В 2015 г. был принят Закон о ГЧП РФ, который позволил использовать новые и эффективные модели ГЧП в российской практике. Специальное законодательство о ГЧП состоит из Закона о ГЧП, Закона о концессионных соглашениях (Закон о КС), других нормативных правовых актов РФ, а также нормативных правовых актов ее субъектов. Однако, как следует из Закона о ГЧП, все правовые нормы в сфере ГЧП, содержащиеся в других нормативных правовых актах России должны соответствовать Закону о ГЧП и Закону о КС.

Указанными законами предусмотрена возможность передавать отдельные права и обязанности публичного партнера (концедента) иным лицам (государственным органам, органам местного самоуправления, а также юридическим лицам).

Наиболее успешный пример ГЧП в сфере телекоммуникаций РФ - это «электронное правительство» в городе-спутнике Москвы - Зеленограде. В «виртуальный город» входит несколько десятков баз данных и многочисленные сервисы - служба «одного окна», тематических SMS-оповещений, интернет-опросов, навигационная система городского транспорта, электронный документооборот. В Поволжье реализуются ряд проектов «ЭРТелеком Холдинга» по подключению к Интернету школ, городских систем видеонаблюдения и мониторинга объектов ЖКХ.

24 апреля 2017 года внесены поправки в Федеральный Закон «О государственно-частном партнерстве, муниципально-частном партнерстве в Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации» и «О концессионных соглашениях», **признающие ИТ-системы объектами ГЧП и концессии** – ранее таковыми признавались только объекты недвижимого имущества. Так, согласно пункту 1 статьи 33.1, частный партнер обязуется создать объект соглашения, а затем осуществлять его эксплуатацию, а публичный партнер предоставляет частному права пользования результатами интеллектуальной деятельности. При этом не ясно, может ли создание программного обеспечения и баз данных считаться объектом соглашения о ГЧП. Также обязательными условиями соглашения является создание объекта соглашения частным партнером и осуществление им полного или частичного финансирования создания объекта соглашения, а также эксплуатация и техническое обслуживание объекта частным партнером.

В Казахстане основным двигателем развития и реализации ИКТ проектов ГЧП на республиканском уровне является проект государственной программы «Цифровой Казахстан», в котором ряд проектов предусмотрен для реализации через механизм ГЧП. Постановлением Правительства Республики Казахстан в 2016 году Национальный инфокоммуникационный холдинг «Зерде» определен Национальным институтом развития в области ИКТ (далее – НИР), одной из задач которого является привлечение и осуществление инвестиций в индустриально-инновационные проекты в области ИКТ, путем участия в уставных капиталах субъектов индустриально-инновационной деятельности, создания юридических лиц, в том числе с иностранным участием.

Холдинг «Зерде» является крупнейшей компанией и лидером в области ИКТ Республики Казахстан, проводит большую работу по привлечению прямых инвестиций через механизм ГЧП. Участие инвесторов в ИКТ проектах, через механизм ГЧП позволяет государству сэкономить бюджетные средства и привлечь трансферт передовых технологий, обеспечивая решение важных задач в области цифровизации традиционных отраслей в долгосрочной перспективе.

В качестве примеров можно назвать проекты по созданию интеллектуальной транспортной системы, проекты в области медицины, ряд проектов по «Smart city» и многие другие. Интеллектуальная транспортная система будет создана в целях повышения эффективности управления транспортно-дорожным комплексом на республиканском уровне. Это будет единая платформа, объединяющая посредством интеграционной шины комплекс взаимосвязанных автоматизированных систем по решению задач управления дорожным движением, мониторинга и управления работой всех видов транспорта, информирования граждан, перевозчиков, предприятий, государственных органов об организации транспортного обслуживания на территории города, региона, страны.

Основной целью построения «Smart city» или «умного города» является повышение общей удовлетворенности жизнью горожан за счет совершенствования инфраструктуры города Астаны, а также выработки единого подхода устойчивого развития города Астаны путем внедрения принципов и механизмов «умного города». «Smart city» оптимально использует ИКТ для повышения качества жизни, конкурентоспособности экономики, создания необходимой инновационной, энергоэффективной инфраструктуры, разработки международных конкурентоспособных продуктов и услуг для местных и иностранных туристов и обеспечения устойчивого ее развития.

Раздел 20. Связанные изменения в ГК

Содержание

- вопросы подписания и исполнения сделок и договоров присоединения в цифровой форме,
- обеспечение прав на цифровые активы,
- проведение сделок с такими активами, платежи в электронной форме.

Текущее регулирование (действующее законодательство):

1. Гражданский Кодекс Кыргызской Республики
2. Закон Кыргызской Республики «Об электронной подписи»
3. Закон Кыргызской Республики «О виртуальных активах»
4. Закон Кыргызской Республики «О введении в действие Налогового кодекса Кыргызской Республики»
5. Закон Кыргызской Республики «О нотариате»

Краткое описание выявленных недостатков и ориентиров из мировой практики

№	Описание недостатка	Тип[40]	Лучшая практика
20.1	В Гражданском кодексе не обозначено такое определение, и не упомянут смарт-контракт, то есть совершение или исполнение сделки с помощью цифровых технологий. Также совершенно отсутствуют такие понятия, как: - криптовалюта, - блокчейн, - майнинг, - токены. Необходимо закрепление в Гражданском кодексе понятий, отталкиваясь от которых, возможно было бы осуществлять работу рынка существующих в информационно-телекоммуникационной сети новых объектов экономических отношений («токены», «криптовалюта», «майнинг» и т.д.).	**П**	Члены Сената и Ассамблеи Калифорнии одобрили законопроект, который позволит ввести *блокчейн, смарт-контракты* и связанные с ними технологии в правовое поле. В Российской Федерации был принят проект Федерального Закона *«О цифровизации финансовых активов»*, согласно которому будут урегулированы отношения, возникающие при создании, выпуске, хранении и обращении цифровых финансовых активов, а также осуществлении прав и исполнении обязанностей по смарт-контрактам. В проекте данного закона четко определены цифровые понятия, особенности работы криптовалюты, цифровых обращений и подобные вопросы. Республика Беларусь к вопросу внедрения цифровизации права в гражданское законодательство подошла более кардинально. Не менее важными представляются изменения, которые были внесены в законодательство Белоруссии. Белоруссия стала первой в мире страной, которая законодательно закрепила смарт-контракт. Президент

[40] В таблице приводятся следующие типы недостатков регулирования:
(П) пробел в регулировании (регулирование требуется, но его нет)
(У) устаревшая норма (норма есть, но её нужно менять)
(Н) неработающая норма (норма есть, но в силу описанных причин она не работает)
(Б) действующая норма является необоснованным препятствием для осуществления деятельности

			Беларуси утвердил *Декрет «О развитии цифровой экономики»*, где смарт контракт является самостоятельным гражданско-правовым договором. Помимо этого, было подписано Постановление Национального Банка Беларуси *«О совершении и (или) исполнении юридически значимых действий посредством смарт-контрактов»*.
20.2	В настоящее время ГК КР предусматривает, что к объектам гражданских прав относятся вещи, включая деньги и ценные бумаги, иное имущество, в том числе имущественные права; работы и услуги; охраняемая информация, результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации (интеллектуальная собственность), а также другие материальные и нематериальные блага. В связи с этим не определен гражданско-правовой режим цифровых прав и виртуальных активов	**У**	В Российской Федерации был принят проект Федерального Закона «О цифровых финансовых активах», согласно которому будут урегулированы отношения, возникающие при создании, выпуске, хранении и обращении цифровых финансовых активов, а также осуществлении прав и исполнении обязанностей по смарт-контрактам. Помимо этого, Федеральным Законом «О внесении изменений в части первую, вторую, и статью 1124 части третьей Гражданского кодекса Российской Федерации» были внесены изменения в ГК РФ, в соответствии с которыми в ГК РФ появилось понятие Цифровые права и обязанности; сделка, совершенная с помощью электронных либо иных технических средств, исполнение некоторых обязательств путем применения информационных технологий, определенных условиями сделки и т.д. В швейцарском кантоне Цуг с 2021 года можно платить налоги в криптовалюте - налоговые отчисления будут приниматься в биткоинах и эфирах. С 7 сентября 2021 г. в Сальвадоре вступил в силу закон о наделении первой криптовалюты биткоина статусом законного платежного средства наравне с долларом США. В Японии криптовалюты получили в определенной части статус платежного средства, которое может использоваться любым признающим его лицом для осуществления платежей за товары, работы, услуги

			во взаимоотношениях с неопределенным кругом лиц. В Бразилии установлено достаточно широкое определение цифровой валюты, в силу чего криптовалюты вроде биткоина вполне подпадают под соответствующее понятие и регулирование.
20.3	В ГК КР необходимо поименовать смарт-контракты, как самоисполняемую сделку, дав четкое определение данному виду договоров.	**П**	Помимо США, Российской Федерации, Беларуси и ряда других стран, где законодательно закреплены смарт-контракты, они также находят свое активное применение и в странах Центральной Азии. Например, казахстанские разработчики впервые внедряют смарт-контракты на базе блокчейн в сфере наружной рекламы. Компания Citix, известная как автор нескольких инновационных разработок в области Smart City, представила свою новую технологию для автоматизации и удобного запуска рекламной кампании. IT-департамент компании в этом году внедряет смарт-контракты на основе блокчейн-платформы Hyperledger для управления и контроля смартбордами, а точнее — для автоматизации бизнес-процессов и их прозрачности. Министерство юстиции Азербайджана планирует внедрить технологию блокчейн и смарт-контракты в сферы жилищно-коммунального хозяйства и бытового обслуживания. Несколько других штатов (помимо вышеуказанных) США признали юридическую силу смарт-контрактов на блокчейне или намереваются сделать это в ближайшее время. Например, Аризона сделала это еще весной 2017 года, Огайо внес соответствующее предложение в мае, а Флорида – в январе. Также в июле 2020 года сообщалось, что Великобритания может узаконить смарт-контракты на блокчейне.

Комментарии

Объем цифровых услуг в Кыргызстане предположительно будет также быстро расти с каждым днем, вовлекая всё большее число граждан и юридических лиц в ряды пользователей. При этом отсутствие в гражданском законодательстве Кыргызской Республики каких-либо упоминаний о цифровом праве оставляет пользователей и поставщиков таких услуг вне правовой регламентации и юридической защиты, которая нацелена на упорядоченное стимулирование гражданского оборота. Отсутствие правового регулирования в этой сфере безусловно является серьёзным сдерживающим фактором, делая гражданское законодательство всё более архаичным и неадекватным текущему стремительному прогрессу.

В Гражданском кодексе Кыргызской Республики только начинают появляться нормы, предполагающие элементы цифровизации гражданско-правовых отношений, однако также не обозначены такие определения как криптовалюта, блокчейн, майнинг, токены, не упомянуты такие виды договоров, как смарт-контракты, совершения сделки с помощью цифровых технологий.

Здесь следует отметить, что Закон «О введении в действие Налогового кодекса Кыргызской Республики» от 18 января 2022 года №4, в пункт 1 статьи 176 ГК вводит следующее понятие: «Письменная форма сделки считается соблюденной также в случае совершения лицом сделки с помощью электронных либо иных технических средств, позволяющих воспроизвести на материальном носителе в неизменном виде содержание сделки, при этом требование о наличии подписи считается выполненным, если использован любой способ, позволяющий достоверно определить лицо, выразившее волю. Законом, иными правовыми актами и соглашением сторон могут быть предусмотрены специальные способы достоверного определения лица, выразившего волю.»

Также, в Кыргызской Республике действует Закон «Об электронной подписи» от 19 июля 2017 года № 128. Данный Закон регулирует отношения по использованию электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, а также при совершении юридически значимых действий. В данном законе даются определения электронной подписи, ключу подписи и сертификату ключа подписи и т.д.

Поскольку смарт-контракт представляет собой: во-первых, некий алгоритм, предназначенный для автоматизации процесса исполнения контрактов, то есть, это набор правил и последовательность действий для исполнения; во-вторых, эти правила хранятся для обсуждения условий контракта, далее автоматически проверяются, после чего выполняются условия согласно цифровому протоколу. Также смарт-контракты подтверждаются электронно-цифровой подписью, каждый из сторон договора имеет свой электронный ключ подписи.

Исходя из вышесказанного, становится ясным, что законодательство Кыргызской Республики не запрещает заключение смарт-контрактов сторонами договора, то есть заключение гражданско-правовых сделок с использованием смарт-контрактов может осуществляться без нарушений закона. При том, что правовое регулирование такого вида договоров не осуществляется и ответственность сторон при рисках заключений таких договоров также не обозначена.

Помимо вышеуказанного регулирования, следует отметить, что на стадии общественного обсуждения сейчас находится Закон «О виртуальных активах» от 21 января 2022 года №12.

Целью проекта Закона «О виртуальных активах» является создание правовой основы оборота криптовалют и деятельности поставщиков услуг обмена криптовалют, а также снижения рисков финансирования террористической деятельности и легализации (отмывания) преступных доходов.

В проекте Закона криптовалюта поименована, как вид виртуального актива, являющийся цифровым выражением стоимости, который создается, хранится и обращается в электронной (цифровой) форме и не является денежным средством, валютой и/или средством

платежа, а также не удостоверяет имущественные и неимущественные права. Однако, само определение «виртуальный актив», как и весь проект закона, не дает ответа на фундаментальный вопрос: что такое виртуальный актив – это имущество, товар, нематериальный/инвестиционный актив, биржевой товар, ценность, услуга?

Становится ясным, что возникают вопросы к трактовке криптовалюты именно в таком определении, а также к обороту криптовалюты в гражданском праве. Поскольку до сих пор понятие «криптовалюта» является неоднозначным. В случае полной либерализации использования криптовалют могут возникнуть определенные риски.

Подход к определению виртуального актива недостаточно проработан с юридической точки зрения и порождает правовую неопределенность, а также не учитывает сложившуюся мировую практику и опыт регулирования криптоиндустрии в других юрисдикциях.

Такой законопроект в текущей редакции не направлен на адекватное регулирование и выработку правовой позиции с учетом интересов криптоиндустрии, что приведет к «зарегулирванности» (по российской модели) нарождающегося рынка, приведя к тому, что криптоэнтузиасты и профессионалы будут крайне осторожно работать с криптовалютой или перестанут вовсе, уходя для развития криптопроектов в более комфортные юрисдикции.

Одним из самых больших недостатков законопроекта является запрет на использование виртуальных активов в качестве средства платежа/платежного средства в качестве оплаты товаров, работы и услуг, что противоречит природе и назначению криптовалюты, созданной как простой инструмент платежа, средство расчета, доступное для использования любому человеку.

К примеру, поименованные в законопроекте как «необеспеченные виртуальные активы» в отношении которых отсутствует лицо/лица, несущие обязательства перед каждым обладателем таких виртуальных активов – это биткоин, эфириум, лайткоин, прочие монеты, запущенные на блокчейне – они как раз и являются средством платежа.

Криптобизнес, по сути, не сможет использовать криптовалюту для своих операций, ему будет невыгодно работать на территории Кыргызской Республики, что повлечет исход в более благоприятные юрисдикции. Запрет на использование виртуального актива в качества платежного средства снижает экономическую целесообразность владения криптовалютой, затормозит эту инновационную индустрию в стране. Соответствующие криптообменники либо уйдут за пределы страны, либо закроются. Запреты в первую очередь коснутся коммерческих структур.

Подчеркнем, что частные сделки отследить практически невозможно, использование криптовалют в качестве платежного средства может происходить без использования банковских каналов, что не дает возможности органам финансового надзора в полной мере реализовывать контроль денежных потоков в стране; уполномоченные органы государства не в состоянии в полной мере осуществлять контроль частных финансовых операций с криптовалютами и в силу технических ограничений.

Таким образом, становится ясным, что в настоящее время уполномоченные органы государства не в состоянии в полной мере осуществлять контроль финансовых операций с криптовалютами как в силу технических ограничений, так и по причине отсутствия соответствующей нормативно-правовой базы.

Следует также отметить, что, к примеру, налогообложение объекта, не признаваемого гражданским законодательством в каком-то определенном качестве (имущество, инвестиционный актив и т.п.), невозможно. Если это имущество – возникают ли у владельцев обязательства по декларированию владения таким имуществом и с какого порога, кто его определяет и где, в каком НПА, уплаты причитающихся налогов в случае распоряжения (отчуждения, н-р) им от суммы полученного дохода, кто и как ведет учет и т.п.

В целом, существующие на сегодняшний день в Кыргызской Республике нормативно-правовые акты не дают четкого регулирования вопросов реализации работы смарт-контрактов, информацию о криптовалюте, а также работы технологии блокчейн в праве.

Что касается внедрения данных нововведений в различные страны мира, можно заметить, что уже активно начинают реализовываться использование криптовалюты,

осуществление договоров с помощью смарт контрактов, использование технологии блокчейн в праве. Однако, лишь малая часть государств закрепили криптовалюту как «цифровой товар», а смарт-контракт, как договор в гражданском праве и осуществили принятие нормативных-правовых актов, связанных с полномерной легализацией криптовалюты, как финансового актива.

В некоторых странах на октябрь 2021 года криптовалюту можно использовать для покупки товаров и услуг, вводится либеральный режим, чтобы дать людям возможность развивать эту сферу (Германия, Япония, Швейцария), одновременно поддерживаются строгие требования по процедурам идентификации клиентов, стараясь эффективно интегрировать криптовалюты в свою экономику.

В швейцарском кантоне Цуг с 2021 года можно платить налоги в криптовалюте - налоговые отчисления будут приниматься в биткоинах и эфирах. С 7 сентября 2021 г. в Сальвадоре вступил в силу закон о наделении первой криптовалюты биткоина статусом законного платежного средства наравне с долларом США. Власти Сальвадора купили биткоины и в общей сложности государство владеет 1120 BTC на сумму свыше $66 млн.$ США. Германия - страна, где можно расплачиваться биткоинами. В Японии с 2016 г. биткоин является цифровым средством платежа. Сингапур поддерживает благоприятная среда в индустрии электронных финансовых технологий. Блокчейн проекты реализуются в ОАЭ. Компания Tesla рассматривает возможность разрешить покупателям оплачивать электромобили криптовалютами. Онлайн-платформа Amazon объявила о работе по интеграции биткоин-платежей.

В США криптовалюта рассматривается в различных качествах, в том числе как имущественный актив (property) для целей налогообложения или (Комиссией по срочной биржевой торговле США) биржевой товар для целей применения отдельных положений законодательства о биржевой торговле. По мнению Комиссии по рынку ценных бумаг США (SEC), в случаях, когда криптовалюта используется для привлечения инвестиций в рамках Initial Coin Offering, на действия по ее размещению может распространяться законодательство США о ценных бумагах, а сама криптовалюта (токен) может рассматриваться в качестве такой разновидности ценной бумаги, как инвестиционный контракт (investment contract).

Помимо этого, члены Сената и Ассамблеи Калифорнии одобрили законопроект, который позволит ввести блокчейн, смарт-контракты и связанные с ними технологии в правовое поле. В рамках законопроекта №2658 соответствующие поправки будут внесены в гражданский, правительственный, страховой и корпоративный кодексы штата. Одним из главных достижений законопроекта Кальдерона также является легальное определение DLT и криптовалютных технологий. Смарт-контракт определяется как «управляемая событиями программа, функционирующая в распределенном, децентрализованном и общем реестре, которая может взять под контроль и поручить передачу активов в этом реестре». Кроме того, в соответствии с поправками, смарт-контракты будут включены в общее легальное определение «контрактов».

Несколько других штатов США признали юридическую силу смарт-контрактов на блокчейне или намереваются сделать это в ближайшее время. Например, Аризона сделала это еще весной 2017 года, Огайо внес соответствующее предложение в мае, а Флорида – в январе. Также в июле сообщалось, что Великобритания может узаконить смарт-контракты на блокчейне.

В Российской Федерации был принят проект Федерального Закона «О цифровизации финансовых активов», согласно которому будут урегулированы отношения, возникающие при создании, выпуске, хранении и обращении цифровых финансовых активов, а также осуществлении прав и исполнении обязанностей по смарт-контрактам. В проекте данного закона четко определены цифровые понятия, особенности работы криптовалюты, цифровых обращений и подобные вопросы. Также Федеральным Законом «О внесении изменений в части первую, вторую, и статью 1124 части третьей Гражданского кодекса Российской Федерации» были внесены изменения в ГК РФ, в соответствии с которыми в ГК РФ появилось понятие Цифровые права и обязанности; сделка, совершенная с помощью электронных либо

иных технических средств, исполнение некоторых обязательств путем применения информационных технологий, определенных условиями сделки и т.д.

Однако, пока остается трудным сказать наверняка, повлияли ли положительно такие изменения в гражданское законодательство и старание внедрить правовое регулирование технологии блокчейн, а также оборота криптовалют в государстве. Поскольку на практике остается неясным возможно ли осуществление контроля и регулирования оборота тех же криптовалют в цифровой действительности, а также вопросы ответственности по смарт-контрактам также остаются актуальны, несмотря их регламентацию в законе.

Республика Беларусь к вопросу внедрения цифровизации права в гражданское законодательство подошла более кардинально. Не менее важными представляются изменения, которые были внесены в законодательство Беларуси. Беларусь стала первой в мире страной, которая законодательно закрепила смарт-контракт. Президент Беларуси утвердил Декрет «О развитии цифровой экономики», где смарт контракт является самостоятельным гражданско-правовым договором. Помимо этого, было подписано Постановление Национального Банка Беларуси «О совершении и (или) исполнении юридически значимых действий посредством смарт-контрактов».

При этом многие подходы к квалификации криптовалют, отраженные в зарубежных правопорядках, обусловлены спецификой терминологии и конкретной правовой системы и спецификой задач, для решения которых был выработан тот или иной подход.

За рубежом, как правило, используется точечное регулирование: соответствующие акты и разъяснения принимаются по отдельным, преимущественно публично-правовым вопросам (налогообложение, применимость законодательства о противодействии легализации денежных средств, полученных преступным путем, и т.п.), в остальных сферах законодатели и регуляторы занимают выжидательную позицию, обеспечивая участникам оборота простор для саморегулирования. Такое точечное регулирование необходимо и в Кыргызской Республике.

Вопрос выработки системы регулирования обращения криптовалют напрямую связан с пониманием ее сущности и закреплением в национальном законодательстве соответствующего термина. Определяя криптовалюты в качестве платежного средства, регулирующие органы власти сталкиваются с дилеммой частных и государственных денег (фиатные валюты), поэтому многие страны рассматривают криптовалюты как вид цифрового актива.

Такие новшества в гражданском законодательстве являются крайне важными для внедрения цифровизации права в страны постсоветского пространства. Однако, следует подойти внимательно к вопросу внедрения такого вида договоров, как смарт-контракты в Гражданский Кодекс Кыргызской Республики.

Таким образом, стоить рассмотреть вопросы, в первую очередь, внесения изменений в Гражданский кодекс Кыргызской Республики, а именно:

- к видам объектов гражданских прав отнести также цифровые права, виртуальные активы, определив объект такого права в гражданском обороте;
- к способам исполнения обязательств отнести - исполнение обязательств путем применения цифровых технологий, определенных условиями сделки, а также в вопросах конклюдентных действий;
- в некоторых видах договоров по «форме совершения сделки» дополнить терминами «цифровых», «электронного», в соответствии с указанными выше изменениями;
- помимо этого, закрепление в Гражданском кодексе понятий, отталкиваясь от которых, возможно было бы осуществлять работу рынка существующих в информационно-телекоммуникационной сети новых объектов экономических отношений («токены», «криптовалюта», «майнинг» и т.д.).
- также необходимо поименовать в Гражданском Кодексе смарт-контракты, как самоисполняемую сделку, дав четкое определение данному виду договоров.

То есть необходимы соответствующие (пакетные) изменения в Гражданский Кодекс Кыргызской Республики в части отнесения виртуальных активов к объектам гражданских прав (что виртуальный актив является объектом гражданских прав прямо указано в Законе «О виртуальных активах») с указанием категории (что это такое), как и введению именно в ГК КР понятия смарт-контракта, в категории самоисполняемых сделок).

Подводя общие итоги вышеперечисленным подходам следует резюмировать, что внесение изменений в нормативно-правовые акты на соответствие практикующимся новшествам вызвано объективным развитием в сфере цифровизации права, которые коснутся и Кыргызской Республики. В частности, правовое закрепление статуса смарт-контрактов и регулирование отношений сторон станет необходимым фактором развития экономической и финансовой системы государства.

Раздел 22. Платежные системы

Содержание

- Банковский сектор и финансовые технологии (вопросы электронных денег, платежных систем, электронные платежные инструменты, передача электронных денежных средств, внедрение финансовых технологий в заинтересованные ведомства (Министерство финансов КР, Счетная палата КР, Национальный банк КР)

Текущее регулирование (действующее законодательство):

1. Закон КР "О платежной системе Кыргызской Республики"
2. Закон Кыргызской Республики "Об электронном управлении"
3. Закон КР "Об электронной торговле"
4. Закон КР "О виртуальных активах"
5. Постановление Правительства КР "Об утверждении Положения о государственной системе электронных платежей" от 28 октября 2017 года № 709
6. Постановление Национального банка Кыргызской Республики "Об утверждении Положения "Об электронных деньгах в Кыргызской Республике" от 30 марта 2016 года № 15/6

Краткое описание выявленных недостатков и ориентиров из мировой практики

№	Описание недостатка	Тип[41]	Лучшая практика
22.1	Проблемными вопросами являются слабая интегрированность рынка с электронными платежными системами, а именно среди представителей среднего и малого бизнеса. Если государственные и иные организации уже используют возможности эквайринга, то в среднем и малом сегментах такие нововведения пока не сильно используются из-за дополнительных комиссий, что зачастую отпугивает и граждан, и бизнес. Необходимо провести работу по внедрению поощрений по использованию электронных платежей в расчетах, на примере государственных и муниципальных услуг можно предусмотреть скидки при получении услуг в электронном формате до 20%, а при их полной автоматизации до 50%. В частном секторе стимулом будет служить система кэшбэков, что также требует закрепления в нормативных	**П**	*В Турции* в соответствии с Законом о платежных и расчетных системах по ценным бумагам (Payment and Securities Settlement Systems) все организации, осуществляющие платежные услуги и использующие электронные деньги, с 2013 года могут являться провайдерами по предоставлению платежных услуг путем создания двух новых видов провайдеров услуг: платежных организаций (PI — Payment Institutions) и организаций по выпуску электронных денег (EMI — Electronic Money Institution). Первый тип организаций PI может осуществлять расчеты за услуги, но не может выпускать электронные деньги. А организации EMI (второй тип), к которым предъявляются более жесткие требования по уставному капиталу (5 млн турецких лир по сравнению с 1–2 млн для платежных организаций), могут свободно открывать счета для расчета

[41] В таблице приводятся следующие типы недостатков регулирования:
(П) пробел в регулировании (регулирование требуется, но его нет)
(У) устаревшая норма (норма есть, но её нужно менять)
(Н) неработающая норма (норма есть, но в силу описанных причин она не работает)
(Б) действующая норма является необоснованным препятствием для осуществления деятельности

	правовых актах, а именно в Законе «О платежных системах». Одной из мер использования электронных платежей также будет упрощение процедуры подачи единой налоговой декларации для лиц, кто все операции проводит только в электронных платежах.		электронными деньгами своим клиентам. Агентство по банковскому регулированию и надзору (Banking Regulation and Supervision Agency), созданное в рамках закона о платежных и расчетных системах по ценным бумагам, лицензирует и ведет контроль за двумя обозначенными типами организаций в Турции.
22.2	Слабая интегрированность платежных систем между собой и отсутствие национальной системы моментальных платежей создает трудности для межбанковского взаимодействия в вопросах увеличения доли электронных платежей, которая должна была быть реализована еще до 1 мая 2021 года в соответствии с Указом Президента Кыргызской Республики “О дальнейших мерах по повышению доступности и качества предоставления государственных и муниципальных услуг населению” от 8 февраля 2021 года УП № 27 Необходимо запустить национальную систему моментальных платежей чтобы ускорить внутренние процессы по электронным денежным операциям.	**Н**	**Европейский союз** - один из самых зрелых регионов на рынке электронной коммерции. Евро используется в качестве национальной валюты в 19 из 28 государств-членов ЕС, а SEPA (единая зона платежей в евро) стала общеевропейским методом для передачи денежных средств. Несмотря на то, что дебетовые и кредитные карты являются наиболее предпочтительным способом оплаты в большинстве европейских стран, рынок ЕС продолжает быть весьма разнообразным с точки зрения местных, альтернативных способов оплаты (платежных систем): ELV, Sofort и GiroPay в Германии, iDEAL в странах Бенилюкса и т.д. Платежные методы в различных частях региона составляют сложный набор способов оплаты. В данном контексте необходимо обратить внимание и на опыт США где рынок электронной коммерции является вторым по величине онлайн-рынком в мире, уступая только Китаю. Основным способом оплаты в Северной Америке и в США в частности являются карточные платежи, однако представители онлайн-бизнеса должны учитывать набирающие популярность платежи с помощью цифровых кошельков и другие альтернативные платежные методы. По данным ежегодного отчета о состоянии платежей в мире World Payments Report, который готовит французская Capgemini совместно с банком BNP Paribas, в 2011 году в

			Швеции лишь 3% расчетов совершались с помощью наличных, в 2015-м — только 2%. К 2020 году эта доля должна сократиться до 0,5%. Даже 40% церковных сборов в стране уже принимаются по безналичному расчету.
22.3	Внедрение цифровой национальной валюты также до настоящего момента не регламентировано, при том, что эмиссия и обращение такой валюты избавляет Национальный банк от расходов на печать реальной валюты, а ее распространенность будет способствовать развитию рынка цифровых платежей. Необходимо закрепить в законодательстве положения по национальной цифровой валюте.	**П**	На примере цифрового Юаня видно, что ведущие экономики мира уже начинают проявлять интерес к внедрению цифровой национальной валюты, В КНР официально работа по введению цифрового Юаня началась в конце 2019 года. В мае 2020 года Народный банк Китая в рамках пилотной программы ввёл в четырех городах страны национальную криптовалюту DCEP; появилась возможность совершать оплату покупок в цифровых юанях. Внутренние пилотные испытания также будут проводиться в ходе зимних Олимпийских игр 2022 года в Пекине. Источник, близкий к запуску DC / EP, сообщил Global Times, что «олимпийские» тесты будут сосредоточены на цифровых платежах в иностранной валюте гостями мероприятия. Для иностранных туристов цифровой кошелек может быть загружен из магазина приложений или включен в SIM-карты китайских операторов связи. Кандидатами на следующий раунд испытаний могут стать Шанхай и крупные города острова Хайнань, где присутствуют значительные объёмы внешней торговли и потоки капитала; (в мае китайские власти объявили о плане превращения Хайнаня в порт свободной торговли, и технология блокчейн, на которой основан проект цифровой валюты DC / EP, упоминается в нём несколько раз). Основное преимущество цифровой валюты в оперативности сделок с ней в то время, как международные долларовые-традиционные платежные системы SWIFT и CHIPS

			устаревают, их расчеты слишком медлительные и дорогостоящие.
22.4	Необходимо вносить пакетные изменения в налоговое, гражданское и банковское законодательство для полноценного внедрения цифровых финансовых активов и криптовалют, а для надзора и администрирования - в административное и уголовное законодательство, создав в совокупности легальную систему по нормированию различного вида денежных единиц на рынке Кыргызской Республики.	**П**	В различных странах мира уже активно начинают реализовываться использование криптовалюты, осуществление договоров с помощью смарт контрактов, использование технологии блокчейн в праве. В некоторых странах на октябрь 2021 года криптовалюту можно использовать для покупки товаров и услуг, вводится либеральный режим, чтобы дать людям возможность развивать эту сферу (**Германия, Япония, Швейцария**), одновременно поддерживаются строгие требования по процедурам идентификации клиентов, стараясь эффективно интегрировать криптовалюты в свою экономику. В **швейцарском кантоне Цуг** с 2021 года можно платить налоги в криптовалюте - налоговые отчисления будут приниматься в биткоинах и эфирах. С 7 сентября 2021 г. в **Сальвадоре** вступил в силу закон о наделении первой криптовалюты биткоина статусом законного платежного средства наравне с долларом США. Власти Сальвадора купили биткоины и в общей сложности государство владеет 1120 BTC на сумму свыше $66 млн.$ США. Германия - страна, где можно расплачиваться биткоинами. В **Японии** с 2016 г. биткоин является цифровым средством платежа. **Сингапур** поддерживает благоприятная среда в индустрии электронных финансовых технологий. В **США** криптовалюта рассматривается в различных качествах, в том числе как имущественный актив (property) для целей налогообложения или (Комиссией по срочной биржевой торговле США) биржевой товар для целей применения отдельных положений законодательства о биржевой торговле. По мнению

			Комиссии по рынку ценных бумаг США (SEC), в случаях, когда криптовалюта используется для привлечения инвестиций в рамках Initial Coin Offering, на действия по ее размещению может распространяться законодательство США о ценных бумагах, а сама криптовалюта (токен) может рассматриваться в качестве такой разновидности ценной бумаги, как инвестиционный контракт (investment contract) .

Комментарии

Объем цифровых услуг в Кыргызстане предположительно будет также быстро расти с каждым днем, вовлекая всё большее число граждан и юридических лиц в ряды пользователей. Активная цифровизация привела к формированию цифрового профиля человека, характеризующего все стороны его жизни, а также способствовала определенным мировоззренческим изменениям – наряду с материальными или «осязаемыми» ценностями, появились цифровые: начиная от прав на объекты интеллектуальной собственности и заканчивая персонажами в компьютерных онлайн-играх. Эти товары и услуги стали «производиться», покупаться и продаваться на глобальном цифровом рынке, который с момента своего появления не имел географических границ. Особенностью этого рынка является то, что подавляющее большинство товаров и услуг потребляются и используются в цифровом пространстве. Следствием этого является ускорение коммуникации и «доставки» цифровых продуктов между продавцами и покупателями. В то же время обслуживание сделок купли-продажи осуществлялось (и осуществляется) с использованием фиатных денег и банковской инфраструктуры.

Виды и формы денег всегда следовали за изменениями в экономической системе, отражая текущие запросы в мере стоимости, средстве обращения, платежа, накопления. В цифровой экономике функции денег остаются прежними, но при этом требования к ним возрастают:

- переход в максимальной степени к безналичной (цифровой) форме хранения и расчетов;
- минимальные затраты на осуществление расчетов и хранение денежных средств;
- максимальная унификация технологий передачи и хранения стоимости;
- возможность самостоятельного осуществления расчетов независимо от времени и места нахождения отправителя;
- отсутствие посредника в расчетах и платежах («peer-to-peer») и
- невозможность влияния третьей стороны на их осуществление;
- скорость, удобство и высокая степень надежности осуществления расчетов и платежей.

Криптовалюты стали первой массовой апробацией технологии блокчейн (технологии распределенного реестра). В постсоветской доктрине представлен широкий спектр подходов к определению правовой природы криптовалюты. Использование криптовалют и технологии блокчейн стало одним из ответов на возможности и вызовы развития мировой экономики в том числе, связанные с несовершенством государственного и рыночного регулирования:

- криптовалюта – продукт цифровой экономики;
- при создании криптовалюты применяются алгоритмы, основанные на объективных математических законах;

- контроль обращения криптовалют осуществляется самой системой, что делает ее более устойчивой по отношению к действиям третьих лиц;
- криптовалюты позволяют снижать транзакционные издержки;
- криптовалюты – интернациональный продукт, созданный в интересах и для обслуживания всех участников расчетов.

Развитие электронных платежей в Кыргызской Республике можно описать следующим образом: дебетовые (включая предоплаченные) и кредитные карты, кредитные и дебетовые переводы составляют основу безналичных типов платежей, обычно используемых сегодня потребителями и предприятиями. Эти основные типы безналичных платежей используются как традиционными способами, такими как личные покупки, начисление заработной платы и оплата счетов, так и инновационными способами, такими как мобильные платежи, электронная коммерция. Сегодня, наряду со значительными достижениями в области телекоммуникаций, электронные системы быстро заменяют традиционные способы оплаты. Безналичные платежи являются важным источником экономического развития и оказывают большое влияние на потребительские расходы.

Платежная система – это технологический процесс, когда посредством различных финансовых инструментов расплачиваются за товары и услуги, переводят деньги, выплачивают кредиты и т.п.

В Кыргызской Республике (КР) существуют 3 компонента платежных систем:

1. Система крупных платежей НБ:

- Гроссовая системы расчетов в режиме реального времени (ГСРВВ). ГСРРВ обеспечивает проведение межбанковских срочных и крупных платежей и осуществление окончательного расчета по каждому платежу на индивидуальной основе в режиме реального времени на основе процедур, правил, технологий и технической инфраструктуры. Используется, когда требуется немедленное проведение окончательного расчета.

2. Система розничных платежей:

- Система Пакетного Клиринга (СПК) проводит мелкие розничные и регулярные платежи. В СПК обрабатывается большое количество небольших по стоимости платежей, погашения кредита, перевода денег с одного счета на другой. Клиринг в значительной степени позволяет сэкономить на банковских комиссиях и операционных расходах. Расчеты по клирингу проводятся на определенную дату (например, конец отчетного периода или каждое первое число месяца).
- Системы расчетов платежными картами – это “знакомые” пластиковые карты, которые используются для оплаты товаров и услуг, в том числе через интернет и снятии наличных.
- Системы денежных переводов – это форма перевода денег по банковской системе, где отсутствует необходимость открытия счета в банке. Денежные переводы могут быть внутренние (в пределах одного государства) и внешние (межгосударственные).
- Системы для моментальных платежей, системы электронных денег. Это платежи, которые осуществляются без использования наличных денег, такие как переводы через интернет-банкинг, мобильный банкинг, электронные кошельки и т.п. Также существуют платежные терминалы, автономные аппараты, которые осуществляют прием денег за услуги мобильной связи, коммунальные услуги, в счет погашения банковских кредитов, пополнения счетов банковских карт и т.п.

3. Система для маршрутизации финансовых сообщений:
   - УКП SWIFT2 – эта система позволяет финансовым учреждениям во всем мире отправлять и получать информацию о финансовых операциях в безопасной, стандартизированной и надежной форме.
   - МКС – межбанковская коммуникационная сеть, которая служит технической основой для передачи сообщений между банками.

В соответствии со статьей 26 Закона Кыргызской Республики “Об электронном управлении” государственная система электронных платежей предназначена для обмена информацией об уплате физическими и юридическими лицами платежей за оказание государственных и муниципальных услуг, иных платежей в пользу республиканского или местных бюджетов.

Положением о государственной системе электронных платежей, утвержденным постановлением Правительства Кыргызской Республики от 28 октября 2017 года № 709 определяется:

1) перечень информации, необходимой для совершения оплаты за государственные и муниципальные услуги, а также совершения иных платежей, включая подлежащую уплате сумму, порядок получения и предоставления такой информации;
2) перечень информации, подтверждающей совершение оплаты за государственные и муниципальные услуги, а также совершение иных платежей, включая уплаченную сумму, порядок получения и предоставления такой информации;
3) порядок доступа к государственной системе электронных платежей.

Банк, иная кредитная организация, а также иные органы или организации, через которые производится уплата денежных средств заявителем, обязаны незамедлительно направлять информацию об их уплате в государственную систему электронных платежей.

Государственные и муниципальные учреждения после осуществления начисления суммы, подлежащей оплате заявителем за предоставляемые услуги, а также иных платежей, в случаях, предусмотренных законами Кыргызской Республики, обязаны незамедлительно направлять информацию, необходимую для ее уплаты, в государственную систему о государственных и муниципальных платежах.

Постановление Национального банка Кыргызской Республики “Об утверждении Положения “Об электронных деньгах в Кыргызской Республике” от 30 марта 2016 года № 15/6 регулирует помимо самой инфраструктуры электронных платежей вопросы по операциям с электронными деньгами, которые включают в себя выпуск, распространение, погашение электронных денег и предоставление платежных услуг с использованием электронных денег на территории Кыргызской Республики.

В дополнение к этому в законодательстве Кыргызской Республики по вопросам электронных платежей имеется Закон Кыргызской Республики “О платежной системе Кыргызской Республики”, а также постановление Национального банка Кыргызской Республики “Об утверждении Положения “О регулировании деятельности платежных организаций и операторов платежных систем” от 30 сентября 2019 года № 2019- П-14/50-2 - (ПС).

Проблемными вопросами здесь являются слабая интегрированность рынка с электронными платежными системами, а именно среди представителей среднего и малого бизнеса. Если государственные и иные организации уже используют возможности эквайринга, то в среднем и малом сегментах такие нововведения пока не сильно используются из-за дополнительных комиссий, что зачастую отпугивает и граждан, и бизнес.

Также, слабая интегрированность платежных систем между собой и отсутствие национальной системы моментальных платежей создает трудности для межбанковского взаимодействия в вопросах увеличения доли электронных платежей.

Отсутствие национальной системы денежных переводов затрудняет возможности переводов внутри Кыргызской Республики и влечет за собой повышение дороговизны переводов и использование иных систем денежных переводов. При этом спрос на денежные переводы по стране только растет. Затруднен процесс интеграции всех платежных систем и агрегаторов между собой, в том числе и с Государственной системой электронных платежей.

Необходимо снятие таких ограничений и стимулирование операторов платежных систем по внедрению своих продуктов не только на всех уровнях оказания услуг и взаимодействия B2B, B2C, B2G, а также C2C и C2G, в том числе по созданию минимальных ставок на электронные сделки между гражданами при встраивании эквайринга непосредственно в мобильные банковские приложения, то есть возможность межбанковских переводов резидентами разных банков между собой в режиме реального времени при минимальных комиссионных сборах.

Помимо этого, снижение доли наличных платежей можно стимулировать введением ограничений на оплату сделок наличными средствами размером до какого-либо предельного показателя, например, 2000 расчетных показателей (т.е. 20 тыс. сомов).

Например, **в Турции** в соответствии с Законом о платежных и расчетных системах по ценным бумагам (Payment and Securities Settlement Systems) все организации, осуществляющие платежные услуги и использующие электронные деньги, с 2013 года могут являться провайдерами по предоставлению платежных услуг путем создания двух новых видов провайдеров услуг: платежных организаций (PI — Payment Institutions) и организаций по выпуску электронных денег (EMI — Electronic Money Institution). Первый тип организаций PI может осуществлять расчеты за услуги, но не может выпускать электронные деньги. А организации EMI (второй тип), к которым предъявляются более жесткие требования по уставному капиталу (5 млн турецких лир по сравнению с 1–2 млн для платежных организаций), могут свободно открывать счета для расчета электронными деньгами своим клиентам. Агентство по банковскому регулированию и надзору (Banking Regulation and Supervision Agency), созданное в рамках закона о платежных и расчетных системах по ценным бумагам, лицензирует и ведет контроль за двумя обозначенными типами организаций в Турции. Организации типа EMI обязаны держать все средства, поступающие от их клиентов, на доверительных счетах в уполномоченных банках. А уполномоченные банки, в свою очередь, обязаны блокировать поступающие средства от организаций типа EMI на своих счетах, открытых в Центральном банке Турции.

При этом **Европейский союз** - один из самых зрелых регионов на рынке электронной коммерции. Евро используется в качестве национальной валюты в 19 из 28 государств-членов ЕС, а SEPA (единая зона платежей в евро) стала общеевропейским методом для передачи денежных средств.

Несмотря на то, что дебетовые и кредитные карты являются наиболее предпочтительным способом оплаты в большинстве европейских стран, рынок ЕС продолжает быть весьма разнообразным с точки зрения местных, альтернативных способов оплаты (платежных систем): ELV, Sofort и GiroPay в Германии, iDEAL в странах Бенилюкса и т.д. Платежные методы в различных частях региона составляют сложный набор способов оплаты (рис.2).

В Германии, например, наиболее предпочитаемым методом онлайн-платежей является ELV (сокращенно от Elektronisches Lastschriftverfahren) — метод электронного прямого дебетового платежа, который поддерживается немецкими банками. В Нидерландах самым популярным является также локальный платежный метод — iDeal, поддерживаемый большинством государственных банков в стране. 55% интернет-покупателей предпочитают использовать iDeal при оплате покупок в сети.

В Турции оплата кредитными и дебетовыми картами очень популярна (87%), но при этом Visa и MasterCard практически не используются. PayPal является вторым по популярности платежным методом (7%), также используются другие электронные кошельки (6%).

Что касается постсоветских стран, то, например, **в Российской Федерации** популярными являются не только кредитные и дебетовые карты, но также электронные платежи Qiwi, Яндекс.Деньги и Webmoney. Компанией Mediascope было изучено, как и за что платили онлайн жители РФ в 2018-2019 годах. Оказалось, что в целом доля пользователей, которые периодически платят через интернет, почти не изменилась. При этом выросло число тех, кто рассчитывается онлайн за такси, бронирование отелей и покупку билетов на транспорт, а пользователей, которые отправляют денежные переводы и платят за онлайн-игры, стало немного меньше. Чаще всего для оплаты люди используют банковские карты, Сбербанк Онлайн и Яндекс.Деньги.

Большая часть пользователей уже имеет опыт онлайн-оплаты мобильной связи (85,8%), покупок в интернет-магазинах (81%) и услуг ЖКХ (74%). Эти категории уже несколько лет входят в число самых популярных. Динамичнее всего растет доля пользователей, которые платят онлайн за такси. За год она выросла почти на 12% — с 45,4% в 2018 до 50,8% в 2019 году. Интересно, что за такси чаще рассчитывались молодые люди — около 64% респондентов в возрасте от 18 до 24 лет и почти 63% в группе от 25 до 34 лет. Среди аудитории от 35 до 44 лет платили онлайн 50% опрошенных, а в группе от 45 до 55 лет — всего 39%. Выросло также число людей, которые через интернет бронируют отели и покупают билеты на транспорт — примерно на 3% в каждой категории. Только в двух категориях доля пользователей, которые платят через интернет, уменьшилась — это денежные переводы (с 57,2% до 55%) и онлайн-игры (с 28,5% до 25,3%).

Банковские карты остаются самым популярным средством для платежей в интернете. Ими за год воспользовались 90,5% россиян. Через интернет-банкинг платили 89,7%, электронными деньгами — 77,6%.

Самая активная платежная аудитория в онлайне — пользователи от 25 до 34 лет. Электронными деньгами платили 82,2% респондентов этой возрастной группы, через интернет-банкинг — 93,9%. Самая большая доля пользователей банковских карт в более старшей группе — от 35 до 44 лет (94,4%).

Лидером среди платежных онлайн-сервисов традиционно остался Сбербанк Онлайн. С его помощью хотя бы раз за год платили 83,2% россиян. Яндекс.Деньги оказались вторым по популярности сервисом — через них рассчитывался каждый второй пользователь рунета (52,8%). В тройку лидеров вошел также PayPal (46,1%). На четвертом и пятом местах оказались электронные кошельки WebMoney и QIWI (39,9% и 36,9% соответственно). Около четверти респондентов платили онлайн через интернет-банкинги ВТБ, Альфа-Банка и Тинькофф Банка. Через сервис VK Pay, который вышел на рынок позже других электронных кошельков, рассчитывались 15,4% пользователей. В основном этот способ выбирает молодая аудитория: самая большая доля пользователей сервиса — от 18 до 24 лет. У остальных сервисов электронных денег больше всего пользователей в группе от 25 до 34 лет. Тем не менее даже у аудитории 18-24 лет самые популярные платежные сервисы — это Сбербанк Онлайн (83,2%), Яндекс.Деньги (45%), QIWI (40,6%).

При этом наблюдается уверенный рост бесконтактных платежей. Так, бесконтактные платежи популярнее всего у аудитории от 25 до 34 лет (57,3%). В среднем ими воспользовались за год 44,8% россиян, годом ранее — 38,3%. Среди бесконтактных систем лидирует Google Pay, число пользователей которой за год выросло с 19,6% до 22,9%. Через Apple Pay платили 18,9% респондентов, через Samsung Pay — 15,5%. У Garmin Pay аудитория заметно меньше — с его помощью рассчитывались около 2% респондентов. Однако среди пользователей 18-24 лет Apple Pay занял первое место (29%). Больше всего пользователей Google Pay в группе от 25 до 34 лет. Samsung Pay традиционно замыкает тройку лидеров. У людей от 35 до 44 лет корейский сервис оказался популярнее, чем Apple Pay, но он не смог обогнать Google Pay.

Таким образом во всем мире наблюдается тенденция к внедрению новых методов организации интернет-платежей уже на уровне C2B с привлечением банковского сектора только на этапе зачисления денежных средств на счета.

Что касается **правового регулирования криптовалюты** и введение такого понятия в законодательство в мире, то в различных странах мира уже активно начинают реализовываться использование криптовалюты и использование технологии блокчейн в праве. Однако, лишь очень малая часть государств закрепили криптовалюту как «цифровой товар» и осуществили принятие нормативных-правовых актов, связанных с полномерной легализацией криптовалюты, как финансового актива.

В некоторых странах на октябрь 2021 года криптовалюту можно использовать для покупки товаров и услуг, вводится либеральный режим, чтобы дать людям возможность развивать эту сферу (Германия, Япония, Швейцария), одновременно поддерживаются строгие требования по процедурам идентификации клиентов, стараясь эффективно интегрировать криптовалюты в свою экономику.

В швейцарском кантоне Цуг с 2021 года можно платить налоги в криптовалюте - налоговые отчисления будут приниматься в биткоинах и эфирах. С 7 сентября 2021 г. в Сальвадоре вступил в силу закон о наделении первой криптовалюты биткоина статусом законного платежного средства наравне с долларом США. Власти Сальвадора купили биткоины и в общей сложности государство владеет 1120 BTC на сумму свыше $66 млн.$ США. Германия - страна, где можно расплачиваться биткоинами. В Японии с 2016 г. биткоин является цифровым средством платежа. Сингапур поддерживает благоприятная среда в индустрии электронных финансовых технологий. Блокчейн проекты реализуются в ОАЭ. Компания Tesla рассматривает возможность разрешить покупателям оплачивать электромобили криптовалютами. Онлайн-платформа Amazon объявила о работе по интеграции биткоин-платежей.

В зарубежной нормативно-правовой практике существует и множество примеров использования криптовалюты:

- **в Японии криптовалюты** получили в определенной части статус платежного средства, которое может использоваться любым признающим его лицом для осуществления платежей за товары, работы, услуги во взаимоотношениях с неопределенным кругом лиц;
- **в Бразилии у**становлено достаточно широкое определение цифровой валюты, в силу чего криптовалюты вроде биткоина вполне подпадают под соответствующее понятие и регулирование;
- **В США** криптовалюта рассматривается в различных качествах, в том числе как имущественный актив (property) для целей налогообложения или (Комиссией по срочной биржевой торговле США) биржевой товар для целей применения отдельных положений законодательства о биржевой торговле. По мнению Комиссии по рынку ценных бумаг США (SEC), в случаях, когда криптовалюта используется для привлечения инвестиций в рамках Initial Coin Offering, на действия по ее размещению может распространяться законодательство США о ценных бумагах, а сама криптовалюта (токен) может рассматриваться в качестве такой разновидности ценной бумаги, как инвестиционный контракт (investment contract).

При этом многие подходы к квалификации криптовалют, отраженные в зарубежных правопорядках, обусловлены спецификой терминологии и конкретной правовой системы и спецификой задач, для решения которых был выработан тот или иной подход.

За рубежом, как правило, используется точечное регулирование: соответствующие акты и разъяснения принимаются по отдельным, преимущественно публично-правовым вопросам (налогообложение, применимость законодательства о противодействии легализации денежных средств, полученных преступным путем, и т.п.), в остальных сферах законодатели и регуляторы занимают выжидательную позицию, обеспечивая участникам оборота простор для саморегулирования.

Отдельной возможностью может стать закрепление в законодательстве Кыргызской Республики вопросов, относящихся к цифровой национальной валюте. То есть создание действенных налоговых и административных механизмов по сопровождению хождения

данного вида финансовых средств, поскольку доля сделок с такого рода валютами в ближайшем будущем будет только расти, а также собираемость по налогам и администрирование таких сделок будут проблематичными ввиду отсутствия их законодательного закрепления.

Необходимо вносить пакетные изменения в налоговое, гражданское и банковское законодательство для полноценного внедрения цифровых и криптовалют, а для надзора и администрирования - в административное и уголовное законодательство, создав в совокупности легальную систему по нормированию различного вида денежных единиц на рынке Кыргызской Республики.

Следует отметить, что **недавно принятый Закон «О виртуальных активах» от 21 января 2022 года №12** в текущей редакции не направлен на адекватное регулирование и выработку правовой позиции с учетом интересов криптоиндустрии, что приведет к «зарегулированности» (по российской модели) нарождающегося рынка, приведя к тому, что криптоэнтузиасты и профессионалы будут крайне осторожно работать с криптовалютой или перестанут вовсе, уходя для развития криптопроектов в более комфортные юрисдикции.

Одним из самых больших недостатков законопроекта является запрет на использование виртуальных активов в качестве средства платежа/платежного средства (ст. 4, 5) в качестве оплаты товаров, работы и услуг, что противоречит природе и назначению криптовалюты, созданной как простой инструмент платежа, средство расчета, доступное для использования любому человеку. Более того, майнеры, как правило, получают вознаграждение именно в виде криптовалюты, что и указано в определении майнинга (ст.4): «Майнинг может сопровождаться созданием виртуального актива, поступающего во владение лица, осуществляющего майнинг, в качестве вознаграждения за подтверждение совершения операций в распределенном реестре.». Если это не средство платежа, то как быть в этом случае? Создается правовая неопределенность с негативными для государства и бизнеса последствиями. В вопросах регулирования необходимо учитывать требования национального законодательства и рекомендации международных организаций в части обращения денежных средств, соблюдения мер по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма; тенденции снижения анонимности операций на финансовых рынках; взимания налогов и другие.

Также необходимо отметить то, что 9 февраля 2022 года был принят Указа Президента «О мерах по дальнейшему развитию финансового рынка», который также предусматривает задачу для Правительства и Национального банка по разработке законопроекты в части введения регулирования оборота криптовалют для создания правовой основы их оборота, защиты прав потребителей и снижения рисков.

Одновременно с внесением вышеуказанных изменений в законодательство по платежным системам, необходимо стимулировать внедрение электронных платежных систем и сервисов для скорейшего перевода экономики на цифровые рельсы, а также упрощения налогового администрирования всех сфер экономической деятельности.

Инструментами стимулирования использования электронных платежных систем может стать форма дисконтов и кэш-бэков при их использовании, в том числе при оплате государственных услуг, такие меры стимулирования могут ускорить процессы по выведению экономики и серой зоны и созданию условий прослеживаемости движения денежных масс, что в значительной степени улучшит положение Кыргызской Республики в рейтингах ФАТФ.

Раздел 23. Связанные изменения в закон о госслужбе

Текущее регулирование (действующее законодательство):

1. Закон Кыргызской Республики «О государственной гражданской службе и муниципальной службе» от 27 октября 2021 года №125
2. Закон Кыргызской Республики «Об электронном управлении» от 19 июля 2017 года №127
3. Указ Президента Кыргызской Республики «О Национальной стратегии развития Кыргызской Республики на 2018-2040 годы» от 31 октября 2018 года УП №221
4. Указ Президента Кыргызской Республики «О неотложных мерах по активизации внедрения цифровых технологий в государственное управление Кыргызской Республики» от 17 декабря 2020 года УП №64
5. Указ Президента Кыргызской Республики «О Национальной программе развития Кыргызской Республики до 2026 года» от 12 октября 2021 года УП №435
6. Постановление Кабинета Министров Кыргызской Республики «О вопросах Государственного агентства по делам государственной службы и местного самоуправления при Кабинете Министров Кыргызской Республики» от 15 ноября 2021 года №258
7. Постановление Кабинета Министров Кыргызской Республики «Об утверждении Плана мероприятий Кабинета Министров Кыргызской Республики по реализации Национальной программы развития Кыргызской Республики до 2026 года» от 25 декабря 2021 года №352
8. Распоряжение Кабинета Министров Кыргызской Республики от 12 января 2022 года №2-р
9. Распоряжение Кабинета Министров Кыргызской Республики от 24 марта 2022 года №134-р
10. Концепция цифровой трансформации "Цифровой Кыргызстан 2019-2023", одобренной решением Совета безопасности Кыргызской Республики от 14 декабря 2018 года № 2

Краткое описание выявленных недостатков и ориентиров из мировой практики

№	Описание недостатка	Тип[42]	Лучшая практика
23.1	Законодательство, регулирующее профессиональную переподготовку и повышение квалификации государственных служащих, не содержит в себе требований по обучению цифровым навыкам и компетенциям. Также, отсутствуют установленные показатели эффективности, не развернуты онлайн-обучение и сертификация, возможность создания цифровых команд в ведомствах	**П**	Развитие инновационной цифровой реальности предъявляет особые требования к профессиональным компетенциям государственного служащего, которые должны включать в себя также и цифровые компетенции, в соответствие с которыми государственный служащий должен совершенствовать свои знания, умения и навыки, уметь работать с современными информационными инструментами, платформами и программами. Вместе с тем, как показал анализ, большинство программ обучения

[42] В таблице приводятся следующие типы недостатков регулирования:
(П) пробел в регулировании (регулирование требуется, но его нет)
(У) устаревшая норма (норма есть, но её нужно менять)
(Н) неработающая норма (норма есть, но в силу описанных причин она не работает)
(Б) действующая норма является необоснованным препятствием для осуществления деятельности

			государственных служащих за рубежом (64%) ориентированы на решение проблем в двух областях: информационной безопасности и формировании успешных лидеров в цифровую эпоху. В области цифровых коммуникаций и взаимодействия с гражданами 55% программ развивают компетенции у сотрудников системы государственного управления. Например, в Сингапуре государственных служащих обучают использовать онлайн-офис для совместного редактирования файлов с заинтересованными лицами, а в США организуется отдельный курс обучения персонала по умению предоставлять информацию гражданам в простой форме. Вопросам управления социальными сетями и сотрудничеству со СМИ уделяется особое место в образовательных программах. Например, социальные сети в Великобритании рассматриваются как инструмент для повышения инноваций. Навыкам работы с данными (их анализу, интерпретации и графической визуализации, дружелюбной для пользователя) при создании государственных услуг обучаются слушатели почти половины изученных образовательных программ. На основе анализа зарубежных программ профессионального развития государственных служащих выявлено, что в 11 странах-лидерах по цифровому развитию уделяется особое внимание таким направлениями обучения в образовательных программах по ИКТ, как безопасность, руководство и коммуникации в цифровую эпоху.

Комментарии

Законодательство Кыргызской Республики не содержит требований о необходимости обучения (профессиональной переподготовки и повышения квалификации) государственных служащих цифровым навыкам и компетенциям.

Вместе с тем, эффективность системы государственного управления зависит от уровня результативности профессиональной деятельности государственных служащих и качества

реализации государственных решений. На современном этапе мир находится на стадии трансформации институтов государственного управления, обусловленной развитием цифровых технологий, которые являются ключевым фактором, определяющим темпы экономического роста.

Происходящие технологические изменения оказывают влияние на структуру требований, предъявляемых к уровню квалификации сотрудников государственных структур. Внедрение цифровых технологий расширяет инструментарий работы государственных служащих, что требует обновления их навыков и компетенций.

Национальные стратегические документы отмечают важность и актуальность профессиональной подготовки государственных служащих. Так, Национальная стратегия развития Кыргызской Республики на 2018-2040 годы, обращает внимание на необходимость масштабных программ переобучения и повышения квалификации государственных служащих. Концепция цифровой трансформации "Цифровой Кыргызстан 2019-2023", отмечает, что, исходя из вызовов цифровой трансформации, необходимо правовое преобразование всей системы государственного управления, которая будет направлена на совершенствование нормативных правовых актов, в том числе, в области государственной службы (вопросы цифровых компетенций и цифровых навыков государственных служащих, их профессиональной переподготовки и повышения квалификации). Наряду с этим, Указ Президента Кыргызской Республики "О неотложных мерах по активизации внедрения цифровых технологий в государственное управление Кыргызской Республики" от 17 декабря 2020 года УП № 64 дает поручение к 1 июня 2021 года сформировать программу подготовки и повышения квалификации для государственных и муниципальных служащих по цифровым навыкам и кибербезопасности, оказания услуг в условиях цифровой экономики, а Указ Президента Кыргызской Республики «О Национальной программе развития Кыргызской Республики до 2026 года» от 12 октября 2021 года УП №435, предусматривает запуск национальной образовательной программы «Системное повышение цифровых компетенций государственных служащих для поддержания цифрового государственного управления».

Таким образом, на данный момент существуют планы по обучению государственных служащих цифровым навыкам и компетенциям. Так, например, в рамках подготовки по внедрению системы электронного документооборота сотрудникам администрации Президента КР провели тренинг, на котором продемонстрировали процессы движения документов с момента создания в системе и до отправки адресату. Сотрудники также прошли обучение по созданию внутренних поручений, отслеживания маршрута и статуса отправленного документа, а также формирования отчета по исполнительской дисциплине[43].

Однако, подготовка государственных служащих по вопросам повышения цифровых навыков и выработки цифровых компетенций должна носить системный и постоянных характер.

Согласно Закону Кыргызской Республики "О государственной гражданской службе и муниципальной службе", предусматривается, что государственный служащий обязан не реже одного раза в 3 года проходить курсы повышения квалификации. Установленный максимальный период между курсами повышения квалификации должен быть сокращен, когда речь идет о цифровых навыках, исходя из реалий динамично развивающегося рынка. Вместе с этим, на сегодняшний день каждый государственный служащий должен обладать цифровыми навыками и компетенциями, вследствие чего, необходимо предусмотреть прохождение курсов повышения квалификации всеми государственными служащими, которые ими не обладают. Также, принципиально новый подход к взаимодействию государства и граждан выдвигает и совершенно новые требования к государственным служащим, которые будут воплощать в жизнь этот подход. Так, в рамках государственных органов требуется предоставление возможности создания «цифровых команд» - это симбиоз компетенций, т.е. команда, построенная на ролевой модели управления проектами, при которой выделяется несколько основных ролей участников команды, каждый со своей

[43] https://24.kg/vlast/232805_chinovnikov_prezidentskoy_administratsii_uchat_elektronnomu_dokumentirovaniyu/

квалификацией, компетенциями, зоной ответственности и т.д., для решения конкретной задачи, достижения цели (привлекаются сотрудники из разных отделов/департаментов).

Международный опыт

Направления профессионального развития цифровых компетенций государственных служащих за рубежом. Согласно глобальному рейтингу цифровой конкурентоспособности, США и Сингапур стабильно являются лидерами по внедрению цифровых технологий.

В основе рейтинга находятся три фактора: человеческий капитал, информационные технологии и готовность к цифровой трансформации.

Рассмотрим ТОП-15 стран рейтинга для дальнейшего изучения направлений профессионального развития цифровых навыков государственных служащих.

В группе из 11 стран-лидеров были найдены организации, которые предоставляют программы ДПО для сотрудников государственного сектора (Таблица 1).

Таблица 1. Организации, реализующие программы цифрового развития государственных служащих, в странах-лидерах в сфере цифровизации в 2020 г.

	Страна	**Организации, осуществляющие дополнительное образование государственных служащих**
1	США	Университет цифровых технологий
2	Сингапур	Колледж государственной службы
3	Швеция	Шведский институт государственного управления
4	Гонконг	Институт подготовки и развития государственной службы
5	Нидерланды	Европейский институт государственного управления
6	Южная Корея	Национальный институт развития человеческих ресурсов
7	Финляндия	Финский институт государственного управления
8	Канада	Цифровая академия канадской школы государственной службы
9	Великобритания	Академия государственных цифровых услуг; Колледж государственной службы
10	ОАЭ	Виртуальная академия
11	Австралия	Институт государственного управления Австралии

Для выявления лидирующих ключевых тематик развития цифровых навыков государственных служащих за рубежом рассмотрим содержание курсов профессионального развития государственных служащих в сфере ИКТ в странах-лидерах цифровой конкурентоспособности, реализующих программы для государственных служащих в сфере информационных технологий в 2020 г.

В Таблице 2 представлены наиболее часто встречающиеся направления для обучения государственных служащих в сфере ИКТ, тематики, которые используют 45% и более вышеупомянутых организаций в исследуемых странах.

Таблица 2. Основные направления профессионального развития цифровых навыков государственных служащих в организациях из стран-лидеров в сфере цифровизации в 2020 г.

	Тематика программ	**Число организаций, реализующих программы**
1.	Информационная безопасность	(7 из 11) 64%
2.	Лидерство в цифровую эпоху	(7 из 11) 64%
3.	Цифровые коммуникации и взаимодействие с гражданами	(6 из 11) 55%
4.	Вызовы и новые технологии	(5 из 11) 45%
5.	СМИ и социальные сети	(5 из 11) 45%
6.	Дизайн при создании цифровых услуг, ориентированных на пользователя	(5 из 11) 45%
7.	Анализ данных и машинное обучение	(5 из 11) 45%
8.	Визуализация данных	(5 из 11) 45%

Как показал анализ, большинство программ обучения государственных служащих за рубежом (64%) ориентированы на решение проблем в двух областях: информационной безопасности и формировании успешных лидеров в цифровую эпоху. В области цифровых коммуникаций и взаимодействия с гражданами 55% программ развивают компетенции у сотрудников системы государственного управления. Например, в Сингапуре государственных служащих обучают использовать онлайн-офис для совместного редактирования файлов с заинтересованными лицами, а в США организуется отдельный курс обучения персонала по умению предоставлять информацию гражданам в простой форме. Вопросам управления социальными сетями и сотрудничеству со СМИ уделяется особое место в образовательных программах. Например, социальные сети в Великобритании рассматриваются как инструмент для повышения инноваций. Навыкам работы с данными (их анализу, интерпретации и графической визуализации, дружелюбной для пользователя) при создании государственных услуг обучаются слушатели почти половины изученных образовательных программ.

Отметим, что направления изучения цифровых технологий государственными служащими разнообразны в каждой стране, но, на наш взгляд, можно выделить общие тенденции формирования компетенций в сфере ИКТ: забота об информационной безопасности, обучение руководителей цифровой трансформации и развитие навыков всех категорий сотрудников в области цифровых коммуникаций.

Выводы и рекомендации

Исходя из вышеперечисленного, понятие профессионального развития государственных служащих можно определить как совершенствование уровня квалификации для более качественного выполнения профессиональных обязанностей и соответствия требованиям условий социально-экономической среды. Подтверждено, что в современных условиях для соответствия квалификаций сотрудников государственного сектора меняющейся

профессиональной среде необходимо развивать цифровые компетенции, которые включают в себя не только технические знания и умения в специализированной среде, но и личностные качества, цифровую культуру.

Развитие компетенций в области информационных технологий является основой цифровой трансформации государственного управления. Цифровизация изменяет социальные отношения внутри и за пределами государственного сектора: требует совершенствования рабочих практик и цифровых навыков государственных служащих. Раскрывая проблему развития цифровых компетенций персонала системы государственного управления с помощью изучения тематических направлений обучения сотрудников государственного сектора других стран, удалось выявить, что ключевыми сегодня являются следующие направления: информационная безопасность, лидерство в цифровую эпоху и цифровые коммуникации и взаимодействие с гражданами.

Таким образом, требуется внесение изменений в законодательство, в части:

- установления требований по прохождению курсов повышения квалификации государственными служащими в целях приобретения ими цифровых навыков и компетенций;
- снижения максимального периода между курсами повышения квалификации, когда речь идет о цифровых навыках;
- включения в программы курсов повышения квалификации государственных служащих цифровых навыков и компетенций по следующим направлениям: кибербезопасность, лидерство в цифровую эпоху и т.д.;
- предоставления преимущества лицам, поступающим на государственную службу, в случае наличия у них цифровых навыков и компетенций;
- создания возможности прохождения курсов обучения и сертификации онлайн;
- установления показателей эффективности государственных служащих;
- предоставления возможности создания цифровых команд в рамках государственных органов.

Раздел 24. Облачные технологии

Содержание

- правовое регулирование облачных технологий
- вопросы защиты персональных данных при использовании облачных технологий

Текущее регулирование (действующее законодательство):

1. Закон Кыргызской Республики «Об электронном управлении»;
2. Закон Кыргызской Республики «Об информации персонального характера»;
3. Указ Президента Кыргызской Республики «О Национальной программе развития Кыргызской Республики до 2026 года» от 12 октября 2021 года УП №435;
4. Указ Президента Кыргызской Республики «О Национальной стратегии развития Кыргызской Республики на 2018-2040 годы» от 31 октября 2018 года УП № 221;
5. Постановление Правительства Кыргызской Республики Об утверждении Требований к защите информации, содержащейся в базах данных государственных информационных систем» от 21 ноября 2017 года № 762;
6. Распоряжение Кабинета министров Кыргызской Республики от 12 января 2022 года №2-р;
7. Концепция цифровой трансформации «Цифровой Кыргызстан 2019-2023» утвержденное Решением Совета безопасности от 14 декабря 2018 года №2.

Краткое описание выявленных недостатков и ориентиров из мировой практики

№	Описание недостатка	Тип[44]	Лучшая практика
24.1	Законодательство Кыргызской Республики прямо не регулирует вопросы использования облачных технологий. Законодательно не закреплено понятия «облачных технологий».	**П**	Республика Корея в вопросах правового регулирования отрасли ИКТ применяет системный подход, который характеризуется те, что каждая сфера цифрового развития предполагает наличие специального закона. Относительно облачных технологий действует Закон «О развитии облачных вычислений и защите ее пользователей» от 27 марта 2015 года №13234 в редакции от 26 июля 2017 года (ACT ON THE DEVELOPMENT OF CLOUD COMPUTING AND PROTECTION OF ITS USERS Act No. 13234, Mar. 27, 2015 Amended by Act No. 14839, Jul. 26, 2017). Закон устанавливает т требования по обеспечению качества облачных услуг и защите информации защиты прав пользователей облачных услуг, прав и обязанностей поставщиков облачных услуг

[44] В таблице приводятся следующие типы недостатков регулирования:
(П) пробел в регулировании (регулирование требуется, но его нет)
(У) устаревшая норма (норма есть, но её нужно менять)
(Н) неработающая норма (норма есть, но в силу описанных причин она не работает)
(Б) действующая норма является необоснованным препятствием для осуществления деятельности

			17 февраля 2022 года Верховной Радой Украины был принят Закон «Об облачных услугах» № 2075-IX, подписанный Президентом Украины 17 марта 2022 года. Закон определяет правовые отношения, возникающие при предоставлении облачных услуг, и устанавливает особенности использования облачных услуг органами государственной власти, органами местного самоуправления, военными формированиями, образованными в соответствии с законами Украины, государственными предприятиями, учреждениями и организациями. властных полномочий и другими субъектами, которым делегированы такие полномочия. Законом вводятся понятия «облака», «технологии облачных вычислений», «облачных услуг». Закон устанавливает следующие виды облачных услуг: - инфраструктура как услуга; - платформа как услуга; - программное обеспечение как услуга; - безопасность как услуга. В соответствии с данным законом Облачные услуги предоставляются: - частным облаком; - коллективным облаком; - публичным облаком; - гибридным облаком. Участниками отношений в сфере облачных услуг являются: - пользователь облачных услуг, включая общественного пользователя; - поставщик облачных услуг; - поставщик услуг центра обработки данных; - органы гос власти. Закон устанавливает требования к поставщику облачных услуг и услуг центра обработки данных, к ведению перечня облачных услуг и/или услуг центра обработки данных. При этом согласно статье 10 Закона облачные услуги и услуги центров обработки данных предоставляются на договорной основе. Типовой договор

			о предоставлении облачных услуг утверждается Кабинетом министров. Предоставление облачных услуг и услуг центра обработки данных публичным пользователям облачных услуг осуществляется с соблюдением требований законодательства о защите персональных данных, о защите информации и о кибербезопасности. В части ограничений по предоставлению облачных услуг следует отметить запрет обработки информации, составляющей государственную тайну, служебной информации, государственных и единых реестров, создание и обеспечение функционирования которых установлено законом, с помощью облачных ресурсов и/или центров обработки данных, размещенных за границей. по своей сути принятый Закон является попыткой внедрения концепции Cloud first на законодательном уровне в Украине.
24.2.	Закон Кыргызской Республики «Об электронном управлении», являясь основным в сфере обеспечения правового регулирования вопросов цифрового развития, устанавливает принципы электронного управления, одним из которых является право участников электронного управления по своему усмотрению использовать любые информационные технологии, если при их использовании выполняются требования, установленные данным Законом и иными законами Кыргызской Республики. В данном случае единственным условием. которое может нарушить Закон может являться хранение в облачных сервисах данных имеющих конфиденциальный характер. Так, статьей 13 устанавливается доступ к информации конфиденциального характера. В этой связи при пользовании облачными сервисами могут устанавливаться ограничения в части хранения данных	**П**	Статья 12 Закона «Об облачных услугах» Украины предусматривает отдельный порядок предоставления облачных услуг, связанных с обработкой государственных информационных ресурсов или с ограниченным доступом. Данный порядок предусматривает: -обязательное резервное копирование и сохранение резервных копий в независимых системах; - передачу данных от пользователя облачных услуг к облачным услугам и/или услугам центра обработки данных для обеспечения облачных услуг, а также от поставщика облачных услуг к пользователю облачных услуг; - передачу данных от одного поставщика облачных услуг и/или услуг центра обработки данных в другой; - предоставление информации, необходимой для оценки безопасности сетевых и информационных систем облачных услуг и/или услуг центра обработки

	относящихся к конфиденциальной информации.		данных, в том числе документально установленной политики безопасности.
24.3	Закон Кыргызской Республики «Об информации персонального характера» определяет условия работы с информацией персонального характера, определяет порядок формирования массивов информации персонального характера, определяет права и обязанности субъектов информации персонального характера, держателей (обладателей) и получателей массивов такой информации. Закон относит персональные данные к конфиденциальной информации. При этом статья 25 Закона допускает трансграничную передачу персональных данных. Одним из условий при трансграничной передаче персональных, находящийся под юрисдикцией Кыргызской Республики, является наличия международного договора между сторонами, согласно которому получающая сторона обеспечивает адекватный уровень защиты прав и свобод субъектов персональных данных и охраны персональных данных, установленный в Кыргызской Республике. Однако использование облачных сервисов может находиться вне юрисдикции какого-либо государства. При передаче персональных данных по глобальной информационной сети (Интернет и т.п.) держатель (обладатель) массива персональных данных, передающий такие данные, обязан обеспечить передачу необходимыми средствами защиты, соблюдая при этом конфиденциальность информации. В этой связи положения Закона с одной стороны допускают передачу персональных данных по сети Интернет и допускают их хранение вне территории Кыргызской Республики, но вопрос возможности их хранения в облачных сервисах	**П**	Анализ практик правового регулирования различных стран показывает, что в вопросах защиты персональных данных трудно определить однозначно лучшую практику, подходящую в условиях Кыргызской Республики. Отчасти к лучшим практикам можно отнести правила Общий регламент по защите данных Европейского Союза (GDPR), согласно которому к поставщикам услуг (ЦОД и облачных сервисов) предъявляются достаточно жесткие требования по защите персональных данных. Поставщики услуг ЦОД и облачных сервисов обязаны следовать следующим основным принципам установленным статьей 5 GDPR: - законность, справедливость и прозрачность — должны быть легальные основания в рамках GDPR для сбора и использования данных, не нарушение любых законов, открытость, честность от начала и до конца об использовании персональных данных; - ограничение целью — обработка должна сводиться к тому, что было заявлено субъекту данных. Все конкретные задачи должны быть закреплены в политике конфиденциальности и должны чётко соблюдаться; - минимизация данных — использование минимально необходимого объёма данных для выполнения поставленных целей; - точность — персональные данные должны быть точными и не должны вводить в заблуждение; ошибочные данные подлежат корректировке; - ограничение хранения данных — не хранить данные дольше, чем нужно, периодически проводить аудит данных и удалять неиспользуемые; -целостность и конфиденциальность/безопасность — хранить данные в безопасном

	остается открытым, поскольку в данном случае для обеспечения защиты прав владельцев персональных данных Закон должен прямо предусматривать возможность хранения персональных данных в облачных сервисах.		месте и уделять достаточное внимание сохранности данных. В рамках обеспечения реализации данных принципов поставщики услуг ЦОД должны также следовать правилам статьи 28 GDPR в части прав и обязанностей обработчика данных, а также статьи 32 защиты данных при обработке. С точки зрения гибкости в правовом регулировании отчасти к лучшим практикам можно отнести и опыт правового регулирования США. Так, в США облачные вычисления не регулируются конкретным «облачным законом», и на их услуги не распространяется прямое регулирование. Вместо этого правовая и нормативная среда состоит из матрицы различных правил, столь же широких, как и область применения самой технологии, охватывающих несколько отраслей. При этом В США облачные вычисления не регулируются конкретным «облачным законом», и на их услуги не распространяется прямое регулирование. При этом в части защиты данных действует ряд нормативных правовых актов, к которым можно отнести Закон Грэмма-Лича-Блайли (GLBA) и Закон о семейных правах на образование и неприкосновенность частной жизни (FERPA). GLBA содержит 2 ключевых правила для «финансовых учреждений», хранящих данные в облаке: правило финансовой конфиденциальности и правило защитных мер. FERPA — защищает информацию об учащихся, собираемую учебными заведениями и связанными с ними поставщиками. Защита информации о студентах в соответствии с правилами FERPA является ключевым моментом при использовании облачных приложений, обрабатывающих записи студентов. ИТ-администраторы должны быть осведомлены об информации,

			которая передается в облачную сеть или приложение .

Комментарии

Исходя из анализа законодательства Кыргызской Республики и обзора практик других стран следует констатировать, что действующее правовое регулирование облачных технологий в Кыргызской Республике является явно недостаточным. В связи с этим обеспечение адекватного правового регулирования облачных технологий может осуществляться по различным моделям. Одним из моделей является регулирование путем принятия специального закона по примеру Кореи, Украины. Другой моделью может быть закрепление вопросов правового регулирования облачных технологий в разных отраслевых нормативных правовых актах как в США, Германии, Франции. Еще одним вариантом может быть оставить вопрос использования облачных технологий на усмотрение пользователей и поставщиков облачных услуг, другими словами осуществлять данные отношения на договорной основе.

Принимая во внимание, реалии сегодняшнего дня и опыт разных стран ни один из перечисленных выше вариантов правового регулирования не может быть оптимальным в чистом виде для Кыргызской Республики. В этой связи, учитывая особенность облачных технологий, а именно, то что облачные хранилища могут находиться вне юрисдикции конкретного государства необходимо законодательно предусмотреть условия использования облачных технологий, при этом не применяя методов жесткого регулирования всего спектра облачных услуг и с точки зрения предоставления права выбора пользователям и поставщикам облачных услуг самим определять варианты взаимодействия. Правовое регулирование облачных сервисов должно быть направлено больше на создание условий и возможностей использования облачных сервисов, по примеру законодательства Кореи. Однако не стоит и забывать вопросы защиты прав и свобод граждан Кыргызской Республики при пользовании различными облачными сервисами. Исходя из этого предлагается рассмотреть законодательное закрепления общих условий применения облачных технологий, в части определения понятия облака, облачных услуг и иных понятий, связанных с облачными вычислениями, прав граждан и юридических лиц возможности использования облачных услуг, защиты персональных данных при трансграничной передаче, случаях и возможностях хранения персональных данных, вопросов кибербезопасности. При этом на подзаконном уровне также важно закрепить требования, порядок предоставления облачных услуг, виды, способы предоставления облачных услуг, использования облачных услуг, требования к поставщикам услуг, центрам обработки данных, модели облачных услуг, модели их развертывания, регулирование государственных облачных сервисов итд.

На наш взгляд такой вариант обеспечения правового регулирования позволит успешно внедрить политику Cloud First (Облако первично) в Кыргызстане, что обеспечит эффективную реализацию национальных стратегических документов в части построения современной цифровой инфраструктуры.

Раздел 25. Технические требования к центрам обработки данных (ЦОД)

Содержание

- ЦОД (общие положения, технические требования)
- стандарты ЦОД

Текущее регулирование (действующее законодательство):

1. Закон Кыргызской Республики «Об электронном управлении»;
2. Закон Кыргызской Республики «Об основах технического регулирования в Кыргызской Республике;
3. Указ Президента Кыргызской Республики «О Национальной программе развития Кыргызской Республики до 2026 года» от 12 октября 2021 года УП №435;
4. Указ Президента Кыргызской Республики «О Национальной стратегии развития Кыргызской Республики на 2018-2040 годы» от 31 октября 2018 года УП № 221;
5. Постановление Правительства Кыргызской Республики «Об утверждении Требований к государственным центрам обработки данных и соединяющим их каналам связи» от 31 декабря 2019 года №747;
6. Постановление Правительства Кыргызской Республики «Об утверждении Требований к защите информации, содержащейся в базах данных государственных информационных систем» от 21 ноября 2017 года №762;
7. Постановление Правительства Кыргызской Республики «О некоторых вопросах, связанных с государственными информационными системами» от 31 декабря 2019 года №744;
8. Распоряжение Кабинета министров Кыргызской Республики от 12 января 2022 года №2-р;
9. Концепция цифровой трансформации «Цифровой Кыргызстан 2019-2023» утвержденное Решением Совета безопасности от 14 декабря 2018 года №2.

Краткое описание выявленных недостатков и ориентиров из мировой практики

№	Описание недостатка	Тип[45]	Лучшая практика
25.1	Закон Кыргызской Республики «Об электронном управлении» предусматривает регулирование только государственных центров обработки данных. Так, согласно части 2 статьи 24 в составе государственной инфраструктуры электронного управления могут использоваться центры обработки данных и соединяющие их каналы связи, как построенные за счет средств республиканского и местных бюджетов, так и используемые на основании договоров аренды,	**П**	Наиболее приемлемым в условиях Кыргызской Республики выглядит установление общих положений по ЦОД включая вопросы поставщиков услуг ЦОД. При этом предусмотреть договорной характер взаимоотношений пользователей с поставщиками по примеру Закона «Об облачных услугах» Украины

[45] В таблице приводятся следующие типы недостатков регулирования:
(П) пробел в регулировании (регулирование требуется, но его нет)
(У) устаревшая норма (норма есть, но её нужно менять)
(Н) неработающая норма (норма есть, но в силу описанных причин она не работает)
(Б) действующая норма является необоснованным препятствием для осуществления деятельности

	оказания услуг, иной договорной основе. В соответствии с пунктом 10 части 2 статьи 6 Правительство Кыргызской Республики утверждает требования к государственным центрам обработки данных и соединяющих их каналам связи. При этом упоминания о других ЦОД не входящих в состав государственной инфраструктуры электронного управления нет.		
25.2	Постановлениями Правительства КР от 31 декабря 2019 года №747 и от 21 ноября 2017 года № 762 установлены основные, базовые требования к ГЦОД, включая более детальные требования к серверным помещениям, установленным и требования к информационным системам. Однако в целом положения указанных нормативных правовых актов не устанавливают каких-то специфичных критериев к параметрам и инженерной инфраструктуре ГЦОД.	**П**	Обзор законодательства ряда стран (Российская Федерация, Казахстан) и существующих стандартов ЦОД (стандарты- EN 50600 Design of Data Centre Facilities and Infrastructures, Стандарты Uptime Institute, ISO ISO27001 и ISO9001) показывает, что требования к ЦОД как правило включают гораздо больше условий и базовых нормативных параметров, чем это предусмотрено в законодательстве Кыргызской Республики. В основном стандарты предусматривают схожие требования к ЦОД. К примеру, стандарт TIA/EIA-942 фиксирует: - требования к месту расположения дата-центра и его структуре; - требования к кабельной инфраструктуре - требования к надежности, специфицированные по уровням инфраструктуры - требования к внешней среде. На сегодняшний день из числа стандартов, применяемых в сертификации ЦОД TIA/EIA-942 является одним из наиболее широко распространенных руководящих документов для специалистов, имеющих непосредственное отношение к проектированию и созданию структурированной кабельной системы в ЦОД. В стандарте TIA/EIA-942 содержатся требования и рекомендации, описывающие ряд тонкостей и моментов, которые необходимо учитывать при проектировании структурированной кабельной системы в дата-центре. В частности,

			данный стандарт содержит детальное описание функциональных подсистем и пассивных элементов структурированных кабельных систем, а также архитектуры структурированной кабельной системы.
25.3	Законодательно не закреплены вопросы стандартизации ЦОД. Законодательством о техническом регулировании не предусмотрены достаточные механизмы принятия на национальном уровне международных стандартов.	**П**	Одним из вариантов обеспечения стандартизации является принятие национальных стандартов к телекоммуникационной инфраструктуре, гармонизированных с международными стандартами по уровням надежности инженерной инфраструктуры ЦОД по примеру Республики Казахстан.

Комментарии

Закон Кыргызской Республики «Об электронном управлении» вступивший в силу 25 июля 2017 года закрепил задачи и принципы электронного управления, полномочия отдельных государственных органов в сфере электронного управления. Статья 24 Закона дает определение государственных центров обработки данных. Так, в соответствии с данной статьей Закона «государственные центры обработки данных и соединяющие их каналы связи предназначены для размещения и функционирования государственных информационных систем. В составе государственной инфраструктуры электронного управления могут использоваться центры обработки данных и соединяющие их каналы связи, как построенные за счет средств республиканского и местных бюджетов, так и используемые на основании договоров аренды, оказания услуг, иной договорной основе. Требования к государственным центрам обработки данных и соединяющим их каналам связи, включая требования к устойчивости и защищенности, а также порядок включения центров обработки данных и соединяющих их каналов связи в состав государственной инфраструктуры электронного управления устанавливаются Правительством Кыргызской Республики».

Согласно пункту 4 части 3 статьи 18 Закона центры обработки данных входят в состав государственной инфраструктуры электронного управления. При этом

В соответствии с пунктом 10 статьи 6 данного Закона требования к государственным центрам обработки данных и соединяющих их каналам связи, в том числе требования по их защищенности и устойчивости, а также порядок включения центров обработки данных и соединяющих их каналов связи в состав государственной инфраструктуры электронного управления утверждает Правительство Кыргызской Республики.

В реализацию указанного положения Закона Правительством Кыргызской Республики принято постановление «Об утверждении Требований к государственным центрам обработки данных и соединяющим их каналам связи» от 31 декабря 2019 года №747. Требования устанавливают цели и задачи государственных центров обработки данных (далее- ГЦОД), их параметры и структуру, также определяют требования по защищенности и устойчивости ГЦОД и соединяющих их каналов связи. Согласно данному постановлению основными параметрами ГЦОД являются

- высокая скорость обработки запросов (скорость не должна зависеть от объема хранилища данных);

- параллельное обслуживание заданного числа пользователей без заметного для пользователей снижения производительности.

В части структуры ГЦОД устанавливается, что структура ГЦОД включает информационную, телекоммуникационную, инженерную инфраструктуру.

Информационная инфраструктура включает высоконадежное серверное оборудование и программное обеспечение, обеспечивающие основные функции ГЦОД - обработку и хранение информации.

Телекоммуникационная инфраструктура обеспечивает взаимосвязь элементов ГЦОД, а также передачу данных между ГЦОД и пользователями.

Требования к размещению ГЦОД регулируются требованиями к защите информации, содержащейся в базах данных государственных информационных систем, утвержденных постановлением Правительства Кыргызской Республики от 21 ноября 2017 года № 762. (далее -постановление 762) Этим постановлением устанавливаются Требования к системам бесперебойного функционирования технических средств серверного оборудования и к серверному помещению государственного органа, органа местного самоуправления, организации.

Таким образом вышеуказанными решениями Правительства установлены основные, базовые требования к ГЦОД, включая более детальные требования к серверным помещениям, установленным постановлением 762 и требования к информационным системам, утвержденные постановлением 744. Однако в целом положения указанных нормативных правовых актов не устанавливают каких-то специфичных критериев к параметрам и инженерной инфраструктуре ГЦОД.

В условиях необходимости обеспечения достаточного правового регулирования государственных центров обработки данных следует обратить внимание на законодательство Кыргызской Республики о техническом регулировании. С 22 мая 2004 года действует Закон Кыргызской Республики «Об основах технического регулирования в Кыргызской Республике». Закон устанавливает правовые основы в области:

-разработки, принятия, применения и исполнения обязательных требований к продукции, в том числе к зданиям и сооружениям, и/или к связанным с требованиями к продукции процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, хранения, перевозки, реализации, эксплуатации и утилизации;

- разработки, принятия, применения и исполнения на добровольной основе требований к продукции или процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, хранения, перевозки, реализации, эксплуатации, утилизации, выполнению работ, оказанию услуг.

Согласно статье 2 одним из принципов технического регулирования является единство правил установления требований к продукции или процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, хранения, перевозки, реализации, эксплуатации, утилизации, выполнению работ или оказанию услуг.

Указанный Закон устанавливает принципы, цели и порядок принятия технических регламентов, стандартизации и подтверждения соответствия. В соответствии со статьей 14 стандартизация осуществляется в целях:

- стимулирования научно-технического прогресса;
- повышения конкурентоспособности продукции, работ и услуг в соответствии с уровнем развития науки, техники и технологии;
- повышения уровня безопасности объектов с учетом степени риска возникновения чрезвычайных ситуаций природного и техногенного характера;
- содействия соблюдению требований технических регламентов;
- обеспечения энергетической эффективности и ресурсосбережения;
- технической и информационной совместимости;
- обеспечения единства измерений, сопоставимости результатов измерений и испытаний;
- взаимозаменяемости продукции;
- повышения уровня безопасности жизни, здоровья физических лиц, а также жизни и здоровья животных и растений, имущества физических и юридических лиц, государственного и муниципального имущества, окружающей среды.

Согласно статье 15 одними из принципов стандартизации являются добровольность применения стандартов и использование международных, региональных стандартов и правил как основы для подготовки национальных стандартов. Статья 16 устанавливает, что «международные, региональные стандарты и национальные стандарты других стран, а также региональные своды правил и своды правил иностранных государств принимаются в Кыргызской Республике в качестве национальных документов по стандартизации согласно методике, установленной национальным органом по стандартизации».

При этом на сегодняшний день такой методики, установленной национальным органом по стандартизации нет.

Исходя из вышеизложенного следует, что законодательство Кыргызской Республики устанавливает базовые требования к ГЦОД, при этом не охватывает деятельность других (частных) ЦОД. В этой связи, вопрос правового регулирования негосударственных ЦОД следует рассматривать с точки зрения права участников электронного управления по своему усмотрению использовать любые информационные технологии, если при их использовании выполняются требования, установленные Законом “Об электронном управлении” и иными законами Кыргызской Республики. Однако для частных ЦОД не предусмотрены какие-либо требования.

Исходя из вышеизложенного, в условиях Кыргызской Республики применение каких-либо жестких требований к ЦОД не представляется целесообразным. Вопрос установления требований к сертификации государственных центров обработки данных также вызывает вопросы, поскольку сертификация по общепризнанным мировым стандартам требует большого объема финансовых средств.

Исходя из вышеизложенного, предлагается законодательно закрепить общее понятие ЦОД и установить, что услуги ЦОД предоставляются на договорной основе (данное положение применять отдельно от ГЦОД), при этом определить какие обязательные условия должен содержать договор. Это будет относиться и к вопросу применения облачных услуг.

В части стандартизации и улучшения требований к ЦОД предлагается несколько вариантов совершенствования правового регулирования как ГЦОД, так и ЦОД в целом.

1) действующие положения нормативных правовых актов Кыргызской Республики необходимо дополнить более специфичными параметрами, установленными в общепризнанных стандартах, которые будут призваны обеспечить необходимую безопасность, энергоэффективность, отказоустойчивость ЦОД;

2) принятие национальных стандартов к телекоммуникационной инфраструктуре, гармонизированных с международными стандартами по уровням надежности инженерной инфраструктуры ЦОД. При этом важно обеспечить соответствие основных параметров проектирования, размещения, эксплуатации, энергоэффективности, отказоустойчивости, и др. с указанными стандартами.

3) принятие международных стандартов или стандартов иностранных государств как национальных. В данном случае необходимо законодательно закрепить правила и порядок принятия таких стандартов как национальных (возможно разработать и утвердить методику в соответствии с законодательством о техническом регулировании).

Раздел 30. Кибербезопасность

Содержание:

- Уголовно-правовая и административная ответственность;
- Цифровые доказательства в уголовном судопроизводстве;
- Цифровые доказательства в гражданском судопроизводстве;
- Защита информации и кибербезопасность.

Текущее регулирование (действующее законодательство)

1. Уголовный кодекс Кыргызской Республики;
2. Уголовно-процессуальный кодекс Кыргызской Республики;
3. Кодекс Кыргызской Республики о правонарушениях;
4. Закон Кыргызской Республики «О защите государственных секретов Кыргызской Республики»;
5. Закон Кыргызской Республики «Об электронном управлении»;
6. Закон Кыргызской Республики «Об информации персонального характера»
7. Закон Кыргызской Республики «О гарантиях и свободе доступа к информации»;
8. Закон Кыргызской Республики «Об электрической и почтовой связи»;
9. Закон Кыргызской Республики «Об электронной подписи»;
10. Закон Кыргызской Республики «О правовой охране программ для ЭВМ и баз данных»;
11. Закон Кыргызской Республики «Об основах технического регулирования в Кыргызской Республике»;
12. Указ Президента Кыргызской Республики «О Национальной стратегии развития Кыргызской Республики на 2018-2040 годы» от 31 октября 2018 года УП №221;
13. Указ Президента Кыргызской Республики «О Концепции национальной безопасности Кыргызской Республики» от 20 декабря 2021 года УП №570;
14. Постановление Правительства Кыргызской Республики «О Концепции информационной безопасности Кыргызской Республики на 2019-2023 годы» от 3 мая 2019 года №209;
15. Постановление Правительства Кыргызской Республики «Об утверждении Стратегии кибербезопасности Кыргызской Республики на 2019-2023 годы» от 24 июля 2019 года №369;
16. Постановление Правительства Кыргызской Республики «Об утверждении Требований к защите информации, содержащейся в базах данных государственных информационных систем» от 21 ноября 2017 года №762;
17. Постановление Правительства Кыргызской Республики «О вопросах организации и управления государственными предприятиями Кыргызской Республики в сфере цифровизации» от 4 июля 2019 года №340;
18. Концепция цифровой трансформации «Цифровой Кыргызстан 2019-2023».

Краткое описание выявленных недостатков и ориентиров из мировой практики

№	Описание недостатка	Тип[46]	Лучшая практика
30.1	Существующие статьи Уголовного кодекса не в полной мере отвечают современным и потенциальным угрозам в киберпространстве.	**П/У/Н**	В настоящее время Будапештская Конвенция о компьютерных преступлениях 2001 года является базовым международным документом, который может стать

[46] В таблице приводятся следующие типы недостатков регулирования:
(П) пробел в регулировании (регулирование требуется, но его нет)
(У) устаревшая норма (норма есть, но её нужно менять)
(Н) неработающая норма (норма есть, но в силу описанных причин она не работает)
(Б) действующая норма является необоснованным препятствием для осуществления деятельности

	Недостаточность законодательства, формирующего уголовно-правовые основы для борьбы с киберпреступлениями, не отвечающего современным потребностям правоприменителей, не позволяет: успешно пресекать киберпреступления; объективно оценить масштабы киберпреступности; выстроить эффективную правовую базу для противодействия киберпреступности. Специальные термины, используемые по всему тексту Уголовного кодекса, не соответствуют терминологическому глоссарию, используемому в специальных международных актах и стратегических документах в области кибербезопасности, а также в национальном законодательстве, регулирующем сектор связи и телекоммуникаций. Некоторые квалифицирующие признаки преступлений, предусмотренных данной Главой 40, уже охватываются признаками других составов преступлений. Некоторые составы преступлений иных категорий, помимо указанной Главы, не содержат квалифицирующих признаков совершения преступлений с использованием Интернет, компьютерных технологий.		основой для формирования национальной уголовно-правовой базы по борьбе с кибепреступлениями и позволит гармонизировать национальное законодательство с международным. Учитывая трансграничный характер киберпреступлений такой подход в формировании отечественного законодательства очень важен с точки зрения необходимости создания условий для эффективного сотрудничества с другими странами мира. Будапештская конвенция стала открытой для подписания более 20 лет назад, с 23 ноября 2001 года. На сегодняшний день Конвенцию ратифицировали 66 стран, две подписали ее и 10 получили приглашения присоединиться. Более 140 стран работают с Советом Европы над укреплением своего законодательства и потенциала по борьбе с киберпреступностью. Данная конвенция является самым первым международным договором о преступлениях, совершенных через Интернет и другие компьютерные сети, и касается, в частности, нарушений авторских прав, компьютерных мошенничеств, детской порнографии и нарушений безопасности сети. Также следует обратить внимание на создание уголовно-правовой основы для привлечения к ответственности лиц, совершивших деяния, связанные с противозаконным доступом, перехватом данных с использованием технических средств, воздействия на информацию и функционирование системы, противозаконное использование устройств, мошенничество с использованием информационно-коммуникационных технологий и т.п. Также необходимо обеспечить реализацию требований Закона Кыргызской Республики «Об информации персонального характера», который подразумевает

			наличие ответственности за нарушение требований законодательства о персональных данных. Кроме этого, весьма важно унифицировать термины и понятия не только с Будапештской конвенцией, но и с глоссарием МСЭ, международными стандартами, Стратегией кибербезопасности и законодательством Кыргызской Республики в области связи и телекоммуникаций, в том числе в целях обеспечения принципа правовой определенности. Необходимо четко разграничить квалифицирующие признаки составов преступлений. При этом важно унифицировать термины и понятия с Будапештской конвенцией, глоссарием МСЭ, международными стандартами, Стратегией кибербезопасности и законодательством Кыргызской Республики в области связи и телекоммуникаций. Необходимо рассмотреть вопрос внесения изменений в части квалифицирующих признаков совершения преступлений с использованием Интернет, компьютерных технологий в ряд статей Уголовного кодекса, в частности в статью 161. Распространение предметов порнографического характера, статья 204. Нарушение авторских, смежных прав и прав патентообладателей и иные статьи. Конечно же нужно изучить и рассмотреть вопрос единообразной квалификации киберпреступлений на уровне правоохранительных органов, прокуратуры и суда.
30.2	Специальные нормы Кодекса о правонарушениях не отвечают современным и потенциальным угрозам в киберпространстве. Существует конкуренция правовых норм Уголовного кодекса и Кодекса о правонарушениях в части преюдиции.	**П/У/Н**	Требуется унификация терминов и понятий с Будапештской конвенцией, глоссарием МСЭ, международными стандартами, Стратегией кибербезопасности и законодательством Кыргызской Республики в области связи и телекоммуникаций, в том числе в

	Используемые термины не соответствуют терминологии действующего уголовно-правового законодательства, международных актов и требований. Требуется кардинальный пересмотр главы 26 Кодекса о правонарушениях, в том числе через призму необходимости создания условий для уголовно-правовой защиты от нарушения существующих требований законодательства в области защиты информации персонального характера.		целях обеспечения принципа правовой определенности. Также необходимо обеспечить реализацию требований Закона Кыргызской Республики «Об информации персонального характера», который подразумевает наличие ответственности за нарушение требований законодательства о персональных данных. Одним из методов обеспечения неукоснительного соблюдения правовых норм сторонами правоотношений, связанных с обработкой персональных данных, прежде всего является наличие юридической ответственности за нарушение норм права. В условиях отсутствия юридических оснований для привлечения к ответственности лиц, виновных в нарушении законов органы государственной власти не могут обеспечить режим законности, как важной составляющей правового государства, который предполагает гарантии выполнения содержащихся в нормах права предписаний. Именно законодательное установление процедуры обеспечения законности будет восприниматься гражданами как закрепление их реальных возможностей, обеспеченных государством. Особенно это актуализируется в условиях, когда государственные органы используют биометрические данные граждан для обеспечения эффективной цифровой трансформации государственного управления и прозрачности избирательного процесса. В перспективе предусматривается активное использование информационно-коммуникационных технологий для достижения целей модернизации государственного управления, экономики и социальной сферы посредством инновационных технологий, где основным идентификатором гражданина будет выступать только его персональные

			данные. В данных условиях важно предусмотреть ответственность за: − обработку персональных данных без законного основания; − необоснованный отказ в представлении субъекту персональных данных информации, касающейся обработки его персональных данных; − невыполнение законных требований уполномоченного государственного органа по персональным данным; − необоснованный отказ уполномоченному государственному органу по персональным данным или Омбудсмену (Акыйкатчы) Кыргызской Республики.
30.3	Действующее уголовно-процессуальное законодательство не предусматривает правовых основ сбора, хранения, обработки и представления, а также оценки электронных (цифровых) данных для целей последующего доказывания	**П**	В настоящее время Будапештская Конвенция о компьютерных преступлениях 2001 года является базовым международным документом, который может стать основой для формирования национальной уголовно-процессуальной базы по борьбе с кибепреступлениями и позволит гармонизировать национальное законодательство с международным. Учитывая трансграничный характер киберпреступлений такой подход в формировании отечественного законодательства очень важен с точки зрения необходимости создания условий для эффективного сотрудничества с другими странами мира. Будапештская конвенция стала открытой для подписания более 20 лет назад, с 23 ноября 2001 года. На сегодняшний день Конвенцию ратифицировали 66 стран, две подписали ее и 10 получили приглашения присоединиться. Более 140 стран работают с Советом Европы над укреплением своего законодательства и потенциала по борьбе с киберпреступностью. Данная конвенция содержит ряд полномочий и процедур, таких как обыск компьютерных данных, сетей и

			перехват, определяет принципы международного сотрудничества при расследовании киберпреступлений, обмена технической информацией. Также следует обратить внимание на создание уголовно-процессуальной основы для собирания доказательств и дальнейшего привлечения к ответственности лиц, совершивших киберпреступления, в том числе на территории других государств мира, в том числе внести изменения в УПК в части сбора, хранения и оценки электронных данных (доказательств).
30.4	Закон «Об электронном управлении» содержит ряд положений, касающихся вопросов защиты данных и обеспечения информационной безопасности. Большинство указанных норм частично декларируют фундаментальные принципы и направления защиты информации, которые необходимо принимать во внимание и соблюдать при выстраивании системы электронного управления. Но нужно признать, что данные нормы не утратили своей актуальности по сей день, соответствуют существующим парадигмам в области защиты данных, а также коррелируются с отдельными международными принципами и подходами в области кибербезопасности, где главенствующей ролью выступают права и свободы человека. Однако, такая регламентация вопросов кибербезопасности является недостаточной. Кроме этого данные нормы в большей степени можно охарактеризовать как неработающие, хотя и не утратили актуальности. Указанные в Законе положения о защите информации не нашли своей комплексной практической реализации. Многие концептуальные нормы не получили в дальнейшем нормативно очерченные механизмы исполнения. К примеру, статья 3 предусмотрела, что одной из задач электронного	**Н**	Современные тенденции кибербезопасности вышли за пределы традиционных подходов защиты информации. Сегодня появился термин «цифровая устойчивость», которая предполагает системный подход, ориентированный на предотвращение и адаптивность, включающий в себя вопросы управления рисками и состоящий из: предотвращения, сокращения, готовности, реагирования и восстановления. Теперь эта концепция была также направлена на правительства. Это более комплексный подход, требующий активного участия всех заинтересованных сторон, включая правительство, бизнес и гражданское общество. Цифровая устойчивость сегодня - это набор возможностей, методов и благоприятных условий, которые обеспечивают непрерывность деятельности правительства, бизнеса и общества перед лицом изменений в окружающей среде, включая техногенные катастрофы и другие кризисы. Мы должны переосмыслить кибербезопасность как цифровую устойчивость - набор стратегий, практик и возможностей, которые помогают нам предвидеть, готовить, предотвращать и реагировать на неизбежные кризисы и катастрофы, которые будут зависеть от нашего все более зависимого от цифровых

	управления является обеспечение информационной безопасности Кыргызской Республики. Эта задача носит всеобщий характер и налагает обязанности в том числе по защите объектов критической информационной инфраструктуры как на государство, так и на самих субъектов – обладателей массивов информации, что предполагает детализированное подзаконное нормативное регулирование правоотношений в этой сфере.		технологий общества и оказывать на него влияние. Смысл заключается в том, чтобы признать, что цифровая трансформация и цифровая устойчивость идут рука об руку. На прикладном уровне цифровая устойчивость состоит из четырех ключевых основ/компонентов: непрерывность, кибербезопасность, данные и конфиденциальность, а также цифровое гражданство.
30.5	В Стратегии кибербезопасности на 2019-2023 годы, при выстраивании архитектуры ключевых игроков, входящих в государственную систему обеспечения кибербезопасности, и определения их зон ответственности был допущен перекос в сторону милитаризации системы. При этом, не были приняты во внимание роль гражданских государственных органов и частных структур, а также не рассмотрены возможные преимущества государственно-частного партнерства в этой области. Многие важные положения Стратегии остаются не реализованными. В первую очередь это касается принципа приоритетного обеспечения кибербезопасности критической информационной инфраструктуры. Стратегия определила в качестве одной из приоритетных задач необходимость формирования единой системы обеспечения безопасности критической информационной инфраструктуры Кыргызской Республики. Однако до сих пор законодательно: - не определены секторы, отрасли и сферы деятельности, в которых функционируют объекты критической информационной инфраструктуры, в том числе государственные системы; - не утверждены критерии и параметры, определяющие принадлежность объектов к	**Б/У/Н**	Необходимо принять во внимание рекомендации Группы экспертов Комиссии по предупреждению преступности и уголовному правосудию при Генеральной Ассамблеи ООН, которые были изложены в Докладе о работе совещания Группы экспертов для проведения всестороннего исследования проблемы киберпреступности, прошедшего в Вене 27–29 июля 2020 года. В частности, рекомендуется привлечь к усилиям по предупреждению и противодействию киберпреступности неправительственные организации и научные круги, ведь их участие позволяет обеспечить максимально широкий, разносторонний и всеобъемлющий взгляд на проблему и, в частности, гарантировать защиту прав человека, свободу слова и неприкосновенность частной жизни. Кроме этого, как указывалось выше современные тенденции кибербезопасности вышли за пределы традиционных подходов защиты информации. Сегодня необходимо использовать подход, ориентированный на предотвращение и адаптивность, включающий в себя вопросы управления рисками и состоящий из: предотвращения, сокращения, готовности, реагирования и восстановления, то есть говорить о цифровой устойчивости. Это более комплексный подход, требующий активного участия всех

	критической информационной инфраструктуре; - не установлены обязательные требования по обеспечению безопасности их объектов для операторов критической информационной инфраструктуры. Также не реализованы положения Стратегии, касающиеся: - вопросов криминализации составов компьютерных преступлений в соответствии с международными подходами к борьбе с киберпреступностью; - методов и средств компьютерной криминалистики, введение в нормативные правовые акты понятия цифрового доказательства, описание и изложение его критериев, характеристик и способов фиксации; - обеспечения признания юридической силы цифровых доказательств наравне с другими доказательствами; - гармонизации законодательства Кыргызской Республики в части криминализации составов и расследования компьютерных преступлений, трансграничной выдачи с территории Кыргызской Республики лиц, подозреваемых в совершении компьютерных преступлений, либо осужденных за их совершение на территории зарубежных государств; - рассмотрение возможности привлечения частных компаний к сбору цифровых доказательств и проведению судебных экспертиз по цифровым доказательствам для правоохранительных органов Кыргызской Республики.		заинтересованных сторон, включая правительство, бизнес и гражданское общество. На прикладном уровне цифровая устойчивость состоит из четырех ключевых основ/компонентов: непрерывность, кибербезопасность, данные и конфиденциальность, а также цифровое гражданство.
30.6	Постановлением Правительства Кыргызской Республики от 21 ноября 2017 года № 762 были утверждены Требования к защите информации, содержащейся в базах данных государственных информационных систем, которые определяют меры по защите информации, а также государственных информационных	**Н/У**	Несмотря на такие обстоятельства данное Положение актуально и по сегодняшний день, за исключением отдельных положений организационно-технического характера, требующих закономерного пересмотра. Так как с момента принятия постановления прошло более пяти лет. За это время сменились парадигмы обеспечения

	системах и обеспечения безопасности информации, содержащейся в их базах данных. В частности, устанавливаются требования к использованию информационных технологий, к организации кибербезопасности, к информационным системам, к прикладному программному обеспечению, к технологическим платформам, к аппаратно-программным комплексам, к сетям телекоммуникаций, к системам бесперебойного функционирования технических средств серверного оборудования и к серверному помещению. То есть данное постановление практически регламентирует все основные практические аспекты, касающиеся защиты данных и обеспечения кибербезопасности в государственных информационных системах. Однако, на практике данные требования в большинстве случаев не реализуются. До сегодняшнего дня не введены должности специалистов в области кибербезопасности, не говоря уже о специальных подразделениях. Отсутствуют достаточные силы и средства, а также не определены четкие механизмы проведения проверок на соответствие указанным требованиям. На наш взгляд, основными причинами неисполнение данных требований является отсутствие достаточного понимания у большинства руководителей государственных органов и предприятий, несоответствие уровня компетенции сотрудников государственных органов для правильного понимания требований и их применения на практике. По результатам бесед и обсуждений данной проблематики с экспертами и представителями компетентных государственных органов становится очевидным, что в целом у государственной службы не сформирован необходимый уровень		кибербезопасности, были разработаны новые, более эффективные и технологичные подходы и методы обеспечения кибербезопасности. В данном контексте возможно применить отдельные положения и принципы американского национального института стандартов и технологий (NIST), в том числе Минимальные требования безопасности для Федеральных информационных систем и информации федерального значения. Этот стандарт определяет спецификацию минимальных требований безопасности для государственных информационных систем (организационных, эксплуатационных и технических мер).

	понимания и компетенции, а также отсутствует достаточное финансирование для исполнения данных требований, за исключением Министерства цифрового развития Кыргызской Республики и Государственного комитета национальной безопасности Кыргызской Республики.		

Комментарии

Процесс повсеместной цифровизации необратим, поскольку создаваемые им возможности для сокращения издержек в самом широком смысле, оптимизации цепочек создания добавленной стоимости и генерации экономических и общественных благ слишком велики и не могут быть достигнуты какими-либо иными средствами на данном этапе развития цивилизации. Однако из необратимости этих изменений напрямую вытекает и необратимость, неизбежность рисков и угроз безопасности, которые несет с собой развитие ИКТ и цифровой экономики. Прежде всего речь идет:

- о рисках безопасности и устойчивости критической инфраструктуры, функционирование которой все в большей степени оказывается замкнуто на цифровые бизнес-процессы. Одновременно с этим возрастают риски, связанные с развитием трансграничной компьютерной преступности;
- об активизации террористической и экстремистской деятельности, осуществляемой при помощи цифровых коммуникаций;
- о возрастающих масштабах государственного и корпоративного кибершпионажа.

Кыргызстан значительно отстает от мировых тенденций в области кибербезопасности. Сегодня парадигма обеспечения кибербезопасности начала меняться и все больше государств и компаний приходят к понимаю, что построение защиты, которую нельзя сломать, - утопично по своей сути. Еще несколько лет назад информационные технологии расценивались, в большей степени, как средства облегчения документооборота и автоматизации бизнес-процессов[47]. В связи с этим наблюдался рост востребованности высокоинтеллектуальных средств защиты, позволяющих решать задачи по своевременному выявлению атак и инцидентов (системы класса security information and event management (SIEM), network traffic analysis (NTA), комплексных antiAPT решениях[48]). В таких условиях главной задачей любой системы безопасности было максимально быстро обнаружить атаку и атакующего в системе, сократить окно его возможностей настолько, чтобы он не успел нанести непоправимый вред. Достаточно было создать необходимый периметр безопасности, которая будет нацелена на поиск и обнаружение нарушителя периметра безопасности. Однако в условиях, когда процессы выходят за пределы периметра безопасности, непрерывного развития технологий, когда субъекты становятся более мобильными размываются конкретные периметры безопасности. При таком стечении обстоятельств становится сложным найти точку применения вышеуказанных инструментов безопасности. В связи с этими рисками мы должны принять их и понимать, что предотвратить киберпреступления практически невозможно.

Учитывая данные обстоятельства IT-сообщество, в 2018-2020 годах кроме защиты информации все больше говорит об обеспечении **киберустойчивости**, суть которой заключается в обеспечении бесперебойного и устойчивого функционирования информационной инфраструктуры в условиях существования постоянных рисков кибербезопасности. Тем самым основные усилия необходимо направить на проектирование систем с учетом требований обеспечения их киберустойчивости. При этом, одним из основных

[47] https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/cybersecurity-2019-2020-rus.pdf
[48] https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-2019-2020/

и важных направлений обеспечения киберустойчивости является устойчивость международных Интернет соединений. Так как, в условиях развития цифровой экономики, финансовый и бизнес секторы, при осуществлении международных транзакций и других видов международного взаимодействия, все больше используют технологические возможности Интернета. В итоге большинство международных экспертов приходят к тому, что в реалиях XXI века существует острая необходимость в движении в сторону киберустойчивости, которая подразумевает способность быстрого восстановления после киберинцидентов.

Более того, современные тенденции кибербезопасности уже выходят за пределы традиционных подходов защиты информации, в том числе киберустойчивости. Сегодня появился термин **«цифровая устойчивость»**, которая предполагает системный подход, ориентированный на предотвращение и адаптивность, включающий в себя вопросы управления рисками и состоящий из: предотвращения, сокращения, готовности, реагирования и восстановления. Теперь эта концепция была также направлена на правительства. Это более комплексный подход, требующий активного участия всех заинтересованных сторон, включая правительство, бизнес и гражданское общество.

Цифровая устойчивость сегодня - это набор возможностей, методов и благоприятных условий, которые обеспечивают непрерывность деятельности правительства, бизнеса и общества перед лицом изменений в окружающей среде, включая техногенные катастрофы и другие кризисы.

Необходимо переосмыслить кибербезопасность как цифровую устойчивость - набор стратегий, практик и возможностей, которые помогают нам предвидеть, готовить, предотвращать и реагировать на неизбежные кризисы и катастрофы, которые будут зависеть от нашего все более зависимого от цифровых технологий общества и оказывать на него влияние.

Один из уроков заключается в том, чтобы признать, что цифровая трансформация и цифровая устойчивость идут рука об руку.

На прикладном уровне цифровая устойчивость состоит из четырех ключевых основ/компонентов: непрерывность, кибербезопасность, данные и конфиденциальность, а также цифровое гражданство.

1) Кибербезопасность: состоит из стандартов, практики и людских ресурсов, необходимых для поддержания функционирования цифровых систем и обеспечения безопасной цифровой экосистемы. Она включает в себя систему управления рисками, которая позволяет лицам, принимающим решения, рассчитывать величину риска, связанного с цифровыми системами, и регулярно поддерживать возможности, достаточные для прогнозирования и реагирования на инциденты и чрезвычайные ситуации на постоянной основе.

2) **Непрерывность** - включает планирование и возможности для управления кризисными ситуациями и восстановления, которые практикуются для обеспечения того, чтобы учреждения и организации могли продолжать функционировать в неблагоприятных условиях. Непрерывность зависит от наличия соответствующих правил и стандартов, которые обеспечивают непрерывность бизнеса и операций, обеспечивая при этом быструю адаптацию в рамках предсказуемого и общепринятого набора правил и передовой практики.

3) **Защита данных и конфиденциальность** включают в себя надежную экосистему данных, состоящую из законов, учреждений и возможностей, которые определяют и регулируют сбор, хранение и удаление данных. Функционально это включает в себя определение прав собственности и то, как данные, включая личную информацию, собираются и используются правительствами, предприятиями и другими третьими сторонами. Конфиденциальность и защита данных важны для предотвращения ущерба, обеспечения целостности государственных и деловых операций и защиты отдельных лиц от потенциальных злоупотреблений или эксплуатации, а также для обеспечения экономической деятельности.

4) **Цифровое гражданство** означает готовность граждан пользоваться преимуществами цифровых систем и инфраструктуры. Цифровое гражданство включает в себя базовую компьютерную грамотность, базовые методы цифровой гигиены и навыки, обеспечивающие безопасность и безопасность работы в Интернете, а также осведомленность о правах и обязанностях использования цифровых систем и данных.

Целью Правительства для достижения цифровой устойчивости является создание благоприятной (в том числе нормативно правовой) среды и возможностей для всех сторон (самого государства, бизнеса, гражданского общества). Результатом должны стать собственно возможность устойчивости; Управление данными и конфиденциальность; Непрерывность цифровых услуг. Что нужно для этого сделать на правительственном уровне:

- обеспечить устойчивость национальных сетей и цифровых активов, в том числе критической информационной инфраструктуры;
- образовать гражданский государственный орган, ответственный за цифровую устойчивость Center for Digital Resilience – важный компонент. Мы долго говорили о необходимости созданий групп реагирования на кибер атаки – CERT, сегодня нам уже нужен национальный орган цифровой устойчивости;
- информировать и обучать (всех) в области цифровой гигиены на системной основе;
- подготовить и обучить специалистов, работающих в критических секторах экономики и государственного управления;
- пересмотреть законодательство, разработать стандарты.
- стимулировать расширение доступа к широкополосному Интернету;
- предоставить доступ к национальным облачным ресурсам для бизнеса;
- обеспечить перевод государственных услуг в онлайн формат (в первую очередь важных для бизнеса - налогообложение, лицензирование и регистрация).
- поддержать цифровое образование;
- обеспечить надежный доступ к централизованным онлайновым образовательным ресурсам для учителей и учащихся;
- обеспечить доступ к оборудованию и программному обеспечению; а также к высококачественной широкополосной связи;
- расширить доступ к медицинским услугам (развитие телемедицины);
- ускорить доступ к цифровым транзакциям (фин-тех, «песочницы», электронная торговля).

Другой тенденцией мировой практики в области обеспечения кибербезопасности является использование подходов по обеспечению **безопасности цепочки поставок (Supply chain security)**, суть которой заключается в обеспечении безопасности всей цепочки поставок (товаров, услуг, работ и т.д.). Сегодня цепь поставок становится транснациональной и глобальной, безопасность цепочек поставок становится все более важной. Наличие широкого круга рисков кибербезопасности, в том числе связанных с человеческим фактором, у одного участника может вызвать трудности у всех остальных партнеров, взаимосвязанных между собой информационно-коммуникационными технологиями. В большинстве случаев мы сталкиваемся с проблемами, когда поставляемое информационно-телекоммуникационное оборудование или программные продукты намеренно или неосознанно поставляется с нелицензированным программным обеспечением или уже с установленными вредоносными программами. То есть, из-за взаимосвязанности цепочек поставок слабая безопасность одного звена может поставить под угрозу функциональность всей цепочки поставок. Атака на цепочку поставок может произойти в любой отрасли, как в финансовом, так и в государственном или частном секторе.

Атаки на цепи поставок особенно опасны потому, что в случае успеха это открывает доступ к сотням или даже тысячам компаний. К примеру, согласно последнему анализу, средняя стоимость взлома данных составляет 3,86 миллиона долларов, а мега-утечка

(похищение 50 миллионов записей и более) достигает 392 миллиона долларов[49]. Одной из последних кибератак, осуществлённой на цепочку поставок можно назвать атаку на компанию SolarWind, которая занимается ИТ инфраструктурой и имеет около 33 000 клиентов по всему миру. При данной атаке уязвимым стали около 18000 клиентов компании, которые имеют платформу программного обновления SolarWind Orion.

Кроме вышеназванных тенденций в области обеспечения кибербезопасности многие страны начали обращать особое внимание на вопросы **обеспечения безопасности критической информационной инфраструктуры** (далее – КИИ). В мировой практике существует различные подходы в регулировании безопасности КИИ. По результатам сравнительно-правового анализа таких подходов в качестве обобщения можно выделить две основные модели регулирования безопасности КИИ в зависимости от непосредственного предмета регулирования: «объектную» (РФ, Казахстан, Германия) и «субъектно-деятельностную» (ЕС кроме Германии, Грузия, Сингапур, Китай, Япония).

В ряде юрисдикций выделенных моделей можно найти наличие сходных терминов, аналогичные обязанности субъектов КИИ, идентичные полномочия компетентных органов в сфере обеспечения безопасности КИИ, установление административной и уголовной ответственности за нарушения в сфере КИИ. Указанное объясняется общей целью соответствующего регулирования – обеспечение безопасности КИИ.

Особенностями «объектной» модели являются направленность регулирования непосредственно на объекты КИИ, наличие иерархически стройной системы регулирования, построение терминологического аппарата от определения КИИ и ее объектов, установление четких критериев категорирования через формирование «пороговых значений», точное определение обязанностей субъектов на транспарентной основе, основные обязанности содержатся в Законе и ограниченность количества уполномоченных органов с четко-определенной компетенцией.

Указанный подход позволяет, с одной стороны, упорядочить гражданский оборот (новый собственник объекта понимает, к какой категории он относится и какие обязанности на него будут возложены), с другой – упрощает задачу государственным органам по осуществлению контроля за владельцами таких объектов даже в тех случаях, если последние неправильно осуществили категорирование.

Вместе с тем, указанному подходу недостает гибкости в части установления требований к безопасности конкретного объекта.

В отличие от вышеуказанной модели «Субъектно-деятельностная» модель имеет другие особенности, которые заключаются в регулировании деятельности субъектов в сфере КИИ, разрозненности нормативного правового регулирования, построении терминологического аппарата от определения жизненно-важных услуг (сервисов), гибкости в вопросах категорирования, риск-ориентированный подход, множественности регуляторов в разных сферах КИИ.

Субъектно-деятельностная модель определения предмета регулирования является более гибкой. Так, конкретный объект может принадлежать конкретному лицу, но не использоваться, следовательно, ущерб объекту не окажет существенного влияния.

В данной модели имеет значение хозяйственная деятельность субъекта в той или иной сфере и возможный ущерб такой значимой деятельности от компьютерного инцидента. Указанная модель предусматривает большую степень самостоятельности субъектов и, как правило, предполагает риск-ориентированный подход (когда субъект в каждом конкретном случае принимает решение о соразмерности предпринимаемых мер существующим киберугрозам).

Вместе с тем, указанная модель является менее структурированной и недостаточно прозрачной. Указанный вывод характерен в особенности для США[50].

[49] https://www.ibm.com/blogs/supply-chain/what-is-supply-chain-security/

[50] Сравнительный анализ подходов к регулированию КИИ, https://internetpolicy.kg/2020/03/04/sravnitelnyj-analiz-podhodov-k-regulirovaniju-kii/

За последние годы многие страны пришли к пониманию необходимости **сотрудничества между государственным и частным секторами**, а также между международными и региональными сообществами в целях обеспечения принятия эффективных стратегий управления рисками и обеспечения отказоустойчивости в сфере ИКТ, а также обязательство развивать необходимый национальный потенциал для повышения доверия и безопасности в сфере ИКТ, устранения недостатков и реагирования на значительные риски в области кибербезопасности[51].

Краткие выводы и рекомендации

В правовом поле, несмотря на обилие нормативных правовых актов в сфере информатизации, противоречий в вопросах обеспечения кибербезопасности не существует. В целом анализ действующего законодательства в сфере информационной и кибербезопасности, за исключением Стратегии кибербезопасности на 2019-2023 годы, которая была утверждена постановлением Правительства Кыргызской Республики от 23 июля 2019 года, позволяет делать выводы о том, что оно:

- не определяет правовые рамки, основополагающие принципы и единые подходы в вопросе обеспечения кибербезопасности Кыргызской Республики, позволяющие выстроить единую «систему координат» для государственной политики в области обеспечения кибербезопасности;
- представляет собой неполную и устаревшую нормативную базу, большинство законов были сформированы в принципиально иной технологической и социальной среде, и в силу этого не учитывают современных трендов в сфере кибербезопасности;
- не содержит терминов и определений, связанных с критической информационной инфраструктурой и т.п.;
- не обеспечивает эффективный контроль обеспечения прав субъектов правовых отношений в сфере кибербезопасности.
- Вместе с этим, на данный момент в Кыргызской Республике не создан ряд базовых условий, опорных точек, без которых невозможно обеспечить безопасность цифровой трансформации, в частности, и развитие национальной отрасли ИТ и связи в целом. В том числе:
- имеются существенные пробелы в системе нормативных правовых актов и политик обеспечения кибербезопасности (отсутствие концепций и подходов к реагированию на компьютерные инциденты, обеспечению безопасности критической инфраструктуры и автоматических систем управления технологическими процессами, международному сотрудничеству в области обеспечения кибербезопасности);
- в тех нишах и направлениях государственной политики, где система нормативных правовых актов и заданных ими подходов присутствует, наблюдается ее неполнота и отставание от актуальных тенденций развития ИКТ и кибербезопасности (противодействие компьютерной преступности, регулирование в области защиты информации, техническая стандартизация в области ИТ);
- не выстроен подход к повышению уровня компьютерной гигиены и цифровой грамотности, а также в целом к наращиванию потенциала и использованию человеческих ресурсов в рамках государственной политики по обеспечению кибербезопасности.

[51] Managing National Cyber Risks, Melissa Hathaway

- в действующем уголовном законодательстве отсутствуют составы совершаемых сегодня киберпреступлений, а в процессуальном законодательстве – методы поиска, фиксации и оценки цифровых доказательств.

Поскольку Кыргызская Республика еще не сталкивалась с большим количеством судебных дел о киберпреступлениях, ограниченный потенциал представителей правоохранительных и судебных органов в этой области может потенциально привести к неэффективным расследованиям, преследованиям и приговорам, что позволит киберпреступникам оставаться безнаказанными и продолжать свою преступную деятельность.

Проблема уголовно-правовой оценки киберпреступности вытекает из слабой законодательной основы, сложности сбора доказательств и самого процесса доказывания, недостатка компетентных лиц в области информационных технологий в органах государственной власти, отсутствия обобщенной судебной системы и иных факторов, влияющих на развитие противодействия киберпреступности.

Как следствие, в дополнение к укреплению законодательной базы, важно повышать потенциал системы уголовного правосудия в успешной борьбе и предупреждении киберпреступлений.

В условиях цифровой трансформации многих секторов общественных отношений, остается открытым вопрос разрешения гражданских споров. Гражданско-процессуальное законодательство не имеет основы для собирания электронных (цифровых) доказательств,

Также обилие нормативных правовых актов в области связи, цифровизации и телекоммуникаций ведет к неоднозначному толкованию многих терминов и определений, а разрозненность субъектов информационного рынка, ответственных за обеспечение информационной безопасности, мешает проведению четкой политики в этой сфере.

В связи с этим видится необходимым:

Законодательно определить правовые и организационные основы, цели, направления и принципы, а также подходы государственной политики в сфере обеспечения кибербезопасности Кыргызской Республики. Это возможно сделать через внедрение отдельной главы, касающейся вопросов кибербезопасности. При этом целесообразно здесь же обязательно раскрыть базовые понятия в области кибербезопасности.

Начать пересмотр законодательства в области противодействия киберпреступности и использования электронных доказательств, ориентируясь на положительные примеры и успешный мировой опыт проведения реформ. Разработать единую методологию в области идентификации, сбора, получения и хранения свидетельств, представленных в цифровой форме как для уголовного судопроизводства, так и для гражданского. При разработке такого документа в том числе целесообразно за основу взять международный стандарт ИСО/МЭК 27037:2012* «Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме" (ISO/IEC 27037:2012 «Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence»).

Данный стандарт был принят Международной организацией по стандартизации (ISO – International Organization for Standardization) в 2012 году и является руководством по конкретным процессам при обращении с потенциальными доказательствами, представленными в цифровой форме (далее – цифровые доказательства); этими процессами являются: идентификация, сбор, получение и сохранение потенциальных цифровых доказательств. Эти процессы необходимы при проведении расследования и предназначены для поддержки целостности цифровых доказательств, т.е. являются приемлемой методикой получения цифровых доказательств, которая будет способствовать их допустимости для правовых и дисциплинарных действий, а также для других необходимых случаев. Настоящий стандарт также предоставляет общее руководство по сбору цифровых доказательств, которые могут быть полезны на этапе анализа таких доказательств.

Настоящий стандарт предназначен для предоставления руководства лицам, отвечающим за идентификацию, сбор, получение и сохранение потенциальных свидетельств, представленных в цифровой форме. К таким лицам относятся специалисты «оперативного реагирования» по цифровым доказательствам, специалисты по реагированию на инциденты и руководители лабораторий судебной экспертизы. Настоящий стандарт обеспечивает уверенность в том, что ответственные лица осуществляют менеджмент потенциальных цифровых доказательств, рациональными общепризнанными способами, чтобы систематически и беспристрастно содействовать расследованию, использующему цифровые устройства и цифровых доказательств, сохраняя при этом их целостность и подлинность.

Другим основанием для использования данного стандарта является то, что некоторые страны ЕАЭС уже внедрили их в свои стандарты и широко используют в практической деятельности, что позволит использовать совместимые технические стандарты для цифровой криминалистической экспертизы и трансграничного поиска электронных доказательств.

Кроме этого другим базовым международным документом является Будапештская Конвенция о компьютерных преступлениях 2001 года, которая также может стать основой для формирования национальной уголовно-процессуальной базы по борьбе с кибепреступлениями и позволит гармонизировать национальное законодательство с международным.

Учитывая трансграничный характер киберпреступлений такой подход в формировании отечественного законодательства очень важен с точки зрения необходимости создания условий для эффективного сотрудничества с другими странами мира.

Будапештская конвенция стала открытой для подписания более 20 лет назад, с 23 ноября 2001 года. На сегодняшний день Конвенцию ратифицировали 66 стран, две подписали ее и 10 получили приглашения присоединиться. Более 140 стран работают с Советом Европы над укреплением своего законодательства и потенциала по борьбе с киберпреступностью.

Данная конвенция содержит ряд полномочий и процедур, таких как обыск компьютерных данных, сетей и перехват, определяет принципы международного сотрудничества при расследовании киберпреступлений, обмена технической информацией.

Обеспечить реализацию пункта 4.5 Национальной стратегии развития Кыргызской Республики на 2018-2040 годы, а также положений Концепции цифровой трансформации «Цифровой Кыргызстан 2019-2023», касающихся вопросов обеспечения кибербезопасности через разработку и принятие Закона о безопасности критической информационной инфраструктуры и ряда актов Правительства, обеспечивающих его реализацию. Как отмечалось выше, по результатам тщательного сравнительного анализа законодательства и практики стран Европейского союза, Великобритании, стран Азии, включая Китай, Японию, Сингапур, а также Российской Федерации, Казахстана и Грузии выделены две основные модели регулирования безопасности КИИ в зависимости от непосредственного предмета регулирования: «объектная» (РФ, Казахстан, Германия) и «субъектно-деятельностная» (ЕС, кроме Германии, Грузия, Сингапур, Китай, Япония).

Анализ показал, что на ранних этапах развития правового регулирования в сфере безопасности КИИ целесообразно использовать объектный подход. При этом необходимо иметь ввиду, что без установления четких критериев категорирования, оставляя определение категории объекта на усмотрение государственного органа или самого лица – владельца объекта КИИ, затруднительно обеспечить единообразие в сфере защищенности объектов КИИ от потенциальных угроз.

В виду детальной проработанности российского подхода к защите КИИ, опыт Российской Федерации в сфере регулирования КИИ может быть наиболее полезен при разработке подхода Кыргызской Республики, как в целом, в определении законодательной модели (ввиду близости правопорядков двух стран), так и по конкретным аспектам регулирования (например, в части категорирования объектов КИИ). Кроме того, российский подход предполагает также выделение категории значимых объектов КИИ. Отношение к определенной категории значимости означает большую вероятность негативных последствий в определенной сфере и повышенные требования к титульным владельцам таких объектов.

Конкретный список сфер, зависящий от значений тех или иных отраслей с экономической и социальной точек зрения для государства, подлежит определению в соответствии с последующим категорированием объектов критической информационной инфраструктуры.

В качестве возможной модели для терминологии в сфере КИИ может быть взят также российский подход с учётом особенностей существующего законодательства Кыргызстана в сфере информации и информационных технологий.

Таким образом, анализ моделей обеспечения безопасности критической информационной инфраструктуры показал, что российский подход и действующий в Российской Федерации механизм обеспечения безопасности критической информационной инфраструктуры по сравнению с другими системами, созданными в других странах, наиболее соответствует сложившемуся в Кыргызской Республике положению дел по регулированию в сфере использования информационной инфраструктуры.

Обеспечить дополнительную криминализацию деяний, связанных с киберпреступностью. При реализации данного подхода целесообразно учитывать правоприменительную практику других стран и использовать положения международных актов в области кибербезопасности. В целях гармонизации национального законодательства с международными подходами возможно принять во внимание положения Будапештской конвенции о киберпреступности от 2001 года.

Данная конвенция является самым первым международным договором о преступлениях, совершенных через Интернет и другие компьютерные сети, и касается, в частности, нарушений авторских прав, компьютерных мошенничеств, детской порнографии и нарушений безопасности сети.

Также следует обратить внимание на создание уголовно-правовой основы для привлечения к ответственности лиц, совершивших деяния, связанные с противозаконным доступом, перехватом данных с использованием технических средств, воздействия на информацию и функционирование системы, противозаконное использование устройств, мошенничество с использованием информационно-коммуникационных технологий и т.п.

Необходимо обеспечить реализацию требований Закона Кыргызской Республики «Об информации персонального характера», который подразумевает наличие ответственности за нарушение требований законодательства о персональных данных, в том числе ответственность за:

- обработку персональных данных без законного основания;
- необоснованный отказ в представлении субъекту персональных данных информации, касающейся обработки его персональных данных;
- невыполнение законных требований уполномоченного государственного органа по персональным данным;
- необоснованный отказ уполномоченному государственному органу по персональным данным или Омбудсмену (Акыйкатчы) Кыргызской Республики.

Кроме этого, важно обратить внимание на вопросы унификации терминов и понятий не только с Будапештской конвенцией, но и с глоссарием МСЭ, международными стандартами, Стратегией кибербезопасности и законодательством Кыргызской Республики в области связи и телекоммуникаций, в том числе в целях обеспечения принципа правовой определенности.

Разработать и принять акты, касающиеся процессуальных полномочий при проведении досудебного производства по киберпреступлениям и преступлений, с использованием электронных доказательств.

Следует учесть рекомендации изложенные в Докладе Группы экспертов Генеральной Ассамблеи ООН, который был подготовлен по итогам всестороннего исследования проблемы киберпреступности в 2020 году, касающиеся вопросов законодательного закрепления положений по международному сотрудничеству в области обеспечения кибербезопасности.

Учитывая слабый потенциал правоохранительных и судебных органов в области расследования и рассмотрения дел, связанных с цифровыми доказательствами необходимо на систематической основе проводить мероприятия по повышению их квалификации. При этом весьма важно постоянно осведомлять о международной практике и международных тенденциях в области кибербезопасности.

Рассмотреть возможность присоединения к региональным и международным инициативам, координации движений и программам развития потенциала в сфере борьбы с кибепреступлениями в целях укрепления международного сотрудничества в данной области.

Из-за отсутствия анализов риска по кибербезопасности возникает необходимость в государственной стандартизации информационной безопасности, в том числе в области межведомственного взаимодействия. Для поддержания интероперабельности информационных систем, стандарты должны быть открытыми и соответствовать следующим критериям:

- принятие и дальнейшее развитие стандарта должно осуществляться на основе процедуры открытого принятия решений, доступной для всех заинтересованных сторон;
- документы, описывающие стандарт должны находиться в свободном доступе;
- в патентные требования на использование стандарта не должна входить выплата роялти;
- стандарт должен быть технологически нейтральным;
- стандарт должен поддерживать локализацию, в тех случаях, когда это необходимо.

Рассмотреть возможность упрощения или разделения на отдельные положения Требований к защите информации, содержащейся в базах данных государственных информационных систем. При этом, внести коррективы с точки зрения существующих стандартов и актуальных тенденций развития ИКТ и кибербезопасности. В данном контексте возможно применить отдельные положения и принципы американского национального института стандартов и технологий (NIST), в том числе Минимальные требования безопасности для Федеральных информационных систем и информации. Этот стандарт определяет спецификацию минимальных требований безопасности для государственных информационных систем (организационных, эксплуатационных и технических мер).

Раздел 31. Экспериментальные правовые режимы (регуляторные песочницы)

Содержание

- законодательство об экспериментальных правовых режимах

Текущее регулирование (действующее законодательство):

1. Закон Кыргызской Республики «Об электронном управлении»
2. Закон Кыргызской Республики «Об инновационной деятельности»
3. Закон Кыргызской Республики «О Национальном банке Кыргызской Республики, банках и банковской деятельности»
4. Указ Президента Кыргызской Республики «О мерах по развитию креативной экономики и созданию условий для прогрессивного развития Кыргызской Республики» от 21 апреля 2022 года УП №123
5. Постановление Правления Национального Банка Кыргызской Республики «Об утверждении Положения «О специальном регулятивном режиме» от 12 августа 2020 года №2020-П-12\45-3-(НПА)

Краткое описание выявленных недостатков и ориентиров из мировой практики

№	Описание недостатка	Тип[52]	Лучшая практика
33.1	Закон о "регуляторных песочницах" отсутствует. Это запрещает возможность использования механизма "регулятивной песочницы" при апробировании новых правоотношений, поддержки инноваций в области ИКТ, нет механизмов партнерства, государственной поддержки технологических стартапов	**П**	На сегодняшний день насчитывается около 50 стран, где применяются регулятивные песочницы. В 13 из них законодательство о специальных правовых режимах зарекомендовало себя в качестве наиболее эффективного инструмента. Так, регуляторные песочницы были успешно внедрены в США, Австралии, Сингапуре, ОАЭ, Гонконге, Малайзии, Таиланде, Индонезии, Бахрейне, Швейцарии и Канаде. Первой страной, которая прибегла к таким механизмам, стала Великобритания, запустившая песочницу Financial Conduct Authority (FCA) еще в 2016 году. Во время пилотных испытаний регуляторы одобрили 50 из 146 поданных на обкатку в песочнице заявок; 75 процентов принятых компаний успешно прошли тестирование. Песочница хорошо функционирует, туда попадает много стартапов, которые уже на первом этапе становятся инвестиционно привлекательными. На сегодняшний

[52] В таблице приводятся следующие типы недостатков регулирования:
(П) пробел в регулировании (регулирование требуется, но его нет)
(У) устаревшая норма (норма есть, но её нужно менять)
(Н) неработающая норма (норма есть, но в силу описанных причин она не работает)
(Б) действующая норма является необоснованным препятствием для осуществления деятельности

			день FCA является одной из самых крупных в мире песочниц по объему собранных инвестиций. После Лондона песочницами заинтересовался Сингапур, где регулятором выступает денежно-кредитное управление. Критерии оценки стартапов здесь схожи с британской моделью, но единое время для проведения оценки компании не установлено. Оно зависит от направления проекта, поэтому подбирается индивидуально. Согласно данным из открытых источников, в сингапурской песочнице сейчас пилотируются четыре проекта. На постсоветском пространстве первым государством, которое создало аналог песочницы, стала Беларусь. В 2018 году там приняли декрет «О развитии цифровой экономики», в соответствии с ним был установлен специальный режим Парка высоких технологий. В его рамках чиновники узаконили майнинг и обращение криптовалют. Благодаря этому резиденты Парка могут беспрепятственно заниматься созданием криптобирж, торговлей криптовалютой и иных активов. В России в январе 2021 года вступил в силу Федеральный закон "Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации". Он позволяет создать в определенном регионе зону, в которой будет сделано исключение из общего правового регулирования. То есть на этой территории компании в течение трех лет смогут тестировать свои продукты без лицензии и без риска нарушить существующий закон. В случае если инновация окажется безопасной и эффективной, эксперимент могут масштабировать на всю страну. По состоянию на январь 2022 года экспериментальные правовые режимы одобрены в отношении 5 проектов: большегрузных беспилотных перевозок товаров в

			Томской области, экспериментов, связанных с беспилотными такси в отдельных городах, анализом эффективности препаратов на основе больших данных, дистанционной торговлей лекарствами, доставке грузов до 500 кг дронами. Отмечается, что подготовка инициативной заявки на создание «регуляторной песочницы» требует очень большой и серьезной подготовки. Также инвесторы не понимают, как им действовать, если три года работы «регуляторной песочницы» подойдут к концу, а поправки в основное законодательство, закрепляющие успешный «экспериментальный» правовой опыт, не будут приняты

Комментарии

Законодательство, действующее в Кыргызской Республике по состоянию на апрель 2022 года, не содержит специального закона или прямого указания в законах на допустимость применения в стране «цифровой песочницы», предполагающей учреждение экспериментального правового режима в современном понимании. Тем не менее, минимальный, но опыт, как попытка внедрения прообраза экспериментального правового режима, все же состоялся.

В апреле 2020 года в Закон КР «Об инновационной деятельности» от 26 ноября 1999 года №128 внесены изменения и дополнения, предусмотревшие, что особенности правоотношений и условий апробирования инновационных услуг/технологий в сфере предоставления банковских, платежных услуг в рамках специальных регулятивных режимов регулируются Законом КР "О Национальном банке Кыргызской Республики, банках и банковской деятельности" от 16 декабря 2016 года №206. В свою очередь и этот закон дополнен главой 11 «Специальные регулятивные режимы», предусматривающей, что Национальный банк вправе устанавливать на определенный срок на отдельной или на всей территории Кыргызской Республики пилотное регулирование в рамках специального регулятивного режима в целях апробирования правового регулирования общественных отношений в сфере предоставления банковских, платежных услуг, связанных с внедрением инновационных услуг/технологий. Под специальным регулятивным режимом понимается совокупность правил, которые позволяют участникам, занимающимся внедрением инновационных услуг/технологий на рынке банковских и платежных услуг, апробировать их в ограниченной контролируемой среде (по территории, во времени, по количеству и объему операций и пользователей и иное). Такая деятельность имеет целью ускорение ввода на рынок инновационных банковских операций и услуг, а осуществляется на основе лицензии. Согласно Положению «О специальном регулятивном режиме», утвержденному Постановлением Нацбанка КР от 12 августа 2020 года №2020-П-12\45-3-(НПА), такая лицензия дает право обладателю на ограниченный перечень операций и услуг, которые являются принципиально новыми, не применялись ранее или были ограничены, а также не регулируются нормативными правовыми актами и на них нет прямого запрета и регулятивных норм. Согласно реестру специальных регулятивных режимов, размещенному на сайте[53] Национального банка КР в настоящее время из 4 выданных - действующими являются 3 лицензии и 1 лицензия отозвана.

[53] www.nbkr.kg

В 2021 году одним из депутатов ЖК инициировался вопрос о финтехе[54]. Одним из главных обоснований закона послужил тот факт, что на сегодня ни один нормативно-правовой акт не предусматривает развитие финансового сектора страны. В справке-обосновании законопроекта указывалось, что «цели и задачи, поставленные перед Нацбанком, — стабильность, безопасность, надежность, но не развитие». Вместе с тем, по утверждению разработчиков надежности подобных компаний следует добиваться путем хранения активов в хранилище Национального банка Кыргызстана. Национальный банк вправе устанавливать на определенный срок на отдельной или на всей территории КР пилотное регулирование подобных компаний. Законопроект вызвал бурные споры и в итоге в октябре 2021 года был отклонен комитетом ЖК. Главным предметом жарких споров стал пункт документа, дающий разрешение финтех-компаниям открывать корреспондентские счета непосредственно в Национальном банке. Таким образом, Нацбанк из регулятора финансового рынка превратился бы в его участника. Против такого подхода отрицательно высказались тогдашний председатель Нацбанка и некоторые депутаты. В итоге законопроект был отклонен, но выступавшие члены комитета высказались позитивно о самих попытках учреждения экспериментальных правовых режимов при условии, что соответствующие законодательные инициативы будут самым серьезным образом обоснованы, а в предложениях будут приведены убедительные доводы о нивелировании рисков, которые сопровождают любые попытки введения в государстве особых или экспериментальных правовых режимов. Такие попытки при их недостаточной продуманности могут не только создавать возможности для злоупотреблений привилегированным положением отдельными участниками гражданско-правового оборота, но и нести ключевые риски причинения вреда населению при всей добросовестности решений и действий. Таким образом, последующие инициативы пока пребывают в стадии вызревания.

Наряду с этим, предпринимаются попытки ввести институт цифровых песочниц на уровне Евразийского союза. Так, решением Высшего Евразийского экономического совета от 11 октября 2017 года №12 «Об основных направлениях реализации цифровой повестки Евразийского экономического союза до 2025 года»[55] предусмотрено, что регулятивная песочница – специальный согласованный режим проработки и пилотирования решений, в том числе регуляторных, для определения эффективной модели взаимодействия и построения бизнес-процессов. В соответствии с Основными направлениями реализации цифровой повестки Евразийского экономического союза (далее –ЕАЭС) до 2025 года система «регулятивных песочниц» является одним из приоритетов проработки инициатив и их применение заявлено в качестве одного из механизмов успешной реализации цифровой повестки ЕАЭС. Экспертная площадка по созданию системы «регулятивных песочниц», в работе которой принимали участие представители бизнес-сообщества, эксперты и специалисты государственных органов стран-участниц ЕАЭС, научно-исследовательские организации и образовательные учреждения государств-членов Союза, а также эксперты функциональных блоков Комиссии, подготовила доклад о применении «регулятивных песочниц» в ЕАЭС и выдвинула проект распоряжения «О разработке концепции применения специальных режимов («регулятивных песочниц») в рамках реализации цифровой повестки Евразийского экономического союза». В нем описаны ключевые вызовы для реализации цифровой повестки (в том числе ограничения текущего процесса проработки инициатив и реализации проектов), цели, принципы и предлагаемый процесс применения специальных режимов, выгоды для заинтересованных сторон и интеграционные эффекты, приведен обзор альтернативных моделей с их преимуществами и недостатками, проанализированы кейсы возможного применения «регулятивных песочниц»[56]. В настоящее время Комиссия стремится выполнить поручение о разработке совместно с правительствами государств-членов ЕАЭС

[54] https://economist.kg/novosti/ekonomika/2021/09/23/skandalnyj-zakonoproekt-o-finteh-ili-pri-chem-tut-biznes-sestry-deputata/

[55] https://www.alta.ru/tamdoc/17vr0012/

[56] https://docs.cntd.ru/document/551782135

проекта концепции применения специальных режимов. Более подробная информация о текущем статусе вопроса открытые источники не содержат.

Таким образом, необходимость внедрения специальных правовых режимов в Кыргызской Республике в определенном смысле предопределена участием Кабинета Министров страны в выработке коллективных решений в этой сфере на уровне ЕАЭС.

Опыт других стран, уже применяющих экспериментальные правовые режимы в цифровой сфере, свидетельствует о продолжающемся распространении регулятивных песочниц, которые возможно свести к следующему общему определению:

Регулятивные песочницы, или экспериментальные правовые режимы, применяются в сфере инновационной деятельности в том случае, если общее регулирование соответствующей сферы отсутствует или порождает в осуществлении инновационных проектов препятствия, которые могут создать угрозу их реализации. Соответственно, регуляторная песочница прежде всего позволяет восполнить с учетом потребностей быстроразвивающейся цифровой экономики нормативно-правовое регулирование, которое зачастую отстает от инновационной сферы. Кроме того, регулятивная песочница позволяет на льготных правовых условиях предпринимателям протестировать новые технологии. Регулятивная песочница является прогрессивным и опережающим регулированием и достаточно широко применяется в мировой практике. Данный инструмент активно реализуется, в частности, в Великобритании, США, Сингапуре и Канаде. В 2021 году в Российской Федерации вступил в силу Федеральный Закон «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» от 31 июля 2020 г. N 258-ФЗ с открытым, по существу, перечнем сфер и областей деятельности, где может быть применена цифровая песочница. Согласно обобщающим публикациям регулятивная «песочница» (англ. Regulatory Sandbox) — специальный правовой режим регулирования, проработки и пилотирования решений, в том числе регуляторных, для определения наиболее эффективной модели взаимодействия и построения бизнес-процессов в какой-либо новой сфере.

Регулятивные «песочницы» целесообразно использовать для проработки механизмов и правил регулирования экономических процессов в рамках цифровых инициатив и проектов. Условно регулятивные «песочницы» в мировой практике можно разделить на 2 вида: «финтех-песочницы» и универсальные «песочницы». Первые работают с цифровыми инновациями в финансовой сфере - новые механизмы страхования, кредитования, финансового консультирования, краудфандинга, «цифровыми» и «мобильными» банками, микрофинансовой деятельностью. Вторые в свою очередь нацелены на более широкий спектр цифровых инноваций, применяемых в реальном секторе экономики – технологии больших данных, нейротехнологии и искусственный интеллект, системы распределенного реестра, квантовые технологии, новые производственные технологии, промышленный интернет, компоненты робототехники и сенсорика, технологии беспроводной связи, технологии виртуальной и дополненной реальностей. На данный момент самым распространенным видом являются «финтех-песочницы». Это объясняется как особенностями предмета регулирования (финансовая сфера традиционно является самой «зарегулированной» сферой экономики), так и динамикой развития финансовых технологий при значительной маржинальности финтех-технологий.

Условия внедрения экспериментальных правовых режимов бесспорно имеют свои особенности для стран с развитой правовой системой, устоявшейся правовой культурой, традиционно партнерскими отношениями между контролирующими органами и бизнесом по сравнению с развивающимися странами, которые объективно значительно отстают в развитости государственных институтов, призванных обеспечивать справедливую политику регулирования и ограничений, а также слабое участие институтов гражданского общества в обеспечении общественного контроля за процессами реформирования.

В одной из работ[57] содержатся обобщенные выводы о том, что проблемы регуляторного потенциала в развивающихся странах имеют свои особенности.

[57] https://deliverypdf.ssrn.com/delivery

При работе над проектами нормативных правовых актов о цифровой песочнице в Кыргызстане, по-видимому, следует обратить внимание на следующие особенности и риски, которые будут сопровождать как процессы разработки, рассмотрения и принятия соответствующих проектов, так и последующую их реализацию на практике.

1. Регуляторные песочницы могут потребовать времени и уровня квалификации регуляторов, необходимые для определения планов тестирования и показателей производительности, оценки сложных инноваций и претендентов-новаторов в ходе проведения индивидуальных оценок.

2. Необходимо также определить ресурсы для контроля участников в своей песочнице. Это потребует дополнительного персонала и временных обязательств, которые регулирующие органы, особенно в странах с такими ограниченными ресурсами, как в Кыргызстане, могут не обладать и могут быть иным образом заняты (или отвлекаться) от других основных обязанностей в качестве регулирующего органа. В некоторых странах в регулирующих органах учреждается штатный персонал, посвященный работе с песочницей. Формирование специальной кросс-функциональной команды для песочниц особенно сложно в развивающихся странах, у которых много меньше финансовых и людских ресурсов.

3. Песочницы призваны способствовать более открытому общению между регулирующими органами и новаторами, что может производить взаимовыгодный опыт обучения. Но у регулирующих органов может просто не быть ресурсов и необходимого опыта, чтобы понять и оценить сложную природу инновации (особенно с учетом более низкого уровня сложности рынка Кыргызстана) и оставаться в курсе его быстрых темпов и внести изменения. В идеале действия регулирующих органов должны учитывать цели регулирования с учетом и соблюдением правовых границ. Регулирующие органы, не обладающие достаточным потенциалом для полного понимания и оценки того, что может быть новым, сложным, прорывным нововведением, могут сопротивляться одобрению, уклоняться от выбора защиты от риска неудачи и личного воздействия путем сохранения статус-кво. Другая крайность: слишком усердная программа поощрения инноваций может привести к чрезмерному дерегулированию с неоправданными рисками, вводимыми в систему тестирования, и приводящими к возможным сбоям. На окончательный успех «песочницы» могут повлиять самые разные непредусмотренные обстоятельства, которые при этом могут подорвать существующие условия и ограничения, нанести ущерб правовой системе.

4. Хотя песочницы вызвали и вызывают значительный интерес и энтузиазм, они являются лишь одним из нескольких подходов к регулированию и не всегда являются оптимальным решением. Возможно потребуется реформа нормативно-правовой базы для устранения негибкости и несовместимости регулирования, которые могут помешать эффективности и успеху «песочницы».

5. Меньшие по размеру и менее развитые рынки, то есть рынки развивающихся стран, часто создают фундаментальные проблемы. К ним могут относиться ограниченные местные ресурсы (такие как доступность капитала и человеческих ресурсов), удаленность от ресурсов и недостаточные кадровые резервы, ограниченная инфраструктура и неоптимальные рыночные условия.

6. Хозяйственная деятельность местных песочниц также ограничена внутренними границами и достижение достаточной экономии за счет масштаба для долгосрочной жизнеспособности может быть сложной задачей. Такие риски снижают привлекательность инноваций и возможности для прямых местных и иностранных инвестиций. Кроме того, структура и регулирование, которые ограничивают транзакции физическими границами, могут задушить создание трансграничной деятельности и безграничный характер финансовых технологий, который способен обеспечить необходимую и выгодную экономию за счет масштаба.

7. Есть проблемы и с ограниченной прозрачностью. Поскольку подробности соглашений об участии в «песочнице», как правило, не обнародуются и часто подпадают под действие соглашений о конфиденциальности, следует проявлять осторожность, чтобы не вызвать негативного общественного мнения, в Кыргызстане, где существует высокий уровень

коррупции, ¬ особенно. Участники, допущенные в песочницу, могут получить преимущества от особого статуса по сравнению с другими за счет смягчения правил и общения с регулирующим органом. Определенные кандидаты могут быть приняты в «песочницу» при неправомерном лоббировании. Вероятность такого лоббирования в КР чрезвычайно высока.

8. Необходимо стремление к снижению рисков: участники «песочницы» несут ответственность за управление своими делами, такими как обеспечение достаточного финансирования, финансовых счетов в банках и финансовых учреждениях и получение доступа к данным. Эти задачи могут оказаться сложными для новаторов, включая тех, кто обслуживает или работает в Кыргызстане.

Таким образом, необходимо учитывать уже, пусть небольшую, но наработанную, практику в банковской сфере Кыргызской Республики по специальным регулятивным режимам и вовлеченность Кыргызстана в разработку решений по подготовке предложений по регулятивным песочницам на площадках ЕАЭС. Следует принять во внимание и Указ Президента КР «О мерах по развитию креативной экономики и созданию условий для прогрессивного развития Кыргызской Республики» от 21 апреля 2022 года №УП 123, в соответствии с которым Кабинетом министров утверждена Концепция развития креативной экономики в Кыргызской Республике на 2022–2026 годы (Постановление Кабинета Министров КР от 25 апреля 2022 года, поскольку ее целью является создание благоприятных условий для развития креативной экономики, увеличение вклада креативных индустрий в отечественную экономику посредством формирования комплексной государственной политики. Согласно Концепции, сектор креативных индустрий в стране призван стать акселератором предпринимательской деятельности с высокой добавочной стоимостью и высоким экономическим эффектом, а это рационализирует капиталовложения, расширит экспортные возможности и обеспечит прирост занятости. Следует предполагать, что усилия в этом направлении неизбежно вынесут на повестку дня закон об экспериментальных правовых режимах. Креативная экономика по указу действующего главы государства и исполнительной власти в будущем должна стать толчком для стимулирования инноваций, увеличения инвестиционной привлекательности и снизить «зависимость национальной экономики от сектора горнодобывающей промышленности и денежных переводов мигрантов».

Однако при подготовке конкретных проектов нормативных правовых актов следует с крайней осторожностью и предусмотрительностью рассчитать риски, принимая во внимание специфичность нормативно-правовый системы и социально-экономических реалий Кыргызской Республики.

Раздел 33. Налоговое регулирование

Содержание

- эффективная налоговая политика в рамках перехода Кыргызской Республики к цифровой экономике;
- модернизация инструментального и методологического аппарата налоговой политики;
- синхронизация правового инструментария, используемого в налоговом законодательстве.

Текущее регулирование (действующее законодательство):

1. Налоговый кодекс Кыргызской Республики;
2. Закон Кыргызской Республики «Об электронной торговле»;
3. Закон Кыргызской Республики «Об электронном управлении»;
4. Закон Кыргызской Республики «Об электронной подписи»;
5. Закон КР «Об инновационной деятельности»;
6. Закон КР «О виртуальных активах»;
7. Закон КР «Об электронной торговле».

Краткое описание выявленных недостатков и ориентиров из мировой практики

№	Описание недостатка	Тип[58]	Лучшая практика
33.1	Не определены базовые принципы, конкретные задачи и насущные приоритеты налоговой политики в рамках перехода к цифровой экономике, не определены базовые понятия, такие как «совместная экономика», «цифровая платформа» и т.п.	**П**	В мире отсутствует единое кодифицированное законодательство, регулирующее правоотношения в сети Интернет, и существуют совершенно объективные проблемы налогообложения субъектов цифровой экономики (совместной экономики), которые до сих пор не решены. Правила налогообложения не успевают за развитием современных цифровых бизнес-моделей. Иностранные ИТ-гиганты, зарабатывая на пользователях по всему миру, платят налог на прибыль только по месту регистрации своей штаб-квартиры. В результате страны не только теряют налоговые доходы, но и нарушаются принципы справедливой конкуренции - национальные цифровые компании платят больше налогов и, соответственно, работают в менее выгодных условиях, чем зарубежные. ОЭСР с 2015 года пытается найти единый международный подход и

[58] В таблице приводятся следующие типы недостатков регулирования:
(П) пробел в регулировании (регулирование требуется, но его нет)
(У) устаревшая норма (норма есть, но её нужно менять)
(Н) неработающая норма (норма есть, но в силу описанных причин она не работает)
(Б) действующая норма является необоснованным препятствием для осуществления деятельности

			решить проблему несправедливого распределения налогов ИТ-гигантов. Разработать механизм, который устроил бы все страны, пока не удалось. Главная сложность в том, как рассчитать, какая доля прибыли мультинациональной корпорации приходится на ту или иную страну. Сколько прибыли генерируют пользователи в той или иной стране, знают только сами корпорации, но они не раскрывают детальную информацию
33.2	В рамках «цифрового налога» отсутствуют критерии (не только доменное имя и IP-адрес) для образования постоянного учреждения иностранной интернет-компании в целях установления обязанности налоговой регистрации и налогообложения доходов в Кыргызской Республике	**П**	В Заключительном докладе BEPS от 5 октября 2015 года ОЭСР обсудила три меры, которые могут улучшить налогообложение в рамках электронной торговли: - учет связи, основанной на концепции значительного экономического присутствия в пределах юрисдикции, указывающей на место уплаты налога; - налог на цифровые транзакции; - equalization levy / уравнительный сбор, предполагающий налогообложение оборота (а не прибыли) компаний цифровой экономики. Ряд государств, включая Великобританию, Францию, Италию, Турцию, не дожидаясь глобального консенсуса ОЭСР, в одностороннем порядке ввели собственные цифровые налоги и установили собственную практику налогообложения, позволяющую взимать НДС или налог на товары и услуги, поставляемые непосредственно потребителям на их территории в отношении интернет-рекламы и услуг цифрового посредничества. Реализуя собственную заинтересованность во взимании налогов, европейские страны перешли от принципа происхождения к принципу назначения и привели условия взимания налогов в соответствие с

			этим принципом. Далее установили порог для суммы продаж, при котором продавец облагается налогом в стране назначения. Франция стала первой европейской страной, объявившей в 2019 году о введении цифрового налога, который в том числе распространяется на облачные услуги. Платежи по ставке 3% платят цифровые компании с суммарным доходом по всему миру от €750 млн, более €25 млн. из которых принесли французские пользователи. Налог применяется к доходу, который технологические гиганты получают в стране.
33.3	Недостаточно четко определены термины, относящиеся к объектам налогообложения в цифровой экономике, такие как «майнинг» или «виртуальный актив», что приведет к сложностям в применении норм о цифровом налоге на практике	**Н**	Данная проблема требует решения в рамках составления глоссария, поскольку перечисленные термины имеют значение не только для целей налогообложения
33.4	Различные подходы к порядку применения налога на добавленную стоимость в отношении международных услуг электросвязи, продиктованные МСЭ и Договором ЕАЭС, позволяют сделать вывод о наличии правовой коллизии между подходами к взиманию НДС за международные услуги связи, который должен быть разрешен в соответствии с нормами международного права и найти отражение в законодательстве Кыргызской Республики для придания этому ясности	**Б**	Регламентом международной электросвязи в статье «Тарификация и расчеты» (пункт 6.3.1.) установлено правило «Если в соответствии с национальным законодательством какой-либо страны предусматривается налог на взимание таксы за международные службы электросвязи, то этим налогом облагаются, как правило, только те международные услуги, которые оплачиваются клиентами этой страны, если отсутствуют другие соглашения, заключаемые для конкретных специальных случаев». Сложившаяся общемировая практика интерпретирует названное правило как невозможность применения в Кыргызской Республике налога на добавленную стоимость в отношении международных услуг электросвязи, таких как услуги роуминга, межсетевого соединения (интерконнекта) и услуг по обеспечению международного транзитного трафика, при взаиморасчетах между операторами связи, в виду того, что такие услуги оплачиваются клиентами иностранного оператора связи,

			заказывающего оказание подобного рода услуг. Комиссия РСС по экономике связи регионального содружества в области связи Решением №23/10 от 19-20 марта 2009 года рекомендовало администрациям связи и операторам электросвязи стран участников РСС руководствоваться разъяснением Исполкома РСС к международным правилам об освобождении администраций (операторов) связи от уплаты налога на добавленную стоимость при взаиморасчетах с администрациями (операторами) связи других стран за предоставляемые международных услуги связи. В разъяснении приводится ссылка на Регламент международной электросвязи. Указывается, что в странах СНГ налог на добавленную стоимость оплачивается клиентурой при пользовании международными услугами связи, но не может оплачиваться операторами связи других стран при проведении с ними взаиморасчетов. Дается предложение операторам связи стран участников РСС производить взаиморасчеты друг с другом и с операторами связи стран дальнего зарубежья за предоставляемые международные услуги связи без начисления налога на добавленную стоимость. Однако, как показала практика, положения Регламента международного союза электросвязи для налогообложения налогом на добавленную стоимость и исполнение на законодательном уровне рекомендаций Комиссии РСС, не нашли отражения в налоговом законодательстве Кыргызской Республики в качестве специальных норм. Услуги оператора связи, оказываемые иностранному оператору связи, признаются подлежащими налогообложению налогом на добавленную стоимость по месту оказания таких услуг (месту реализации услуг).

			Протокол 18 к Договору ЕАЭС местом реализации услуг связи и соответственно местом уплаты НДС, определил территорию государства члена, если услуги оказываются налогоплательщиком этого государства члена. Административный регламент Международного союза электросвязи, предусматривает взимание налога на добавленную стоимость в той стране, в которой услуги оплачиваются потребителем (абонентом), иными словами, по месту оплаты услуг

Комментарии

Трансформация экономики характеризуется повсеместными процессами внедрения в работу субъектов хозяйственной деятельности информационных и производственных технологий: использование облачных хранилищ, переход к цифровым деньгам, реализация биометрических систем аутентификации, применение функций искусственного интеллекта. Налоговая система является неотъемлемой частью этой картины, стимулируя внедрение цифровых технологий в процессы взаимодействия налоговых органов и налогоплательщиков. Информатизация технологических и производственных процессов становится наиболее эффективным средством для удовлетворения потребностей как граждан, так и органов государственной власти. Ускоренное развитие и глобальные процессы цифровизации порождают новые возможности для государственного бюджета, которые пока находятся в Кыргызской Республике на стадии осмысления и становления.

На государственном уровне до сих не определены принципы налогообложения в сфере интернет-экономики и электронной коммерции. В связи с чем вопросы реформирования и гармонизации налогового законодательства через повсеместное внедрение новых инструментов налогообложения, включая разработку архитектуры налогообложения цифрового бизнеса являются острой потребностью и подлежат скорейшему разрешению с учетом уже сложившейся мировой практики и рекомендаций ОЭСР.

Несмотря на введение с 1 января 2022 года новых инструментов налогообложения, перед государством по-прежнему стоят две основные задачи усовершенствования практики налогового администрирования:

- модернизация инструментального и методологического аппарата существующей налоговой политики, и
- внедрение цифровых технологий и цифровых платформ в экономику.

Необходимыми мерами по реализации указанных задач являются:

- создание системы цифровой идентификации, в том числе на международном уровне;
- применение инструментов взаимодействия с налогоплательщиками, встроенные в естественную среду и общегосударственные сервисы;
- совершенствование стандартов управления данными, обеспечение доступности информации, необходимой для администрирования;
- внедрение и развитие автоматизированных алгоритмов расчета налоговых обязательств, с реализации функции уведомления налогоплательщика на предварительной основе;

- применение искусственного интеллекта и предиктивной аналитики (predictive analytics) для налогового администрирования, развитие новых компетенций у сотрудников налоговых органов;
- выстраивание удобного механизма международного взаимодействия между налоговыми администрациями.

С 1 января 2022 года в налоговом законодательстве введено применение электронной налоговой отчетности и отчетности по социальному страхованию, маркировки товаров для их прослеживаемости, установлены специальные налоговые режимы: «налог на майнинг», «налог на деятельность в сфере электронной торговли» и «налоговый режим в Парке высоких технологий», закреплены специальные термины – «Услуга в электронной форме», «Майнинг», «Виртуальный актив», расширены понятия «Постоянное представительство» и «Место оказания услуг», определены условия налоговой регистрации иностранных юридических лиц.

Следует отметить, в мире отсутствует единое кодифицированное законодательство, регулирующее правоотношения в сети Интернет и существуют совершенно объективные проблемы налогообложения субъектов цифровой экономики (совместной экономики), которые до сих пор не решены. Правила налогообложения не успевают за развитием современных цифровых бизнес-моделей. Иностранные ИТ-гиганты, зарабатывая на пользователях по всему миру, платят налог на прибыль только по месту регистрации своей штаб-квартиры. В результате страны не только теряют налоговые доходы, но и нарушаются принципы справедливой конкуренции - национальные цифровые компании платят больше налогов и, соответственно, работают в менее выгодных условиях, чем зарубежные. ОЭСР с 2015 года пытается найти единый международный подход и решить проблему несправедливого распределения налогов ИТ-гигантов. Разработать механизм, который устроил бы все страны, пока не удалось. Главная сложность в том, как рассчитать, какая доля прибыли мультинациональной корпорации приходится на ту или иную страну. Сколько прибыли генерируют пользователи в той или иной стране, знают только сами корпорации, но они не раскрывают детальную информацию.

Маркетплейсы – самая популярная бизнес-модель в e-commerce. Не являясь собственником товара, он предоставляет владельцам товаров – производителям, дистрибьюторам, продавцам – технологию и инфраструктуру для онлайн-торговли (далее «цифровая платформа»). На сегодняшний день крупнейшими маркетплейсами в мире являются Alibaba, JD.com, Amazon, Pinduoduo.

Эффективное налогообложение продавцов, использующих в своей экономической деятельности цифровые платформы, т. е. лиц, продающих товары или услуги посредством использования ресурса цифровых платформ, является общей проблемой для многих налоговых администраций в свете их продолжающегося быстрого роста. Два ключевых принципа платформенного бизнеса – сервисный формат продукта и гибкий формат оплаты обеспечивают позитивный и продуктивный опыт для многих потребителей, но оказались практически недосягаемы для налогового администрирования. Бурный рост e-commerce торговли в Кыргызстане проходил до 1 января 2022 года без какого-либо серьезного государственного регулирования, в частности, «цифрового налога», который был с успехом введен в 130 странах мира, присоединившихся к глобальному пакту ОЭСР по цифровому налогу.

В Заключительном докладе BEPS от 5 октября 2015 года ОЭСР обсудила три меры, которые могут улучшить налогообложение в рамках электронной торговли:

- учет связи, основанной на концепции значительного экономического присутствия в пределах юрисдикции, указывающей на место уплаты налога;
- налог на цифровые транзакции;
- equalization levy / уравнительный сбор, предполагающий налогообложение оборота (а не прибыли) компаний цифровой экономики.

Ряд государств, включая Великобританию, Францию, Италию, Турцию, не дожидаясь глобального консенсуса ОЭСР, в одностороннем порядке ввели собственные цифровые налоги и установили собственную практику налогообложения, позволяющую взимать НДС или налог на товары и услуги, поставляемые непосредственно потребителям на их территории в отношении интернет-рекламы и услуг цифрового посредничества.

Реализуя собственную заинтересованность во взимании налогов, европейские страны перешли от принципа происхождения к принципу назначения и привели условия взимания налогов в соответствие с этим принципом. Далее установили порог для суммы продаж, при котором продавец облагается налогом в стране назначения.

Франция стала первой европейской страной, объявившей в 2019 году о введении цифрового налога, который в том числе распространяется на облачные услуги. Платежи по ставке 3% платят цифровые компании с суммарным доходом по всему миру от €750 млн, более €25 млн. из которых принесли французские пользователи. Налог применяется к доходу, который технологические гиганты получают в стране. Цифровой налог затронул около 30 глобальных корпораций, в том числе Google, Amazon и Facebook. Объектом налогообложения является «предоставление цифрового интерфейса, который позволяет пользователям вступать в контакт и взаимодействовать между собой, предполагая поставку товаров или оказание услуг прямо между такими пользователями» и «размещение в цифровом интерфейсе целевых рекламных сообщений с учетом данных пользователей, получаемых при использовании ими этого цифрового интерфейса». Местом реализации признается Франция, если устройства пользователей, задействованные в цифровых услугах, находятся на территории Франции. При этом налоговая база – это доход от реализации цифровых услуг (без учета НДС). Сумма дохода определяется как доля всего дохода компании от соответствующей услуги, пропорциональная объему поставок пользователям во Франции, или количеству аккаунтов во Франции, или количеству показов рекламы во Франции, или количеству французских пользователей, чьи данные были обработаны, в общем объеме этих операций.

Турция с 1 марта 2020 года начала взимать цифровой налог по ставке 7,5%.

Великобритания стала взимать цифровой налог на выручку технологических гигантов по ставке 2% с апреля 2020 года.

Италия ввела 3% налог с января 2020 года в отношении поставщиков цифровых услуг (в том числе облачных), которые получают более $831 млн выручки во всем мире и не менее $6 млн в Италии.

Испания ввела налог в размере 3% в отношении иностранных ИТ-компаний с мировыми доходами более 750 млн евро в год и более 3 млн евро в Испании.

В 2019 года правительство Чехии одобрило введение цифрового налога в размере 7%. Его должны будут платить крупные международные компании с оборотом от 750 млн евро в мире и 100 млн крон (3,91 млн евро) в Чехии, а также с пользовательской аудиторией более 200 тыс. человек. Среди них — Facebook и Google. Новым налогом облагаются доходы от продаж таргетированной рекламы на цифровых площадках, а также пользовательских данных. Инициатива действует применительно к услугам, предоставляемым чешским пользователям.

С аналогичной инициативой в 2020 году выступила Бразилия, где в Палату представителей был представлен закон о создании цифрового налога к юридическим лицам, зарегистрированным в Бразилии или за рубежом, а также членам международных групп, чей доход за предыдущий год превышает 3 млрд бразильских реалов ($600 млн). Кроме того, налогоплательщики должны иметь валовой доход в Бразилии, превышающий 100 млн бразильских реалов ($20 млн). Ставка налога дифференцирована с размера валового дохода от 1% до 5%.

Процедура установления цифрового налога была реализованы в некоторых странах Азии и Латинской Америки, а также в постсоветских странах, которые возложили обязанность по взиманию НДС (Налог на товары и услуги) со всех покупок (за весь платный контент, приобретенный пользователями), совершенных пользователями в Google Play Маркете на местных и/или иностранных разработчиков, установив применимые ставки налога. Такая

практика касается Австралии, Бахрейна, Белоруссии, Индии, Чили, Японии, Саудовской Аравии, России, Южной Кореи, Новой Зеландии, Сингапура, Индонезии, Казахстана и пр.

Индия с 2016 года установила сбор по ставке 6% в отношении доходов иностранных компаний от B2B-сделок в области цифровой рекламы.

В 2020 году Таиланд утвердил законопроект, обязывающий иностранных поставщиков облачных и других цифровых услуг платить НДС по ставке 7% с продаж. Закон требует от компаний-нерезидентов или цифровых платформ, которые зарабатывают от оказания цифровых услуг более 1,8 млн батов ($82 831) в год, уплаты НДС.

В мае 2020 года Индонезия приняла закон, обязывающий крупные интернет-компании уплачивать НДС с продаж цифровых продуктов и услуг, а на Филиппинах законодатель внес аналогичный законопроект в парламент о налогообложении цифровых услуг.

С 1 января 2020 года Google начнет взимать 6%-ый налог за свои облачные и другие цифровые услуги в Малайзии. Сумма налога на обслуживание будет взиматься с покупки и отображаться в отдельной строке в транзакциях в разделе «Счета и платежи».

С апреля 2020 года Google начал выплачивать налог на интернет-услуги в Узбекистане. В налоговый кодекс страны были введены поправки, предусматривающие «налог на Google» в отношении компаний, предоставляющих цифровые услуги. Налог обязывает иностранные компании, оказывающие платные услуги интернет-пользователям Узбекистана, платить НДС в размере 15%. Для регистрации в Узбекистане иностранных интернет-компаний налоговый комитет создал специальный онлайн ресурс — НДС-офис, по адресу tax.uz. Согласно нововведениям, иностранные юридические лица, осуществляющие реализацию услуг и товаров в электронной форме, местом реализации которых является Узбекистан, признаются налогоплательщиками таких услуг, оказываемых физическим лицам.

Казахстан с 1 января 2022 года официально ввел в Налоговый кодекс 25 раздел, который называется «Особенности налогообложения иностранных компаний при осуществлении электронной торговли товарами, оказании услуг в электронной форме физическим лицам». С 1 января 2022 года у иностранных интернет-компаний, действующих в Казахстане без образования юридического лица, появится налоговое обязательство по уплате НДС по ставке 12%, при осуществлении ими электронной торговли товарами или оказании услуг в электронной форме физическим лицам – покупателям. Ожидается, что потенциальными плательщиками цифрового налога станут такие крупные технологические компании, как Facebook, Amazon, Apple, Netflix, Alibaba и Google, для которых предусмотрен ряд облегченных процедур прохождения налоговой регистрации в форме условной регистрации в качестве плательщика НДС. Достаточно направить в налоговый орган Казахстана письмо-подтверждение по почте на бумажном носителе. Уплата налога осуществляется без выписки электронных счетов-фактур. Сдача налоговой отчетности также не предусмотрена. Открытие расчетных счетов в банках Республики Казахстан не обязательна, так как оплату налога иностранная компания производит со своих расчетных банковских счетов за границей.

Все страны, принявшие законы о цифровых налогах, предусмотрели специальные методики для определения части валового дохода, подлежащего налогообложению в их стране, а также специальные процедуры налоговой регистрации. В зависимости от основного налогового режима и характера платежей, удержание может варьироваться от простой системы с универсальной установленной ставкой, до более сложной системы, которая учитывает более широкие обстоятельства.

Основными проблемами, с которыми столкнулись страны, принявшие налог на интернет на законодательном уровне, признаются:

a. отсутствие соответствующей (общеприменимой) терминологии в законодательстве;

b. неспособность всеобъемлюще реализовывать контроль прибыли, получаемой в сфере электронной торговли (особенно осуществляемой через анонимные платежные системы), в связи с чем уклонение от цифрового налога представляются безграничными;

c. преобладание нематериальных активов над материальными и их транснациональная мобильность создают дополнительные барьеры;

d. не урегулированы вопросы пересмотра национальных налоговых доктрин и соглашений об избежании двойного налогообложения для установления баланса между источником и налогом по месту регистрации компании;

e. недостаток информации об объемах цифровых активов и услуг, предоставляемых иностранными ИТ-компаниями.

Реализуя свои потребности в эффективном налогообложении электронной коммерции, Кыргызская Республика предложила с 01 января 2022 года собственную модель применения цифрового налога, которая должна была учесть существующий положительный опыт, а также позволить разрешить указанные выше проблемные вопросы. Однако принятое решение оказалось не свободно от недостатков, в частности:

- в рамках «цифрового налога» отсутствуют критерии (не только доменное имя и IP-адрес) для образования постоянного учреждения иностранной интернет-компании в целях установления обязанности налоговой регистрации и налогообложения доходов в Кыргызской Республике;
- недостаточно четко определены термины, относящиеся к объектам налогообложения в цифровой экономике, такие как «майнинг» или «виртуальный актив», что приведет к сложностям в применении норм о цифровом налоге на практике.

Данные проблемы выходят за рамки собственно налогового законодательства и требуют решения в процессе определения границ суверенитета Кыргызской Республики в киберпространстве и составления глоссария, поскольку перечисленные термины имеют значение не только для целей налогообложения.

Кроме того, существуют налоговые коллизии в сфере обложения международных услуг электросвязи. Различные подходы к порядку применения налога на добавленную стоимость в отношении международных услуг электросвязи, продиктованные МСЭ и Договором ЕАЭС, позволяют сделать вывод о наличии правовой коллизии между подходами к взиманию НДС за международные услуги связи, который должен быть разрешен в соответствии с нормами международного права и найти отражение в законодательстве Кыргызской Республики для придания этому ясности.

Регламентом международной электросвязи в статье «Тарификация и расчеты» (пункт 6.3.1.) установлено правило «Если в соответствии с национальным законодательством какой-либо страны предусматривается налог на взимание таксы за международные службы электросвязи, то этим налогом облагаются, как правило, только те международные услуги, которые оплачиваются клиентами этой страны, если отсутствуют другие соглашения, заключаемые для конкретных специальных случаев». Сложившаяся общемировая практика интерпретирует названное правило, как невозможность применения в Кыргызской Республике налога на добавленную стоимость в отношении международных услуг электросвязи, таких как услуги роуминга, межсетевого соединения (интерконнекта) и услуг по обеспечению международного транзитного трафика, при взаиморасчетах между операторами связи, в виду того, что такие услуги оплачиваются клиентами иностранного оператора связи, заказывающего оказание подобного рода услуг. Комиссия РСС по экономике связи регионального содружества в области связи Решением №23/10 от 19-20 марта 2009 года рекомендовало администрациям связи и операторам электросвязи стран участников РСС руководствоваться разъяснением Исполкома РСС к международным правилам об освобождении администраций (операторов) связи от уплаты налога на добавленную стоимость при взаиморасчетах с администрациями (операторами) связи других стран за предоставляемые международных услуги связи.

В разъяснении приводится ссылка на Регламент международной электросвязи. Указывается, что в странах СНГ налог на добавленную стоимость оплачивается клиентурой при пользовании международными услугами связи, но не может оплачиваться операторами связи других стран при проведении с ними взаиморасчетов. Дается предложение операторам

связи стран участников РСС производить взаиморасчеты друг с другом и с операторами связи стран дальнего зарубежья за предоставляемые международные услуги связи без начисления налога на добавленную стоимость.

Однако, как показала практика, положения Регламента международного союза электросвязи для налогообложения налогом на добавленную стоимость и исполнение на законодательном уровне рекомендаций Комиссии РСС, не нашли отражения в налоговом законодательстве Кыргызской Республики в качестве специальных норм. Услуги оператора связи, оказываемые иностранному оператору связи, признаются подлежащими налогообложению налогом на добавленную стоимость по месту оказания таких услуг (месту реализации услуг).

Протокол 18 к Договору ЕАЭС местом реализации услуг связи и соответственно местом уплаты НДС, определил территорию государства члена, если услуги оказываются налогоплательщиком этого государства члена. Административный регламент Международного союза электросвязи, предусматривает взимание налога на добавленную стоимость в той стране, в которой услуги оплачиваются потребителем (абонентом), иными словами, по месту оплаты услуг.

Раздел 34. Таможенное регулирование

Содержание

- вопросы таможенной очистки и контроля с использованием цифровых средств, таможенный контроль интеллектуальной собственности

Текущее регулирование (действующее законодательство):

1. Договор о таможенном кодексе евразийского экономического союза от 11 апреля 2017 года.
2. Таможенный кодекс евразийского экономического союза (приложение № 1 к договору о таможенном кодексе евразийского экономического союза от 11 апреля 2017 года).
3. Закон КР от 24 апреля 2019 года n 52 "о таможенном регулировании"
4. Налоговый кодекс КР от 18 января 2022 года № 3.
5. Закон КР от 2 июля 1997 года № 41 «О государственном регулировании внешнеторговой деятельности в Кыргызской Республике».
6. Закон КР от 23 января 2003 года № 30 «Об экспортном контроле».
7. Закон КР «О товарных знаках, знаках обслуживания и наименованиях мест происхождения товаров» от 14 января 1998 года № 7.
8. Закон КР от 30 декабря 2014 года № 173 «О таможенном тарифе Кыргызской Республики».
9. Постановление Правительства КР от 13 февраля 2020 года № 79 «О некоторых вопросах в сфере таможенного дела».
10. Постановление Правительства КР от 27 ноября 2000 года № 694 «Об утверждении положения о порядке таможенного контроля в отношении товаров, содержащих объекты интеллектуальной собственности".
11. Постановление Правительства КР от 4 мая 2004 года № 330 «О мерах по внедрению в Кыргызской Республике национальной системы экспортного контроля».
12. Постановление Правительства КР от 2 апреля 2014 года № 197 «Об утверждении национального контрольного списка Кыргызской Республики контролируемой продукции".
13. Постановление Правительства КР от 6 августа 2015 года № 563 «О мерах по реализации требований закона Кыргызской Республики "О таможенном регулировании в кыргызской республике".
14. Постановление Правительства КР от 10 августа 2015 года № 564 «О мерах по реализации требований статей 95, 101, 102, 105, 128, 135, 148, 153, 157, 158, 163, 176, 180, 213, 229, 232 закона кыргызской республики "О таможенном регулировании в Кыргызской Республике".
15. Постановление Правительства КР от 23 июня 2016 года № 353 «О реорганизации государственного предприятия "таможенная инфраструктура" при государственной таможенной службе при Правительстве Кыргызской Республики".

Краткое описание выявленных недостатков и ориентиров из мировой практики

№	Описание недостатка	Тип[59]	Лучшая практика
34.1	Неполноценное использование потенциала института электронного предварительного информирования.	**П**	Всемирная таможенная организация (ВТамО) считает показателем высокого уровня развития

[59] В таблице приводятся следующие типы недостатков регулирования:
(П) пробел в регулировании (регулирование требуется, но его нет)
(У) устаревшая норма (норма есть, но её нужно менять)
(Н) неработающая норма (норма есть, но в силу описанных причин она не работает)
(Б) действующая норма является необоснованным препятствием для осуществления деятельности

			таможенной службы использование ею предварительной информации. Международная конвенция по упрощению и гармонизации таможенных процедур (Киотская конвенция) предусматривает необходимость при разработке таможенных процедур использовать предварительную информацию и обеспечивать передачу ее в электронном виде. Наряду с другими механизмами и инструментами предварительное информирование и предварительное декларирование является основой для внедрения Рамочных стандартов безопасности и облегчения торговли, внедрения управления интегрированной цепочкой поставок в рамках проводимой работы ВТамО (Integrated Supply Chain Management Guidelines (WCO, June 2004). Предварительное информирование активно развивается в условиях опасности роста международного терроризма. В частности, Правительствами ряда стран были приняты правила и заключены соглашения с деловыми кругами для обеспечения необходимого уровня безопасности на базе результатов оценки рисков, проводимой до прибытия товаров на таможенную территорию: программа таможенной службы Канады "Партнеры по защите" (PIP), программа таможенной службы Австралии "Передняя линия и аккредитованный клиент", программа таможенной службы США "C-TPAT", программа таможенной службы Новой Зеландии "SEP and FrontLine" Глава 6 «Таможенный контроль» Руководства к Генеральному Приложению Международная конвенция по упрощению и гармонизации таможенных процедур (Киотская конвенция): Таможенные администрации должны разработать таможенные процедуры по внедрению методов таможенного контроля для обеспечения единого

			применения на всей таможенной территории. При разработке данных процедур таможенная администрация должна переключить внимание от исполнительного применения таможенного контроля за передвижением на таможенный контроль, основанный на аудите, учитывая следующие моменты: • сокращение времени задержки во время передвижения товаров/лиц, • увеличение использования периодической подачи таможенных деклараций, • стимулирование проведение участником торговли самооценки, • предоставление возможности участникам торговли (не таможенным органом) задерживать предоставление сопроводительных официальных и коммерческих документов • увеличение использования представления предварительной информации и его электронная передача, • увеличение использования коммерческой системы участников торговли и учета вместо необходимости хранения таможенных документов • стимулирование соблюдения таможенного законодательства, разделяя с торговыми кругами все больше ответственности при партнерстве таможенного органа по снижению уровня риска. В целях оптимизации применения современных методов таможенного контроля рекомендуется использование средств автоматизации. Таможенная администрация должна использовать на местах соответствующий анализ и рассмотреть механизмы для обеспечения эффективности таможенных контрольных процедур, применяемые по всех таможенной территории. Процедуры можно пересматривать и корректировать, при необходимости, для того чтобы

			они соответствовали определенным требованиям.
34.2	Многоконтрольность и дублирование при проведении государственных видов контроля на границе	**П**	"Таможенный контроль" определен в Справочнике таможенных терминов Всемирной таможенной организации как "меры, применяемые для обеспечения соблюдения законов и положений, исполнение которого возложено на таможенные органы.". Для обеспечения надлежащего применения таможенных законов и положений, необходимо, чтобы все международные передвижения были продекларированы для переработки или использования, которые разрешаются таможенным органом. С целью выполнения обязательств по сбору государственного дохода, осуществлению торговой политики и защите населения, одновременно для регулирования увеличением объема международной торговли и туризма, которые проявляются вместе с сокращением таможенного штата, а также для содействия торговле с помощью укрепления соблюдения закона участниками торговли, путешественниками и перевозчиками, таможенная администрация должна применять методы таможенного контроля эффективно и производительно путем внедрения методов управления риском. Постоянный пересмотр данных методов контроля для обеспечения их постоянного обновления поможет таможенной администрации выполнять данные сложные задачи, несмотря на сильное влияние интенсивного развития международной торговли и непрерывные изменения в системе торговли и транспорта. Социальные проблемы вызывают по крайней мере равнозначные по важности изменения требований по таможенному контролю. Содействие законной торговли в процессе управления риском играет очень важную роль. Меморандум взаимопонимания с отдельными компаниями (как рекомендовано в программе Всемирной таможенной

			организации ACTION /DEFIS) может придать официальный статус такому сотрудничеству как таможня-торговля. Существует много способов реагирования на такие изменения путем поднятия на более высокий уровень содействия и таможенного контроля в рамках современной таможенной практики. Один из способов объединения мер содействия и таможенного контроля является использование единой компетентной структуры для выполнения широкого круга задач, таких как фитосанитария, ветеренария или контроль опасных грузов, осуществляемых в настоящее время различными агентствами, возможно, расположенными в разных местах. Таможенные органы, уже существующие на всех границах, и имеющие большой опыт работы по оперативному выполнению требований международной торговли и транспорта, уделяют логически обоснованное и экономически обусловленное внимание выполнению таких обязанностей. Одним из решений рационального и оптимального построения процесса пересечения границы является применение принципа «Единого Окна» Наиболее распространенное определение «Единого Окна» приводится в Рекомендации ЕЭК ООН № 33. Согласно данному определению ЕО – «механизм, позволяющий сторонам, участвующим в международных торговых и транспортных операциях, подавать всю стандартизованную документацию с использованием единого пропускного канала в целях выполнения всех регулирующих требований, касающихся импорта, экспорта и транзита». «Если информация предоставляется в электронной форме, то индивидуальные элементы данных следует предоставлять лишь один раз».

			Единое окно» создается для обмена информацией между участниками торговой деятельности и государственными органами, а также между самими государственными органами по процедурам, связанным с внешней торговлей, таким как получение соответствующих разрешений, лицензий, сертификатов и согласований, прохождение таможенной очистки и выпуск из порта. Система «Единого окна» позволяет участникам торговой деятельности подавать внешнеторговую информацию один раз в одном месте и обеспечивает более эффективную и быструю обработку информации, если она подается в электронном виде.
34.3	Упрощение и оптимизация контроля доставки товаров	**П, У**	**В Азербайджанской Республике**, при импорте товаров от внешней границы до внутренних таможенных органов, применяют только таможенные операции по первичной регистрации товаров и транспортных средств на пунктах пропуска, без таможенного декларирования и помещения под таможенную процедуру транзита. При этом, доставка грузов до внутренних таможенных органов осуществляется с применением GPS-замков и навигационных пломб. В результате чего в Азербайджанской Республике из-за отсутствия необходимости формировать документы, среднее время прохождения через пункты пропуска занимает 15-20 минут. Стоит отметить, что информационная система (Единая автоматизированная управляющая система) Государственного таможенного комитета Республики Азербайджан по оценкам мирового сообщества считается одной из самых успешных моделей таможенного администрирования. Всемирная таможенная организация (ВТамО) рекомендует систему как платформу «лучшей практики».

34.4	Внедрение национальной системы уполномоченных экономических операторов	**Б**	Согласно определению, данному в Рамочных стандартах безопасности ВТамО, Уполномоченный экономический оператор (УЭО) — это любое юридическое лицо, вовлеченное в международное движение товаров и признанное национальным таможенным органом или от его имени как соответствующее стандартам безопасности ВТамО или аналогичной системы поставок. Под категорию УЭО в частности подпадают производители, импортеры, экспортеры, брокеры, перевозчики, консолидаторы, торговые посредники, операторы портов, аэропортов и терминалов, интегрированные операторы, склады и дистрибьюторы. Вот уже много лет, а в некоторых случаях еще с 70-х годов прошлого столетия, таможенные органы уделяют самое пристальное внимание обеспечению безопасности в рамках международной системы поставок, при этом не так давно с этой целью был разработан целый ряд специальных программ, направленных на укрепление безопасности торговли в общемировом контексте. Концепция УЭО является частью этих программ, в связи с чем в 2005 г. ВТамО разработала отдельный стандарт для УЭО — Рамочные стандарты безопасности ВТамО. С тех пор участникам торговли в определенных случаях приходится прилагать немалые усилия, чтобы обрести статус УЭО, но даже став УЭО торговая организация должна постоянно его поддерживать. При этом зачастую таможенные органы не предоставляют носителям статуса УЭО каких-либо значительных льгот в плане упрощения процедур торговли, что, естественно, повышает торговые издержки. Поэтому внедрение программ УЭО в глобальном масштабе идет довольно медленно.

			В рамках программы УЭО таможенные органы должны предоставлять ряд льгот организациям, получившим данный статус, при этом вся работа должна вестись в тесном взаимодействии с представителями сферы торговли. Стандарт 6 Раздела II Рамочных стандартов безопасности ВТамО поощряет сотрудничество между таможенными органами и участниками торговли с целью обеспечения максимального уровня безопасности и упрощенности. Однако данный стандарт отдает приоритет безопасности, а не упрощенности, что и создает определенную дилемму. В связи с этим ВТамО были разработаны специальные Методические указания по УЭО (изложены в Главе 5 Рамочных стандартов безопасности ВТамО), а также План льгот для УЭО, составленный усилиями частного сектора. Данные льготы предполагают сокращение количества инспекций и приоритет при проведении инспекций, взаимное признание иностранных программ УЭО, более мягкие требования в области безопасности и гарантий ускоренный выпуск товаров, а также предварительное оформление, упрощенные процедуры, приоритетное обслуживание в случае чрезвычайных ситуаций и т.д.
34.5	О необходимости разработать технологии совершения операций в упрощенном, ускоренном режиме для отдельных категорий товаров	**П**	Рекомендуется разработать и утвердить в Кыргызской Республике технологии совершения таможенных операций в отношении отдельных категорий товаров, требующих особых условий транспортировки, например, в отношении скоропортящейся продукции, которые позволили бы обеспечить стандартизировано упрощенный порядок их проезда границы и таможенной очистки. В частности, в ст. 7.9 Соглашения по упрощению процедур торговли Всемирной торговой организации говоится, что при оформлении и

			проверке, члены ВТО должны обеспечить приоритет для скоропортящихся товаров и разрешить транспортировку и хранение скоропортящихся товаров в утвержденных складах (государственных или частных), а также предоставить возможность оформления в этих же складах.
34.6	Принятие предварительного решения по вопросам применения методов определения таможенной стоимости ввозимых товаров	**П**	Генеральное соглашение по тарифам и торговле 1994 года (ГАТТ 1994) – это многостороннее межгосударственное соглашение, занимающее центральное место в правовом регулировании международной торговли товарами. Национальные торгово-политические системы стран-участниц ГАТТ, а теперь ВТО способствовало формированию единообразного правового поля в мировой торговле. Статья VII «Оценка товара для таможенных целей» настоящего Соглашения, определяет общие принципы оценки и обязывает применять эти принципы в отношении всех товаров, подпадающих под обложение пошлинами или другими сборами, или под ограничения ввоза и вывоза, основанные на стоимости или регулируемые в какой-либо форме в зависимости от стоимости. При этом, Статья 22 Соглашения по применению статьи VII Генерального соглашения по тарифам и торговле 1994 года гласит о том, что каждый член обеспечивает, не позднее даты начала применения для него положений настоящего Соглашения, соответствие его законов, нормативных актов и административных процедур положениям настоящего Соглашения.

Комментарии

В соответствии с положениями статьи 11 Таможенного кодекса Евразийского экономического союза у участника внешнеэкономической деятельности имеется обязательство предоставления до фактического прибытия на таможенную границу ЕАЭС предварительной информации о товарах, предполагаемых к перемещению через таможенную

границу ЕАЭС, транспортных средствах международной перевозки, перевозящих такие товары, времени и месте прибытия товаров на таможенную территорию Союза, пассажирах, прибывающих на таможенную территорию Союза.

При этом, при непредставлении предварительной информации, которая должна представляться в обязательном порядке, или нарушении сроков ее представления принимаются меры, устанавливаемые в соответствии с законодательством о таможенном регулировании государства-члена, таможенному органу которого подлежит представлению такая предварительная информация.

Законодательством государств-членов может устанавливаться ответственность за непредставление таможенным органам предварительной информации или за нарушение сроков ее представления.

Однако, законодательством Кыргызской Республики не предусмотрено применение ответственности при не предоставлении предварительной информации или нарушении сроков ее предоставления.

Таким образом, потенциал института предварительного информирования не используется в должной мере, т.к. даже если право ЕАЭС обязывает участников внешнеэкономической деятельности предоставлять предварительную информацию, однако, **в национальном законодательстве Кыргызской Республики не имеется мер ответственности как при неподаче предварительной информации в целом, так и при подаче ее вне пределов установленных сроков.**

Согласно постановлению Правительства Кыргызской Республики "О мерах по упорядочению функционирования пунктов пропуска через государственную границу Кыргызской Республики, предназначенных для международного автомобильного, воздушного и железнодорожного сообщения, и внутренних стационарных постов на автомобильных дорогах Кыргызской Республики" от 19 ноября 2007 года № 556, на пунктах пропуска через государственную границу Кыргызской Республики осуществляются следующие виды государственного контроля:

- пограничный;
- радиационный контроль;
- санитарно-карантинный контроль;
- ветеринарный контроль (надзор);
- карантинный фитосанитарный контроль (надзор);
- транспортный (автомобильный) контроль;
- таможенный контроль.

В свою очередь, последовательность действий при осуществлении пограничного, таможенного и иного контроля в автомобильных пунктах пропуска через таможенную границу ЕАЭС в Кыргызской Республике определяется Порядком взаимодействия уполномоченных государственных органов Кыргызской Республики в автомобильных пунктах пропуска через таможенную границу Евразийского экономического союза в Кыргызской Республике (далее – Порядок), утвержденного постановлением Правительства Кыргызской Республики от 19 ноября 2020 года.

В частности, главы 3, 4, 5, 6 Порядка описывает последовательность осуществления государственными органами контрольных действий при прибытии/убытии различных категорий товаров и транспортных средств.

При этом, каждый вид государственного контроля предусматриваем совершение одинаковых контрольных действий, которые часто дублируются.

В этой связи предлагается пересмотреть данный Порядок, в целях исключения проведения дублирующих форм и методов контроля путем внедрения единой межведомственной информационной системы.

В настоящее время при перемещении товаров с точек прибытия на таможенную территорию ЕАЭС в КР независимо от пункта доставки таможенные органы КР для

осуществления контроля доставки товаров применяют таможенную процедуру таможенного транзита.

Более того, таможенная процедура транзита применяется и при доставке товаров по таможенным контролем от внутреннего таможенного органа как до другого внутреннего таможенного органа, так и до пункта убытия с таможенной территории ЕАЭС в КР.

При этом, следует отметить, что согласно ТК ЕАЭС, для помещения товаров под таможенную процедуру таможенного транзита, необходимо соответствовать условиям помещения товаров под данную процедуру.

Так, согласно п.1 ст. 142 ТК ЕАЭС, таможенная процедура таможенного транзита - таможенная процедура, в соответствии с которой товары перевозятся (транспортируются) от таможенного органа отправления до таможенного органа назначения без уплаты таможенных пошлин, налогов, специальных, антидемпинговых, компенсационных пошлин при соблюдении условий помещения товаров под эту таможенную процедуру.

Условия помещения товаров под таможенную процедуру таможенного транзита в свою очередь описаны в ст. 143 ТК ЕАЭС:

«1) обеспечение исполнения обязанности по уплате ввозных таможенных пошлин, налогов в соответствии со статьей 146 настоящего Кодекса - в отношении иностранных товаров;

2) обеспечение исполнения обязанности по уплате специальных, антидемпинговых, компенсационных пошлин в соответствии со статьей 146 настоящего Кодекса в случаях, определяемых Комиссией, - в отношении иностранных товаров;

3) обеспечение возможности идентификации товаров способами, предусмотренными статьей 341 настоящего Кодекса;

4) соответствие транспортного средства международной перевозки требованиям, указанным в статье 364 настоящего Кодекса, если товары перевозятся в грузовых помещениях (отсеках) транспортного средства, на которые налагаются таможенные пломбы и печати;

5) соблюдение запретов и ограничений в соответствии со статьей 7 настоящего Кодекса».

Кроме этого, имеется ряд особенностей при помещении отдельных категорий товаров, например, таких товары для личного пользования, международные почтовые отправления, товары, перемещаемые трубопроводным транспортом и тд., под таможенную процедуру транзита.

Вместе с тем, в соответствии с п. 10 ст. 142 ТК ЕАЭС, особенности применения таможенной процедуры таможенного транзита в отношении товаров, перевозимых по территории только одного государства-члена, могут быть установлены законодательством этого государства-члена о таможенном регулировании.

Следует отметить, что в национальном законодательстве особенности применения таможенной процедуры таможенного транзита регулируются Инструкцией об особенностях совершения таможенных операций при помещении товаров под таможенную процедуру таможенного транзита, утверждённой постановлением Правительства КР О мерах по реализации требований статей 95, 101, 102, 105, 128, 135, 148, 153, 157, 158, 163, 176, 180, 213, 229, 232 Закона Кыргызской Республики "О таможенном регулировании в Кыргызской Республике", от 10 августа 2015 года № 564 (далее – Инструкция).

Данная инструкция была принята в реализацию Закона Кыргызской Республики «О таможенном регулировании в Кыргызской Республике» от 31 декабря 2014 года № 184, который утратил силу с принятием актуального на сегодняшний день Закона Кыргызской Республики «О таможенном регулировании» от 24 апреля 2019 года № 52.

Вместе с тем, Инструкция не устанавливает особенностей применения таможенного транзита, а только определяет порядок совершения таможенными органами таможенных операций, связанных с подачей, регистрацией транзитной декларации и завершением таможенной процедуры таможенного транзита в Кыргызской Республике.

При этом, в таможенном законодательстве Кыргызской Республики не использован потенциал возможности применения особенностей процедуры таможенного транзита в целях упрощения и оптимизации таможенных процессов.

В частности, при перевозке на небольшие расстояния товаров, находящихся по таможенным контролем, таможенные органы вынуждены применять таможенную процедуру транзита, при этом требуя обязательного соблюдения всех условий и положений, установленных ТК ЕАЭС, независимо от того, избыточны ли они или нет.

В этой связи рекомендуется разработать упрощенный механизм контроля доставки товаров под таможенным контролем в пределах Кыргызской Республики, в том числе разработать новую инструкцию, связанную с регулированием особенностей применения таможенной процедуры таможенного транзита в Кыргызской Республике.

С принятием Таможенного кодекса ЕАЭС и принятием в январе 2018 года пересмотренного закона «О таможенном регулировании» началась реализация программы уполномоченный экономический оператор (УЭО) в Кыргызской Республике. В связи с этим она все еще находится на начальном этапе разработки и следует организовать информационную кампанию для повышения уровня общей осведомленности о возможностях и преимуществах среди торгового сообщества.

Одним из критериев получения статуса УЭО согласно положениям Кодекса ЕАЭС является размещение гарантии на сумму не менее 1 миллиона, 700 000 и 500 000 евро в зависимости от трех различных типов сертификатов. Для многих местных компаний эта сумма является слишком высоким порогом. Имеется потребность в изучении других вариантов, регулируемых собственным национальным законодательством, чтобы обеспечить меры по упрощению процедур торговли для местных компаний, установив более разумные и подходящие критерии.

В то время как в настоящее время существует всего одна компания со статусом УЭО, по мере понимания ими преимуществ этого статуса и увеличения их количества, следует обеспечить создание системы валидации/проверки, мониторинга соответствия и других критериев обязательств. Также необходим официальный орган, принимающий решения в части предоставления, аннулирования и восстановления статуса УЭО, а также для обеспечения надлежащего предоставления УЭО преимуществ по упрощению процедур. **ГТС рекомендуется изучить возможность создания более инклюзивной структуры вне программы ЕАЭС по УЭО с более реальными и достижимыми критериями для местных компаний с высоким уровнем соответствия.**

Ст. 81 Таможенного кодекса ЕАЭС предусматривает специальный первоочередной порядок совершения таможенных операций в отношении товаров, необходимых для ликвидации последствий стихийных бедствий, чрезвычайных ситуаций природного и техногенного характера, продукции военного назначения, необходимой для выполнения акций по поддержанию мира либо для проведения учений, товаров, подвергающихся быстрой порче, а также в отношении животных, радиоактивных материалов, взрывчатых веществ, международных почтовых отправлений, экспресс-грузов, товаров, предназначенных для показа на международных выставочных мероприятиях, гуманитарной и технической помощи, сообщений и материалов для средств массовой информации, необходимых для ремонта и (или) поддержания безопасной эксплуатации транспортных средств международной перевозки запасных частей, двигателей, расходных материалов, оборудования, инструментов, валюты государств-членов, иностранной валюты, иных валютных ценностей, драгоценных металлов, в том числе золота, ввозимых национальными (центральными) банками государств-членов и их филиалами, и других подобных товаров.

При этом, согласно ст.78 ТК ЕАЭС «таможенные операции и порядок их совершения определяются настоящим Кодексом, иными международными договорами и актами в сфере таможенного регулирования, а в части, не определенной настоящим Кодексом, иными международными договорами и актами в сфере таможенного регулирования, либо в случаях,

предусмотренных международными договорами и актами в сфере таможенного регулирования, - в соответствии с законодательством государств-членов о таможенном регулировании.

Технологии совершения таможенных операций устанавливаются в соответствии с законодательством государств-членов о таможенном регулировании».

Таким образом, ТК ЕАЭС предоставляет возможность определять таможенные операции и порядок их совершения, неурегулированные ТК ЕАЭС и международными договорами, и в целом технологии совершения этих операций законодательством государств-членов ЕАЭС.

Однако, несмотря на это, **в нормативных правовых актах, регулирующих вопросы не имеется норм, устанавливающих первоочередной порядок совершения отдельных категорий товаров, в частности перечисленных в ст. 81 ТК ЕАЭС.**

В соответствии с положениями статьи 38 Таможенного кодекса Евразийского экономического союза Предварительные решения по вопросам применения методов определения таможенной стоимости ввозимых товаров могут приниматься в случае, если это установлено законодательством государств-членов о таможенном регулировании. Порядок и условия выдачи уполномоченным органом государства-члена предварительного решения по вопросам применения методов определения таможенной стоимости ввозимых товаров, а также порядок и сроки применения такого предварительного решения устанавливаются законодательством государства-члена о таможенном регулировании.

Однако, **законодательством Кыргызской Республики не предусмотрен порядок принятия Предварительного решения по применению методов определения таможенной стоимости товаров, ввозимых в Кыргызскую Республику, до таможенного декларирования ввозимых товаров.**

Реализация механизма выдачи Предварительного решения не только ускорит выпуск товара, но и окажет содействие исключению недостоверного декларирования, что, в свою очередь, позволит участникам внешнеэкономической деятельности качественнее прогнозировать и планировать свою внешнеэкономическую деятельность.