

**СИСТЕМНЫЙ ПРОЕКТ
ФОРМИРОВАНИЯ В РОССИЙСКОЙ ФЕДЕРАЦИИ
ИНФРАСТРУКТУРЫ ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА**

**Министерство связи и массовых коммуникаций
Российской Федерации**

2010 г.

Оглавление

1. Введение	4
2. Федеральный, региональный и муниципальный уровни применения Системного проекта	7
3. Переход на предоставление государственных услуг и исполнение государственных функций в электронном виде.....	10
Типология полномочий федеральных органов исполнительной власти	10
Специфика реализации управленческих полномочий (мониторинг, аналитика, статистика).....	13
Специфика реализации в электронном виде разрешительных полномочий.....	15
Перевод разрешительных полномочий в электронный вид	15
Типология взаимодействий между органами власти и заявителями	17
Ограничения для перевода разрешительных полномочий в электронный вид	23
Специфика реализации в электронном виде контрольно-надзорных полномочий.....	24
Ограничения для перевода контрольно-надзорных полномочий в электронный вид	24
Планирование перевода контрольно-надзорных полномочий в электронный вид	26
Специфика реализации полномочий по принятию нормативных правовых актов	27
Выводы и предложения, связанные с реализацией полномочий федеральных органов исполнительной власти в электронном виде	29
4. Перевод в электронный вид государственной учетной деятельности.....	30
Проблемы, связанные с ведением государственной учетной деятельности	30
Направления деятельности по упорядочиванию государственного учета	31
Единые принципы ведения государственной учетной деятельности	31
Легализация ведения государственной (муниципальной) учетной деятельности в электронном виде	33
Требования к государственным и муниципальным электронным учетным системам	33
Приоритеты	33
5. Информационно-технологические и инженерные компоненты электронного правительства	33
Вводные положения	33
Прикладные государственные информационные системы	34
Информационно-технологическая инфраструктура электронного правительства	34
Инженерная инфраструктура	36
Требования к прикладным государственным информационным системам.....	37
Требования к инфраструктурным информационным системам электронного правительства	37
Типовые решения	38
6. Решение первоочередных проблем и формирование ключевых инфраструктур электронного правительства	41
Инфраструктура обеспечения юридической значимости электронного взаимодействия	48
Юридическая значимость электронного документа	48
Целевое состояние инфраструктуры обеспечения юридической значимости электронного взаимодействия	49
Инфраструктура цифрового доверия	49
Идентификация при электронном взаимодействии	55
Служба доверенного времени	56
Электронный нотариат.....	56
Обеспечение совместимости информационных систем электронного правительства	57
Семантическая совместимость информационных систем электронного правительства	57
Технологическая совместимость информационных систем электронного правительства	58
Формирование инженерной инфраструктуры	61
Информационная безопасность.....	62
7. Обеспечение доступности государственных услуг и инфраструктуры электронного правительства	68
Принципы обеспечения доступности государственных услуг: целевое состояние	69
Принципы качественного правового регулирования	69
Принципы качественного информирования	71
Принципы технологической нейтральности	71
Направления деятельности по обеспечению доступности услуг электронного правительства.....	73
Увеличение доступности товаров и услуг в сфере ИКТ	74
8. Обеспечение эффективности бюджетных расходов на формирование электронного правительства	75

Текущее состояние	75
Целевое состояние системы управления расходами на внедрение ИКТ	76
Меры повышения эффективности бюджетных расходов на внедрение ИКТ	77
Целевые индикаторы мероприятий по повышению эффективности бюджетных расходов	78
Бюджетирование расходов на перевод в электронный вид процессов реализации государственных полномочий	79
9. Управление формированием электронного правительства	80
Планирование и координация деятельности по формированию электронного правительства	80
Нормативное закрепление полномочий, функций и ответственности, связанных с формированием электронного правительства	80
Текущее состояние системы управления формированием электронного правительства	81
Целевое состояние структуры управления	81
Частно-государственное партнерство	81
Управление проектами по формированию электронного правительства	82
Независимая экспертиза проектов в сфере ИКТ	82
Обеспечение методической поддержки, создание центров компетенций для государственных служащих	82
Кадровое обеспечение формирования электронного правительства	82
Разработка и внедрение механизмов повышения мотивации государственных служащих и других участников проектов	82
Оценка эффективности деятельности по формированию электронного правительства	85
Оценка качества государственного управления	85
Индексы развития информационного общества	85
Оценка качества и доступности государственных услуг	85
Оценки выполнения утвержденных планов формирования электронного правительства	85
Целевые показатели формирования электронного правительства	86
10. Заключительные положения	89

1. Введение

В настоящем документе представлены основные положения по формированию в Российской Федерации инфраструктуры электронного правительства (далее – Системный проект).

Настоящий Системный проект предназначен для создания на его основе государственной Программы «Информационное общество», уточнения содержания иных программ, находящихся на данный момент в стадии выполнения или разработки.

В мировой практике для обозначения целевого состояния деятельности органов власти, опирающейся на возможности информационно-коммуникационных технологий (далее — ИКТ), используется понятие «электронное государство» (e-government), относящееся к государству и государственному управлению в целом, а не только к органам исполнительной власти.

Под «электронным государством» далее понимается деятельность всех государственных органов, органов местного самоуправления и подведомственных им организаций на основе применения ИКТ с охватом всех трех ветвей государственной власти Российской Федерации — исполнительной, законодательной и судебной. В свою очередь, выражение «информационное общество», как оно понимается в текущей практике, характеризует всю совокупность общественных отношений. Для целей документа под электронным правительством понимается способ организации деятельности федеральных и региональных органов исполнительной власти, органов местного самоуправления, при котором:

- во всех случаях, когда отсутствует доказанная необходимость административного усмотрения, личного присутствия заявителя, а также бумажного документооборота, применяются формальные процедуры сбора сведений, подготовки и принятия решений, основанные на удаленном электронном взаимодействии;
- обеспечивается повышение качества государственного управления, понимаемого как степень соответствия деятельности государственных органов исполнительной власти легитимным интересам граждан Российской Федерации.

Данные определения являются конкретизацией положений Концепции формирования электронного правительства в Российской Федерации до 2010 г., одобренной распоряжением Правительства Российской Федерации от 6 мая 2008 г. № 632-р, в части разделения терминов «электронное правительство» и «электронное государство».

Главной целью формирования электронного правительства является повышение качества государственного управления, которое выражается через:

- снижение временных, организационных и финансовых издержек для граждан и организаций при получении государственных (муниципальных) услуг;
- снижение административных барьеров и бремени избыточного регулирования для хозяйствующих субъектов;
- сокращение бюджетных расходов на деятельность органов исполнительной власти и повышение эффективности этих расходов;
- повышение прозрачности деятельности органов государственной власти.

Перечисленные характеристики качества государственного управления могут быть объективно измерены, в том числе с помощью индикаторов, поддерживаемых независимыми от органов государственной власти организациями.

Для построения информационного общества необходимы максимально широкие преобразования, затрагивающие все ветви и уровни государственной власти и местного самоуправления, сферы общественных отношений (здравоохранение, образование, культура и т.д.), бизнес и граждан. Формирование электронного государства подразумевает решение меньшего круга задач, связанных лишь с исполнительной, законодательной и

судебной ветвями власти. Электронное правительство затрагивает деятельность исполнительной власти на всех уровнях управления (Рисунок 1.1).

Большая часть концепций и нормативных правовых актов, принятых в 2002–2008 гг., была направлена на создание отдельных государственных информационных систем, типовых программных продуктов и обоснование выделения бюджетного финансирования на закупки ИКТ.

В актах Правительства Российской Федерации, принятых в 2008–2010 гг., немалое внимание уделено вопросам государственного управления и административной эффективности (в противовес экстенсивной информатизации), что позволило инициировать формирование отдельных компонентов электронного правительства (таких как создание реестра и портала государственных услуг, системы межведомственного электронного взаимодействия и ряда иных).

Достижение целевых показателей, определенных в действующих правовых актах, принятых в 2009–2010 гг., является чрезвычайно амбициозной задачей, особенно с учетом незначительности результатов, полученных в ходе информатизации и реализации мероприятий административной реформы в предшествующий период. Планы перехода федеральных органов исполнительной власти и органов государственной власти субъектов Российской Федерации и органов местного самоуправления на предоставление государственных услуг и исполнение государственных функций в электронном виде, утвержденные распоряжением правительства Российской Федерации от 17 октября 2009 г. № 1555-р и распоряжением правительства Российской Федерации от 17 декабря 2009 года № 1993-р, не могут быть выполнены без системных мер, описанных в настоящем документе.



Рисунок 1.1. Место и роль электронного правительства в решении задачи формирования информационного общества в Российской Федерации.

2. Федеральный, региональный и муниципальный уровни применения Системного проекта

Ввиду отсутствия в Российской Федерации основополагающих общегосударственных правовых и технологических инфраструктурных составляющих, необходимых для формирования электронного правительства на всех уровнях, залогом успешности проектов, реализуемых на региональном и муниципальном уровнях в этой сфере, являются действия, осуществляемые федеральными органами власти. Особенно в части формирования «правил игры» и стандартов, как по разработке самих информационных систем всех уровней власти, так и по обеспечению интероперабельности, интеграции этих систем на базе создаваемой инфраструктуры электронного правительства, по обеспечению электронного информационного взаимодействия.

Ограниченность финансовых, временных, экспертных ресурсов, а также малое число завершенных успешных проектов в сфере создания электронного правительства в Российской Федерации приводит к необходимости локализации усилий государства в данной сфере на наиболее критических направлениях. Поэтому настоящий Системный проект затрагивает, прежде всего, деятельность федеральных органов исполнительной власти, их территориальных органов, подведомственных организаций. При этом деятельность исполнительных органов государственной власти субъектов Российской Федерации и органов местного самоуправления затрагивается в той степени, в которой она связана с реализацией полномочий федеральных органов исполнительной власти. Построение электронного правительства на региональном и муниципальном уровнях рассматривается в Системном проекте с точки зрения обязательных требований к инфраструктуре, без которых функционирование электронного правительства на этих уровнях невозможно. Аналогично региональному компоненту невозможно системно проектировать иные компоненты информационного общества («электронный регион», «электронное здравоохранение», «электронное правосудие» и т. д.) без определения требований к построению электронного правительства на федеральном уровне.

Вопросы деятельности бюджетных учреждений (здравоохранение, образование, культура и т.д.), а также информатизация деятельности судебной и законодательной власти являются предметом государственной программы «Информационное общество» и отдельно в настоящем Системном проекте не рассматриваются. Сводный анализ применимости положений настоящего Системного проекта к уровням и ветвям власти представлен в Таблице 2.1.

Таблица 2.1. Применимость требований Системного проекта к уровням и ветвям власти.

Содержание Системного проекта по направлениям	ФОИВ и их территориальные органы (подразделения)	Органы власти субъектов РФ	Органы местного самоуправления	Судебная, законодательная власть
Переход на исполнение государственных функций в электронном виде	Применимы полностью	Применимы в целом (с учетом нормативно-правовых актов (НПА) на уровне субъекта)	Применимы на уровне подходов и требований	Применимы в части раскрытия НПА
Перевод в электронный вид государственной учетной деятельности	Применимы полностью	Применимы в целом (с учетом НПА на уровне субъекта)	Применимы на уровне подходов и требований	Не применимы

Формирование ключевых инфраструктур электронного правительства	Применимы полностью	Применимы с учетом существующей инфраструктуры	Применимы на уровне подходов и требований	Применимы в части инфраструктуры электронного взаимодействия
Обеспечение доступности государственных услуг для граждан	Применимы полностью	Применимы в целом (с учетом НПА на уровне субъекта)	Применимы на уровне подходов и требований	Не применимы
Обеспечение эффективности бюджетных расходов на ИКТ	Применимы полностью	Применимы на уровне подходов и требований (с учетом НПА на уровне субъекта)	Применимы на уровне подходов и требований	Не применимы
Управление мероприятиями по созданию электронного правительства	Применимы полностью	Применимы с учетом региональных оргструктур	Применимы частично (с учетом местных оргструктур)	Не применимы

Таким образом, требования настоящего Системного проекта могут широко использоваться на региональном и муниципальном уровне в применимой части.

В Системном проекте рассматриваются следующие направления работ по формированию электронного правительства в Российской Федерации:

1. Переход на предоставление государственных услуг и исполнение государственных функций в электронном виде.
2. Перевод в электронный вид государственной учетной деятельности.
3. Информационно-технологические и инженерные компоненты электронного правительства.
4. Формирование ключевых инфраструктур электронного правительства.

К обеспечивающим направлениям работ по формированию электронного правительства относятся:

1. Обеспечение доступности государственных услуг для граждан и организаций.
2. Обеспечение эффективности бюджетных расходов на внедрение ИКТ федеральными органами исполнительной власти.
3. Порядок управления процессом формирования электронного правительства

На базе положений системного проекта должен быть разработан план мероприятий по формированию электронного правительства. Данные положения иллюстрирует рисунок 2.1.

Основополагающие направления работ:

Переход на предоставление государственных услуг и исполнение государственных функций в электронном виде.

Перевод в электронный вид государственной учетной деятельности.

Информационно-технологические и инженерные компоненты электронного правительства.

Формирование ключевых инфраструктур электронного правительства

Обеспечивающие направления работ:

Обеспечение доступности государственных услуг для граждан и организаций.

Обеспечение эффективности бюджетных расходов на внедрение ИКТ федеральными органами исполнительной власти.

Порядок управления формированием электронного правительства

План мероприятий по формированию электронного правительства

Рисунок 2.1. Направления работ по формированию электронного правительства.

3. Переход на предоставление государственных услуг и исполнение государственных функций в электронном виде

Типология полномочий федеральных органов исполнительной власти

В практике российского государственного управления отсутствует единая терминология и нормативно закреплённая типология государственных полномочий, функций и услуг исполнительных органов государственной власти, что создаёт методологические проблемы при формировании электронного правительства. Подобные ограничения также не позволяют в полной мере использовать международные индексы при планировании порядка исполнения государственных функций и предоставления государственных услуг с использованием ИКТ.

В связи с отсутствием нормативного закрепления понятий «полномочие», «государственная функция», «государственная услуга», «бюджетная услуга» для целей настоящего Системного проекта в качестве базового используется понятие «полномочие», используемое преимущественно в положениях о федеральных органах исполнительной власти (далее — Положение о ведомстве), иных нормативных правовых актах.

Термины «государственная функция», «государственная услуга» используются при описании видов деятельности государственных органов власти, а также для сохранения преемственности с действующей правовой базой. Государственные услуги по своему существу являются государственными функциями, исполнение которых инициируется заявителем, содержащими взаимосвязанный и неразрывный состав разрешительных и учетных полномочий, сопровождающих принятие исполнительным органом государственной власти решения, его учет, выдачу соответствующего разрешительного документа и предоставление информации о принятых решениях неограниченному кругу лиц.

Полномочия федеральных органов исполнительной власти в их текущих формулировках можно классифицировать различными способами, каждый из которых будет носить экспертный характер. Для целей настоящего Системного проекта используется следующая классификация:

1. Специфические государственные полномочия.

Формулировка и особенности реализации полномочия специфичны для конкретного федерального органа исполнительной власти. С точки зрения перевода полномочий в электронный вид целесообразно выделить следующие типы специфических полномочий:

- Разрешительные полномочия, реализуемые по волеизъявлению физического или юридического лица и связанные с получением или подтверждением исполнительным органом государственной власти юридически значимого статуса или права юридического или физического лица. К разрешительным полномочиям относят: аттестацию, регистрацию, аккредитацию, лицензирование, выдачу разрешений и т. д., а также связанные с ними полномочия по учету результатов разрешительной деятельности, выраженные в виде формирования, ведения, обработки и предоставления информации из государственных учетных систем.
- Контрольно-надзорные полномочия, реализуемые по инициативе государства (плановые проверки) либо пострадавших лиц (внеплановые проверки) и связанные с проверкой соблюдения и/или соответствия субъекта и объекта проверки обязательным требованиям. Включают в себя: контроль и надзор за объектами, субъектами; мониторинг результатов контроля; рассмотрение дел об административных правонарушениях и т. д.

- **Управленческие полномочия.** Государственные полномочия, имеющие отношение к осуществлению деятельности, не связанной с взаимодействием с гражданами и организациями, и направленные на управление в сфере ведения исполнительных органов государственной власти (мониторинг, аналитика, статистика).
2. Государственные полномочия по принятию нормативных правовых актов.
 3. Государственные учетные полномочия.
 4. Типовые государственные полномочия (документооборот, разъяснения, обращения физических и юридических лиц, мобилизационная подготовка и др.).

На рисунке 3.1 представлены основные полномочия федеральных органов исполнительной власти.

Наибольшая часть взаимодействия исполнительных органов государственной власти с гражданами и организациями осуществляется в рамках реализации специфических полномочий и полномочий по принятию нормативных правовых актов (в форме их публикации для всеобщего сведения).

По состоянию на конец 2009 г. 80 федеральных органов исполнительной власти имеют в своих Положениях о ведомствах более 6300 полномочий (записей). Число полномочий, зафиксированных в законодательстве, но не вошедших в Положения о ведомствах, может достигать нескольких тысяч.

В условиях отсутствия единого перечня государственных функций (государственных услуг), многообразия трактовок этих понятий и соотношения с полномочиями исполнительных органов государственной власти стихийно сложилась ситуация, при которой регламентации подлежал разный состав связанных по существу полномочий. Разрешительные полномочия регламентировались одновременно с полномочиями по проведению контроля (надзора), а также с полномочиями по ведению государственных баз данных и предоставлению информации из них, либо указанные полномочия регламентировались отдельно, в том числе по причине разного субъектного состава заявителей. Правильное формирование составов взаимоувязанных разрешительных, контрольно-надзорных и учетных полномочий позволит сформировать реальный перечень так называемых государственных функций и услуг.

В российской практике традиционная пятиэтапная классификация ООН перехода к электронным услугам имеет ограниченное применение (только к части разрешительных полномочий исполнительных органов государственной власти). Целевое состояние перехода к электронным способам взаимодействия для полномочий, связанных с контролем и надзором, и для управленческих полномочий, напрямую не связанных с взаимодействиями с гражданами и организациями, но значимыми для целей создания электронного правительства, должно планироваться по иной шкале.

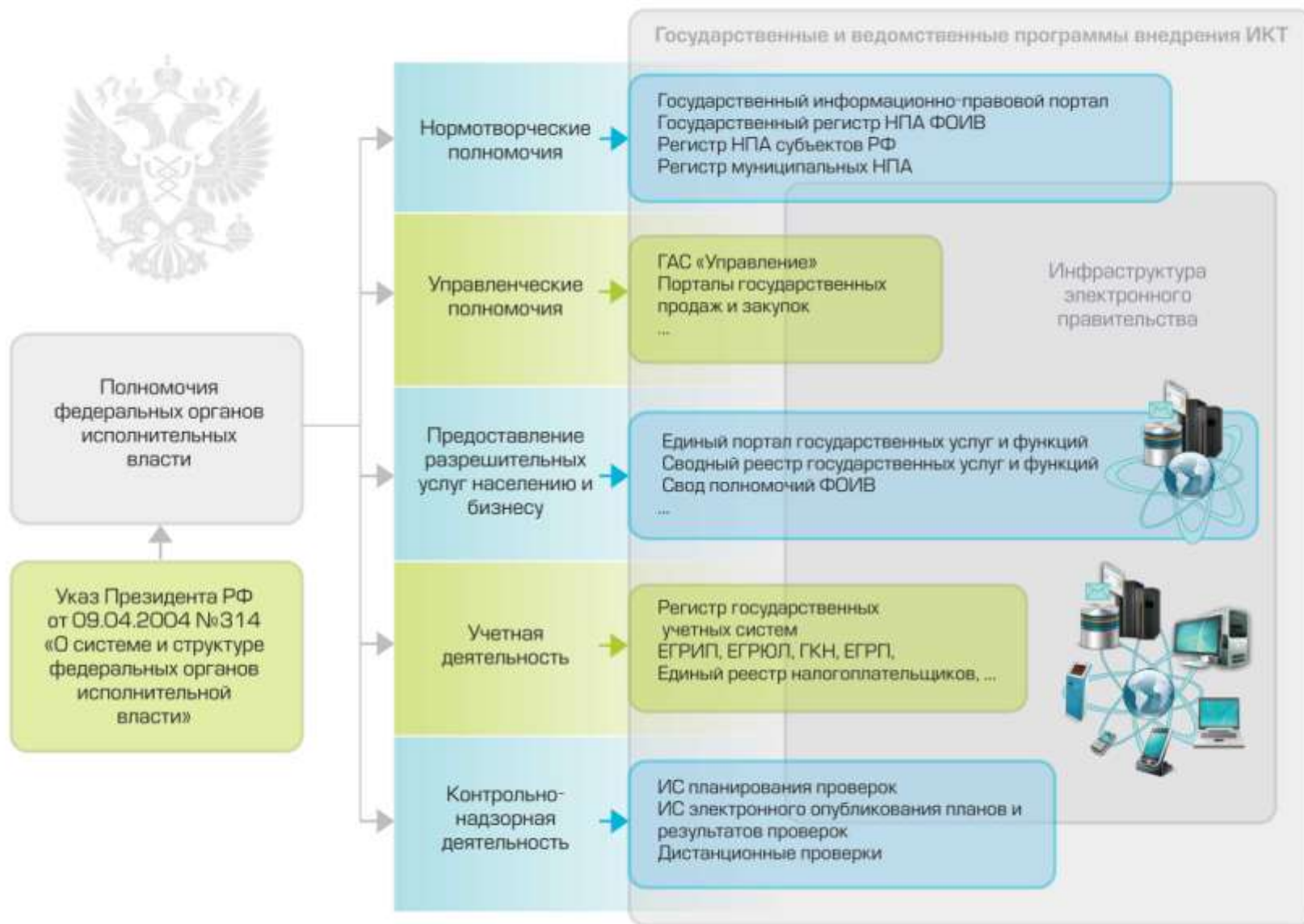


Рисунок 3.1. Полномочия органов исполнительной власти с примерами реализованных информационных систем и ресурсов.

Специфика реализации управленческих полномочий (мониторинг, аналитика, статистика)

Приоритетным направлением перевода в электронный вид полномочий, не связанных с взаимодействием с гражданами и организациями, является деятельность органов исполнительной власти по подготовке принятия управленческих решений в сфере государственного управления и контроль над их исполнением.

Для перевода в электронный вид данного типа полномочий создается единая вертикально-интегрированная государственная автоматизированная информационная система «Управление» (далее — ГАС «Управление»). В 2009 году была разработана и одобрена Правительственной комиссией по проведению административной реформы «Концепция создания единой вертикально-интегрированной государственной автоматизированной системы управления». Постановлением Правительства Российской Федерации от 25 декабря 2009г. №1088 утверждено Положение «О единой вертикально-интегрированной государственной автоматизированной информационной системе «Управление» и рекомендовано органам государственной власти субъектов Российской Федерации создать и обеспечить функционирование региональных автоматизированных информационных систем для интеграции в ГАС «Управление».

ГАС «Управление» предназначена для решения следующих задач:

- обеспечение информационно-аналитической поддержки принятия высшими органами государственной власти решений, а также при планировании деятельности этих органов;
- осуществление мониторинга, анализа и контроля исполнения принятых указанными органами решений, реализации основных направлений деятельности Правительства Российской Федерации, выполнения приоритетных национальных проектов, реализации мероприятий по оздоровлению российской экономики, процессов, происходящих в реальном секторе экономики, финансово-банковской и социальной сферах, социально-экономического развития субъектов Российской Федерации, эффективности деятельности органов государственной власти субъектов Российской Федерации.

В процессе решения этих задач обеспечивается систематизация и анализ:

- информации об уровне социально-экономического развития Российской Федерации и ее субъектов, в том числе в сопоставлении с мировой статистикой;
- информации об эффективности деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации;
- информации о ходе реализации программ, проектов, комплексов мероприятий, реализуемых за счет средств федерального бюджета;
- информации о бюджетных проектировках и об исполнении федерального бюджета, включая информацию о кассовом исполнении федерального бюджета и бюджетную отчетность главных распорядителей средств федерального бюджета;
- государственной официальной статистической информации, собираемой в соответствии с федеральным планом статистических работ;
- картографической информации и связанных с ней данных об объектах и ресурсах на территории Российской Федерации;
- нормативно-справочной информации, содержащейся в ведомственных информационных системах;
- иной информации, требующейся пользователям ГАС «Управление».

Существующие ведомственные автоматизированные информационные системы, участвующие в процессе подготовки принятия управленческих решений в сфере

государственного управления обеспечивают сбор, накопление, функциональную обработку и выдачу информации для поддержки принятия решений и контроля за ходом их выполнения. Вместе с тем государственные информационные ресурсы фактически разделены по сферам влияния и зонам ответственности органов государственной власти.

В этих условиях одной из важнейших задач становится задача интеграции в рамках ГАС «Управление» совокупности разрозненных государственных информационных ресурсов федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации и формирование единого информационного пространства.

При создании ГАС «Управление» целесообразно использовать единую инфраструктуру обеспечения юридически значимого электронного взаимодействия, а также обеспечить совместимость государственных информационных систем. Интеграция ведомственных автоматизированных информационных систем позволит обеспечить оперативный доступ к актуальной ведомственной информации.

Формирование единого информационного пространства позволит применить современный аналитический аппарат для анализа текущей ситуации, ее прогнозирования, выработки управленческих решений и контроля за их выполнением, а также обеспечить возможность комплексного отображения информации для быстрого ее восприятия и оперативного принятия управленческих решений.

На начало 2010 года проведены: первичное проектирование ГАС «Управление», разработка ряда ведомственных информационных систем Минрегионразвития России, Минэкономразвития России, Минкомсвязи России, Минздравсоцразвития России, ФСО России, а также центральных информационных систем, включающих:

- Центральную информационную систему ЦИС ГАС «Управление» шифр «Федерация» (ЦИС ГАСУ «Федерация»);
- Центральную информационную систему ЦИС ГАС «Управление» шифр «Контур» (ЦИС ГАСУ «Контур»);
- Прототип информационной системы обеспечения деятельности заместителя Председателя Правительства Российской Федерации - Руководителя Аппарата Правительства Российской Федерации (прототип ИСОД), обеспечивающей предоставление в едином интерфейсе информационно-аналитических материалов из различных информационных систем, мониторинг и анализ исполнения поручений руководства страны, ведение рабочих планов-графиков деятельности Руководителя Аппарата Правительства Российской Федерации.

В дальнейшем в период 2010 – 2012 годах будут выполняться работы по развитию ГАС «Управление», включая развитие структуры, расширение перечня решаемых задач, расширение состава систематизируемой и анализируемой информации.

Развитие структуры целесообразно осуществлять за счет ввода в состав ГАС «Управление» региональных информационных систем – создание регионального уровня, расширения состава ведомственных информационных систем, входящих в состав ГАС «Управление», расширения перечня взаимодействующих внешних систем и развития структуры центральной системы, а также информационных систем обеспечения деятельности Председателя Правительства РФ и его заместителей.

Расширение перечня решаемых задач предполагает проведение работ по совершенствованию аналитических возможностей ГАС «Управление», обеспечению планирования деятельности высших органов государственной власти, а также анализа и контроля исполнения принятых высшими органами исполнительной власти решений в сфере государственного управления.

Расширение состава систематизируемой и анализируемой информации необходимо проводить за счет использования информации, получаемой с помощью Единой межведомственной информационной статистической системы (ЕМИСС) и автоматизированной информационной системы (далее-АИС) Федерального казначейства,

а также информации от других информационных систем, необходимость использования которой определяется функциональными требованиями к ГАС «Управление», картографической информации и связанных с ней данных об объектах и ресурсах на территории Российской Федерации, нормативно-справочной информации, содержащейся в ведомственных информационных системах.

Специфика реализации в электронном виде разрешительных полномочий

Анализ показал, что в настоящее время к разрешительным полномочиям относится более 825 полномочий федеральных органов исполнительной власти, закрепленных в Положениях о ведомствах (по состоянию на конец 2009 г.). Законодательством и подзаконными актами Президента Российской Федерации и Правительства Российской Федерации может быть установлено до нескольких тысяч разрешительных полномочий (подобная инвентаризация не проводилась).

Реализация разрешительных полномочий всегда сопровождается деятельностью по учету юридически значимых фактов — факта подачи и принятия заявления и пакета документов; факта рассмотрения и принятия решения, включая отказ; факта выдачи документа, подтверждающего получение/подтверждение юридическим или физическим лицом статуса или права; факта предоставления информации из государственной учетной системы. Как следствие, реализация разрешительных полномочий тесно связана с реализацией учетных полномочий по формированию, ведению, обработке юридически-значимых фактов и сведений в соответствующих базах данных (кадастрах, реестрах и др.).

Перевод разрешительных полномочий в электронный вид

Ключевой задачей при реализации разрешительных полномочий в электронном виде является использование электронного межведомственного и межуровневого взаимодействия, взаимодействия с подведомственными организациями вместо запроса документов (сведений) у заявителя. Детализация целевого состояния для любого разрешительного полномочия по каждому этапу приведена ниже:

1. Информационный этап (предоставление информации):
 - Информация о государственной услуге (государственной функции) доступна в сети Интернет (в Сводном реестре и на Едином портале государственных и муниципальных услуг (функций)¹, а также, согласно действующему законодательству на официальных сайтах органов власти).
 - Информация из открытых государственных учетных информационных систем (далее — ИС), в том числе носящая правоподтверждающий или правоустанавливающий характер, доступна в сети Интернет.
 - Выработаны формализованные критерии доступности размещенной информации, реализован механизм мониторинга фактической доступности информации.
 - Разработаны механизмы оперативной корректировки размещаемой информации в результате выявляемых ошибок и неполноты.
 - Реализованы меры, обеспечивающие юридическую значимость размещаемой информации.

¹ См. постановление Правительства Российской Федерации от 15 июня 2009 г. № 478 «О единой системе информационно-справочной поддержки граждан и организаций по вопросам взаимодействия с органами исполнительной власти и органами местного самоуправления с использованием информационно-телекоммуникационной сети Интернет»

- Созданы информационные сервисы, специфичные для конкретной услуги, в том числе поиск ближайшего территориального органа (подразделения), проверка названий регистрируемых объектов и т. д.
2. Этап одностороннего взаимодействия (предоставление необходимых форм и бланков):
- Формы заявлений и иные документы (анкеты, бланки, платежные документы и т.п.) доступны для:
 - заполнения и последующей распечатки заполненного документа заявителем;
 - скачивания и заполнения заявителями в электронной форме;
 - скачивания, распечатки и заполнения заявителем в бумажной форме.
 - Реализованы сервисы контроля корректности заполнения форм, выбора вводимых данных из доверенных нормативно-справочных источников.
 - Реализованы сервисы хранения частично заполненных форм, предоставления предзаполненных типовым образом форм.
 - Обеспечена юридическая значимость размещаемых форм.
 - Обеспечено выполнение требования обязательного приема органом власти документов, формы которых размещены на портале.
3. Двустороннее взаимодействие (начало предоставления услуги в электронном виде):
- Обеспечен прием заявлений (волеизъявлений) о предоставлении государственной услуги в электронной форме.
 - Обеспечен прием в электронной форме документов, необходимых для подтверждения права получения услуги.
 - Обеспечен прием электронных графических образов (изображений) документов, необходимых для подтверждения права получения услуги, предоставленных третьими лицами в бумажной форме.
 - Обеспечен прием платежей (налогов, пошлин, сборов) посредством электронных и мобильных платежных систем.
 - Обеспечен прием реквизитов платежных документов, подтверждающих совершение заявителем обязательных платежей посредством электронных и мобильных платежных систем.
 - Реализованы механизмы взаимного преобразования документов и сведений, хранящихся в юридически значимом виде в бумажной и электронной форме.
 - Обеспечено предоставление заявителю в электронной форме документов (сведений), являющихся доказательством факта удаленного взаимодействия и отражающих его содержание.
 - Обеспечены механизмы оперативного доказательного досудебного обжалования действий (бездействия) органа власти, обращения в контролирующие органы или судебного обращения.
4. Интерактивный этап:
- Заявитель может осуществлять удаленный мониторинг хода предоставления услуги (прием заявления, запрос дополнительных сведений, отказ, принятие решения).
 - Заявитель может поручить (доверить) органу власти получение необходимых для предоставления государственной услуги документов (сведений) в иных федеральных органах исполнительной власти.
 - Заявитель может не предоставлять документы (сведения), имеющиеся у иных федеральных органов исполнительной власти.
 - Мониторинг хода предоставления услуги осуществляется по множественным каналам доступа (компьютеры, мобильные устройства, SMS, почтовые сообщения).
 - Обеспечена электронная форма ведения государственных учетов — юридическим фактом принятия решения и получения результата

предоставления услуги (исполнения функции) является учетная запись в электронной учетной системе.

- Документ, подтверждающий результат предоставления услуги, предоставляется заявителю по его выбору в бумажной и (или) электронной форме и является выпиской (справкой) из электронной учетной системы.
- Заявителю третьей доверенной стороной предоставляются в электронной форме в юридически значимом виде доказательства факта и содержания удаленного взаимодействия с предоставляющим государственную услугу органом власти.

5. Этап полностью удаленного взаимодействия:

- Заявитель может осуществить все необходимые для предоставления государственной услуги действия в полностью удаленном режиме.
- Обеспечено юридически значимое электронное взаимодействие между всеми участниками предоставления услуги.
- Органам власти обеспечена возможность (при согласии заявителя) самостоятельно запрашивать документы (сведения) в электронных учетных системах иных органов власти и организаций, участвующих в предоставлении услуги.
- Документ, подтверждающий результат предоставления услуги, предоставляется заявителю по его выбору в бумажной и (или) электронной форме.
- Заявителю предоставляются в электронной форме доказательства факта и содержания удаленного взаимодействия с предоставляющим государственную услугу органом власти

На рисунке 3.2 представлено целевое состояние разрешительных полномочий федеральных органов исполнительной власти для пяти этапов.

Типология взаимодействий между органами власти и заявителями

Каждый тип взаимодействий между органами власти и заявителями, происходящих в электронной форме, должен быть определен как юридический факт. Это необходимо для определения момента возникновения правовых отношений между государственным органом и заявителем, состава правовых последствий и момента их наступления.

Форма, в которой осуществляется взаимодействие между заявителями и органами власти должна обеспечивать определенность состава правоотношений и наступающих правовых последствий. При автоматических взаимодействиях с помощью программных средств это должно иметь прямое отражение в нормативных правовых актах, регламентирующих порядок предоставления услуги и субъектный состав лиц, вступающих в отношения.

На конец 2009 г. изменение нормативной правовой базы федеральных органов исполнительной власти, региональных и муниципальных властей преимущественно сосредоточено на подаче заявления в электронной форме и мониторинге ее прохождения. Однако порядок реализации государственных полномочий, связанных с получением/подтверждением юридически значимого для заявителя статуса или права, содержит существенно более широкий набор типовых и значимых действий, обязанность совершения которых возложена либо на заявителя, либо на ответственный за выдачу итогового результата орган исполнительной власти (см. рисунок 3.3).

Для каждого из перечисленных ниже типовых действий, связанных с получением/подтверждением статуса или права заявителя, предусмотрено целевое состояние перевода в электронный вид:

1. Получение исчерпывающей информации о порядке исполнения государственных функций и предоставления государственных услуг.
2. Сбор подтверждающих документов, выдаваемых подведомственными организациями, иными государственными органами исполнительной власти, органами местного самоуправления, сторонними организациями.

3. Уплата государственной пошлины, иных неналоговых платежей (если это предусмотрено процедурой получения/подтверждения статуса или права), а также совершения иных юридически значимых действий.
4. Поиск, заполнение заявления в бумажно-письменной форме, скрепление его печатью и/или подписью с указанием контактных данных и способа взаимодействия с исполнительными органами государственной власти (почта, телефон, иные способы).
5. Запись на прием в исполнительный орган государственной власти в случае необходимости подачи заявления, пакета документов, материальных объектов лично, либо при наличии установленного разрешения через представителя.
6. Непосредственное и личное посещение государственного органа исполнительной власти, либо при наличии установленного разрешения через представителя, и представление устного или письменного заявления, пакета документов, материальных объектов уполномоченному должностному лицу.

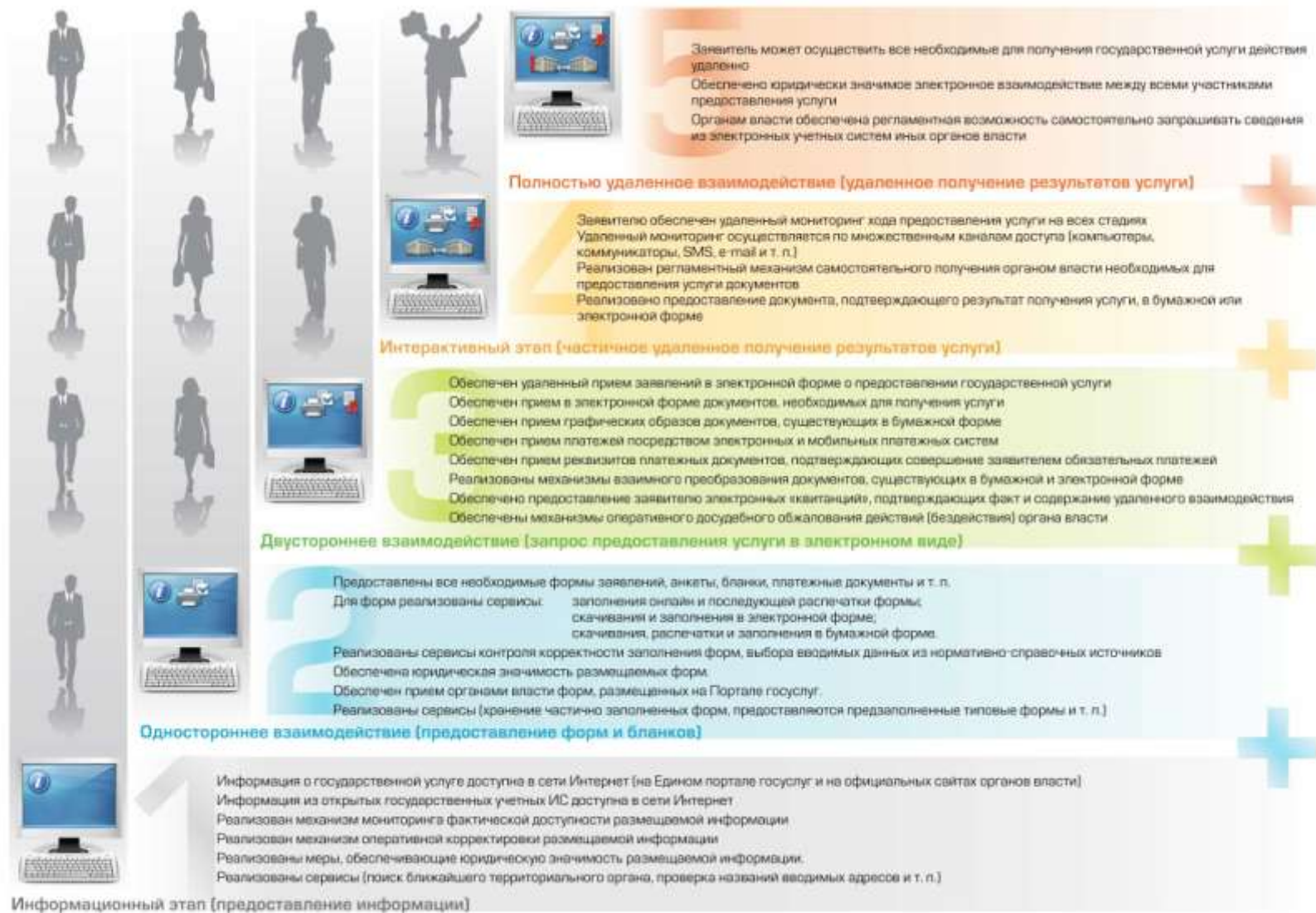


Рисунок 3.2. Целевое состояние разрешительных полномочий федеральных органов исполнительной власти для пяти этапов.

7. Направление заявления и пакета документов при отсутствии требований по представлению оригинальных документов и/или материальных объектов по почтовой связи или иными нормативно установленными способами.
8. Подтверждение исполнительным органом государственной власти получения заявления, пакета документов, материальных объектов.
9. Отказ или приостановление исполнительным органом государственной власти рассмотрения заявления, пакета документов, материальных объектов, до предоставления заявителем дополнительных подтверждающих его статус документов, материальных объектов.
10. Проверка и экспертиза исполнительным органом государственной власти возможности получения/подтверждения статуса или права, в том числе выездная проверка или экспертиза, исследования с участием подведомственных и иных организаций.
11. Размещение, обработка, хранение документов, представленных заявителем в архивных делах в письменно-бумажной форме.
12. Согласование исполнительным органом государственной власти принимаемого промежуточного или итогового решения с иными исполнительными органами государственной власти.
13. Информационное взаимодействие ответственного за итоговое решение исполнительного органа государственной власти с иными органами власти, третьими лицами в целях запроса и/или подтверждения сведений, предоставленных заявителем.
14. Принятие решения исполнительным органом государственной власти, в том числе путем регистрации факта принятия решения и занесения соответствующей записи в государственную базу данных, а также при наличии в учетную информационную систему.
15. Уведомление заявителя о принятом решении с использованием почтовой, телефонной, а также иных применяемых исполнительным органом государственной власти средств коммуникации.
16. Выдача заявителю документа на бумажном носителе, подтверждающего факт отказа или получения/подтверждения статуса или права, являющегося итоговым результатом исполняемых государственных услуг.
17. Внесение регистрационной записи о полученном/подтвержденном статусе или праве в оригинальный документ, принадлежащей заявителю.
18. Предоставление дубликата выданного разрешительного (подтверждающего) документа (за отдельную плату).
19. Приостановление, либо отмена действия выданного на бумажном носителе разрешительного (подтверждающего), с одновременной регистрацией факта принятого решения и занесения соответствующей записи в государственную базу данных, а также при наличии в учетную ИС.
20. Получение материальных результатов по итогам присвоения или подтверждения статуса или права (материальная помощь, денежные средства, льготы, знаки и т. д.).
21. Формирование, ведение, обработка и хранение юридически значимых событий или действий, сопровождающих реализация разрешительных полномочий, в государственной базе данных, а также при наличии в учетной ИС.
22. Делегирование подведомственным организациям учетных полномочий по регистрации факта принятия решения и занесения соответствующей записи в государственную базу данных, а также при наличии в учетную ИС.
23. Предоставление исполнительным органом государственной власти сведений в форме выписок, справок, получившему/подтвердившему статус или право физическому или юридическому лицу, а также третьим лицам.

24. Размещение исполнительным органом государственной власти ограниченного объема сведений о зарегистрированных правах и статусах в свободном или платном доступе на официальном сайте ведомства.

Подача заявления (обращения) в орган власти фиксирует факт обращения (волеизъявления лица), с момента которого обратившийся получает право получить результаты рассмотрения заявления в установленном порядке, а также требовать у органа власти информацию о ходе рассмотрения своего заявления. Целевым состоянием для процедуры волеизъявления (подачи заявления) является возможность осуществления ее в электронной форме. В заявлении на получение государственной услуги заявитель должен сделать выбор, определяющий, можно ли использовать сведения о его новом статусе в процессах предоставления ему государственных услуг (реализации иных полномочий государства в отношении заявителя). Заявитель также может определить срок, в течение которого данное разрешение актуально.

Получение обращения государственным органом означает, что уполномоченное должностное лицо органа власти обязано произвести регистрацию входящего документа, проверить его соответствие предъявляемым требованиям, в том числе, с учетом компетенции государственного органа, обеспечить передачу заявления (обращения) лицу, ответственному за принятие решения по существу, обязанность государственного органа рассмотреть обращение в установленный срок.

Целевым состоянием для процедуры подтверждения нового юридического статуса заявителя является самостоятельный сбор органом власти сведений о статусах заявителя в электронных учетных системах иных органов власти и организациях. Присвоение нового статуса заявителю должно производиться по результатам регламентированной автоматизированной процедуры, инициированной органом власти (организацией), в которую обращается заявитель. В соответствии с регламентом производится запрос в электронные учетные системы иных органов власти, содержащие сведения о текущих статусах заявителя, имеющих значение для получения конкретной услуги. При подтверждении соответствия совокупности статусов заявителя (продукции, объектов) установленным требованиям им присваивается новый статус. Для исключения злоупотреблений факт запроса и получения доступа к статусам заявителей должен фиксироваться, а любой гражданин или организация должны иметь возможность свободного доступа к данным, касающимся их запросов. Анонимные запросы сведений относительно статусов граждан и организаций (например, от имени органа власти) должны быть исключены.

Принятие решения государственным органом влечет за собой возникновение правовых последствий (возникновение права осуществлять деятельность, распоряжаться вещью и т. д.; лишение права; изменение правового статуса лица; прекращение и возникновение обязанности и т. п.). Государственный орган обязан проинформировать заявителя о состоявшемся решении, направить (выдать) ему результат осуществления государственной функции (предоставления государственной услуги), а также зафиксировать срок предоставления услуги. Это в свою очередь лишает заявителя возможности требовать рассмотрения обращения по существу и иных прав, связанных с взаимодействием с государственным органом в процессе рассмотрения им обращения. Одновременно с этим у заявителя возникает право обжаловать решение государственного органа.

Целевым состоянием этапа принятия решения является юридически значимая запись в электронной учетной системе. Бумажный документ должен быть вторичным по отношению к записи в электронной учетной системе при условии исключения имеющихся законодательных ограничений. По желанию заявителя в течение неопределенного времени ему может быть выдан по его выбору электронный или бумажный документ, подтверждающий его статус.

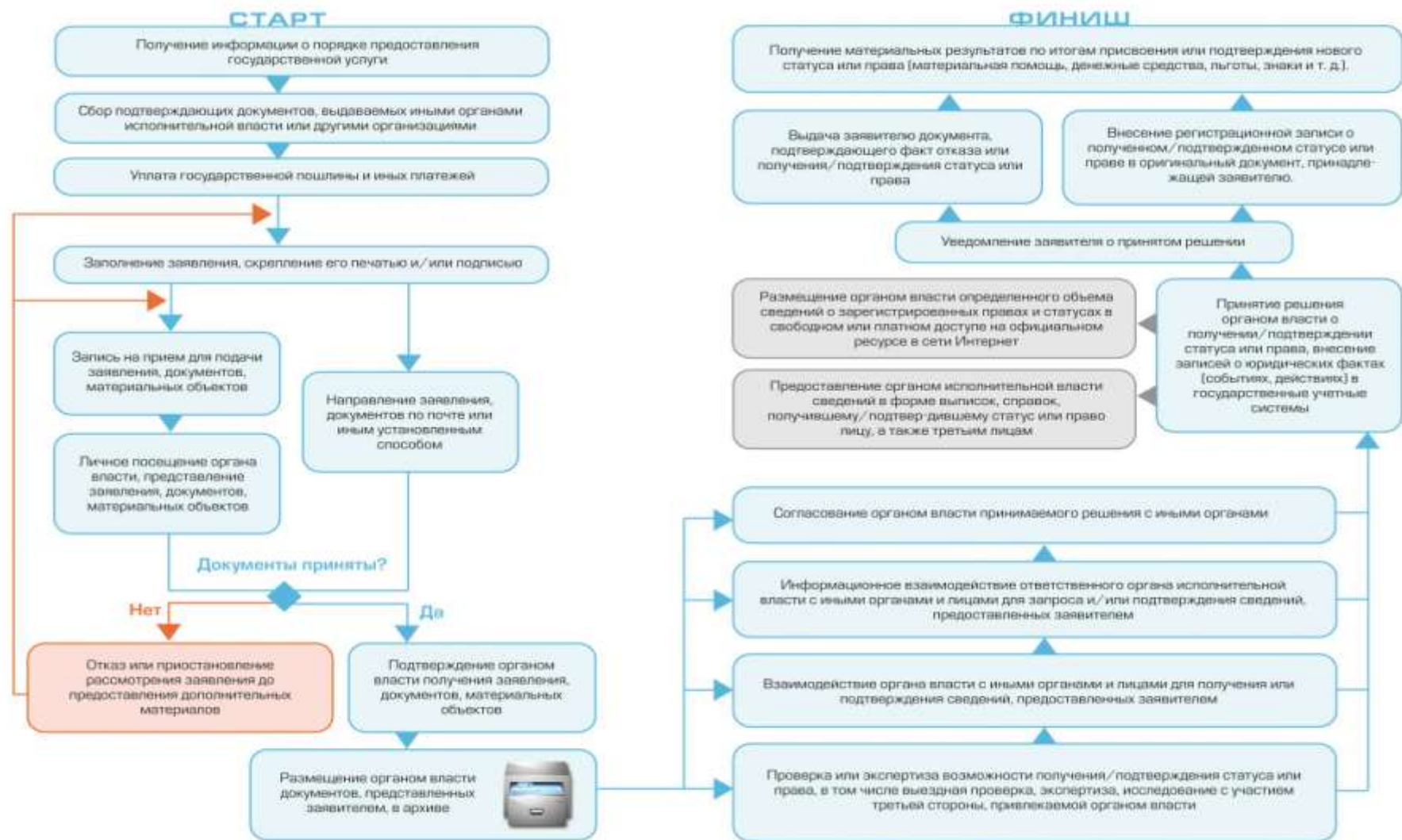


Рисунок 3.3. Типовые действия, связанные с получением/подтверждением юридически значимого для заявителя статуса или права.

Ограничения для перевода разрешительных полномочий в электронный вид

В распоряжениях Правительства Российской Федерации от 17.10.2009 № 1555-р и от 17.12.2009 № 1993-р описывается целевое состояние перевода государственных и муниципальных функций и услуг в электронный вид на основе пяти этапов. Однако изначальная неопределенность «границ» государственной/муниципальной функции (государственной/муниципальной услуги), подлежащей переводу в электронный вид, приводит к невозможности описания целевых характеристик исполнения государственной/муниципальной функции (предоставления государственной/муниципальной услуги) в электронном виде. Исходя из наименования государственной/муниципальной функции (государственной/муниципальной услуги) даже при наличии административного регламента практически невозможно описать все ее результаты, сценарии и участников.

Нормативное правовое регулирование ряда государственных/муниципальных функций (услуг), включая утвержденные административные регламенты, не позволяет исчерпывающим образом определить реальный состав участников. Для многих случаев пятая стадия принципиально недостижима без включения в процесс формирования электронного правительства подведомственных и иных организаций, участвующих в исполнении государственных/муниципальных функций (предоставлении услуг), для дистанционного предоставления результатов экспертиз, исследований и испытаний.

Потенциально из 74 государственных функций (государственных услуг), предусмотренных Перечнем (по распоряжению № 1555-р), полностью могут быть переведены в электронный вид только 47 (т. е. 64%). В прочих случаях останется неизбежным личный контакт заявителя с должностными лицами федерального органа исполнительной власти либо организации.

Проблема описания состава полномочий относится в равной степени также и к контрольно-надзорным полномочиям.

Для системной работы по переводу в электронный вид процедур исполнения полномочий исполнительных органов государственной власти требуется формирование перечня государственных услуг (государственных функций) с описанием характеристик, набор которых достаточен для определения результатов исполнения государственной функции (предоставления государственной услуги), правовых оснований, круга участников (органы власти, организации, типы заявителей). Перечень утверждается актом Правительства Российской Федерации в целях планирования перевода государственных функций (государственных услуг) в электронный вид (содержит ограниченное количество функции (услуг) — до 50 ежегодно). В перспективе перечень должен стать основой для создания юридически значимого и систематизированного учета государственных полномочий федеральных органов исполнительной власти.

Аналогичные проблемы возникают при переводе услуг, предоставляемых органами исполнительной власти региона и органами местного самоуправления.

Отдельную проблему представляет сложность межведомственной координации при переходе на исполнение государственных функций (предоставление государственных услуг) в электронном виде.

На текущий момент деятельность по оптимизации государственных функций (государственных услуг), необходимая для перевода государственных функций (государственных услуг) в электронный вид, практически не скоординирована между уполномоченными федеральными органами власти, координационными органами при Правительстве Российской Федерации, а также между подразделениями федеральных ведомств. Решения по информатизации зачастую опережают действия по оптимизации государственного регулирования, прежде всего, массовых государственных услуг.

Специфика реализации в электронном виде контрольно-надзорных полномочий

Анализ функционала (нормативно установленной деятельности) федеральных ведомств, проведенный Институтом государственного и муниципального управления ГУ-ВШЭ, показал, что в Положениях о федеральных органах исполнительной власти закреплено 558 контрольно-надзорных полномочий (по состоянию на конец 2009 г.). При этом около 400 контрольно-надзорных полномочий касаются проведения проверок юридических и физических лиц, а также индивидуальных предпринимателей.

Всего без учета налоговых проверок и проверок со стороны правоохранительных органов в Российской Федерации в год проводится более 20 млн. проверок предпринимателей. В исполнении контрольно-надзорных функций занято около 70% государственных служащих федеральных органов исполнительной власти.

Ограничения для перевода контрольно-надзорных полномочий в электронный вид

Объективные и неустраняемые ограничения

Основная часть государственного контроля (надзора) осуществляется при обязательном использовании процедур проведения исследований, испытаний, измерений объектов проверки (далее — исследования) в ходе инструментального и визуального контроля, сопровождающегося необходимостью изъятия у проверяемого субъекта образцов продукции, проб обследования объектов окружающей среды и объектов производственной среды. Результатами проведения исследований являются документы, подтверждающие соответствие объекта проверки требованиям (санитарно-эпидемиологические заключения, сертификаты и т. п.). Подавляющее большинство исследований осуществляется подведомственными и/или аккредитованными организациями, аттестованными субъектами, уполномоченными на это органами исполнительной власти.

На конец 2009 г. имеет место объективная невозможность перехода к дистанционному взаимодействию в электронной форме при проведении исследований, сопровождающихся необходимостью изъятия у проверяемого субъекта образцов продукции, проб обследования объектов окружающей среды и объектов производственной среды.

Системные ограничения

К системным ограничениям относятся организационные и нормативные проблемы, устранить которые необходимо в процессе оптимизации контрольно-надзорных полномочий исполнительных органов государственной власти, в том числе путем введения запрета на ведомственное нормотворчество и перевода обязательных требований на уровень законодательных и/или правительственных актов.

Текущей системе государственного контроля (надзора) свойственны:

- Противоречивость, дублирование и избыточность предмета контроля (надзора) или совокупности обязательных требований, предъявляемых проверяющим должностным лицом к объекту и субъекту проверки.
- Отсутствие нормативно закрепленных и унифицированных требований к предмету проверки, отсутствие законодательного закрепления обязательных требований к объектам и субъектам проверки, а также их официальной публикации и бесплатному размещению в открытых источниках, включая официальные сайты органов исполнительной власти (например, платные официальные тексты ГОСТов, СанПиНов обязывают иметь на производстве на бумажном носителе).
- Отсутствие формализованного и нормативно закрепленного набора требований к критериям, необходимым для разграничения компетенции между уполномоченными на проведение государственного контроля (надзора)

органами исполнительной власти по объектам, субъектам и предметам проверки.

- Отсутствие нормативно закрепленных требований к учету субъектов и объектов проверки, результатов проверки, включая санкции, возложенные на субъектов проверки по ее результатам.
- Отсутствие нормативно закрепленной связи между видом государственного контроля (надзора); полномочиями исполнительного органа государственной власти; делегированными полномочиями подведомственных и/или аккредитованных организаций; предметом контроля (надзора); совокупностью обязательных требований, предъявляемых государством к объекту и субъекту проверки; субъектом и/или объектом проверки.
- Отсутствие нормативно закрепленных унифицированных требований и дефиниций, применимых к проверке: документарные (камеральные), выездные проверки; плановые, внеплановые проверки; инструментальный, визуальный, документарный контроль; инспекционный, сертификационный контроль; внутриведомственный, межведомственный контроль и государственный контроль за юридическими лицами, индивидуальными предпринимателями, физическими лицами и т. п.

Ограничения в виде неблагоприятной правоприменительной практики

К таким ограничениям относятся препятствия, устраняемые в ходе реализации Федерального закона № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля».

Возможности перевода ряда контрольно-надзорных полномочий в электронный вид определены следующими положениями названного Федерального закона:

- необходимость публикации ежегодных сводных плановых проверок на сайте органов исполнительной власти и на сайте Генеральной прокуратуры Российской Федерации;
- необходимость согласования внеплановых проверок с Генеральной прокуратурой Российской Федерации;
- обязательность уведомления саморегулируемой организации о проверке ее членов, обязательность уведомления субъекта проверки о плановой проверке;
- обязательность взаимодействия субъекта проверки и исполнительного органа государственной власти, уполномоченного на осуществление государственного контроля (надзора), в том числе для доказательства или подтверждения исполнения выявленных в ходе проверки предписаний.

Однако на начало 2010 г. практика размещения информации о сводных ежегодных планах проведения плановых проверок (являющихся, по сути, правовыми основаниями их проведения) применяется лишь узким кругом ведомств, отсутствуют нормативно определенные санкции и государственный контроль за размещением такой информации.

Нормативно не закреплена необходимость информирования заинтересованных лиц и общественности о результатах проведения проверок, отсутствует нормативно закрепленный перечень сведений, подлежащий обязательному опубликованию в открытом и бесплатном доступе на официальном сайте (к примеру, публикация наименований юридических лиц, деятельность которых приостановлена или прекращена).

Отсутствует практика применения исполнительными органами государственной власти документарных проверок, сопровождающихся обязательным дистанционным взаимодействием субъекта проверки и уполномоченного на осуществление государственного контроля органа исполнительной власти путем направления субъектом проверки в письменной форме документов, подтверждающих его соответствие обязательным требованиям.

Положения Федерального закона №294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля» могут быть по аналогии применены в иных, не входящих в сферу регулирования 294-ФЗ, видах государственного контроля (надзора).

Планирование перевода контрольно-надзорных полномочий в электронный вид

Целевое состояние перевода отдельных процедур в электронный вид в части контрольно-надзорных полномочий имеет вид:

1. Планирование проведения проверок юридических лиц, индивидуальных предпринимателей органами, уполномоченными на осуществление государственного контроля (надзора), а также размещение ежегодных сводных планов проведения плановых проверок на сайте исполнительного органа государственной власти
 - Руководитель любого исполнительного органа государственной власти, уполномоченного на осуществление любого государственного контроля (надзора), утверждает ежегодный сводный план проведения плановых проверок.
 - В законодательство вносятся изменения в части признания юридически значимым факта публикации ежегодного сводного плана проведения плановых проверок на сайте органа исполнительной власти.
 - В законодательство вносятся изменения в части уточнения состава сведений, включаемых в ежегодный сводный план проведения плановых проверок.
 - Допускаются иные способы доведения до сведения заинтересованных лиц ежегодного сводного плана проведения плановых проверок.
2. Размещение планов проведения плановых проверок на сайте Генеральной прокуратуры Российской Федерации:
 - Правительству Российской Федерации необходимо внести изменения в Порядок размещения планов проведения плановых проверок на сайте Прокуратуры Российской Федерации, а также форму и содержание ежегодного сводного плана проведения плановых проверок и предусмотреть подачу документов в том числе на электронном носителе.
 - Генеральной прокуратуре Российской Федерации внедрить государственную автоматизированную информационную систему формирования сводного плана проведения плановых проверок.
3. Информирование о результатах проведения проверок юридических лиц, индивидуальных предпринимателей органами, уполномоченными на осуществление государственного контроля (надзора) на официальном сайте ведомства:
 - Для реализации указанной новеллы Правительству Российской Федерации необходимо разработать и утвердить Порядок подготовки докладов об осуществлении государственного контроля (надзора), а также унифицированные требования к его содержанию (результаты проведения проверок, количество предписаний, количество возбужденных дел об административных правонарушениях, количество штрафов, постановлений о приостановлении деятельности, постановлений об отзыве продукции из оборота и т. п.).
 - Необходимо также предусмотреть обязательное размещение результатов проведения проверок, статистики, а также иной обязательной информации наряду с докладами об осуществлении государственного контроля (надзора) на официальном сайте исполнительного органа государственной власти.

4. Уведомления юридических лиц, индивидуальных предпринимателей органами, уполномоченными на осуществление государственного контроля (надзора), о проведении и результатах плановой проверки.
 - Для целого ряда взаимодействий исполнительного органа государственной власти и субъекта проверки возможна организация взаимодействия с помощью обмена документами в электронном виде, для чего необходимо внесение изменений в Федеральный закон №294-ФЗ.
5. Документарные проверки:
 - Для проведения документарной проверки возможна организация взаимодействия исполнительного органа государственной власти с субъектами проверки с помощью обмена документами в электронном виде, для чего необходимо внесение изменений в Федеральный закон №294-ФЗ.

Детализированное описание этапов реализации в электронном виде контрольно-надзорных полномочий приведено ниже:

1. Инвентаризация и публикация:
 - Перечень контрольно-надзорных полномочий нормативно закреплён.
 - По каждому контрольно-надзорному полномочию в открытом и бесплатном доступе на официальном сайте исполнительного органа государственной власти опубликованы основополагающие и юридически значимые для проведения проверок сведения, включая официальную публикацию совокупности обязательных требований к субъектам и объектам проверки (предмет проверки).
 - По каждому контрольно-надзорному полномочию опубликованы правовые основания и результаты проведения проверок, включая официальную публикацию планов проведения ежегодных плановых проверок, результатов проведения плановых и внеплановых проверок, а также статистики.
2. Двустороннее взаимодействие:
 - Исполнительный орган государственной власти взаимодействует с субъектами проверки путем обмена документами в электронной форме в следующих случаях:
 - уведомление исполнительным органом государственной власти о проверке;
 - направление субъектом проверки документов, необходимых для подтверждения соответствия обязательным требованиям в ходе документарной проверки.
3. Интерактивное взаимодействие:
 - В случае документарных проверок обеспечена возможность самостоятельного получения исполнительным органом государственной власти документов, сведений, информации о статусе субъекта и объекта проверки в иных исполнительных органах государственной власти.
 - Возможность затребования сведений у юридических и физических лиц в электронном виде только по отношению к тем документам и сведениям, которые не могут быть получены в иных исполнительных органах государственной власти.

Специфика реализации полномочий по принятию нормативных правовых актов

Наиболее значимым направлением формирования электронного правительства в сфере реализации полномочий по нормативному правовому регулированию, является деятельность по обеспечению своевременного и полного опубликования в сети Интернет разрабатываемых и принимаемых нормативных правовых актов в электронном виде. Ключевым направлением совершенствования законодательства в данной сфере должно

стать изменение порядка официального опубликования правовых актов, закрепление за текстами правовых актов в электронном виде статуса источника официального опубликования.

Целесообразно определить единый порядок официального опубликования всех правовых актов (федеральных законов; актов Президента Российской Федерации, Правительства Российской Федерации, государственных органов и органов местного самоуправления). Опубликование нормативных правовых актов имеет своей главной целью извещение граждан и организаций о принимаемых нормативных правовых решениях. Создание единого официального сайта в сети Интернет может существенно сократить издержки, связанные с официальным опубликованием актов, сократить сроки их опубликования, существенно повысить доступность текстов правовых актов.

Нормативные правовые акты федеральных органов исполнительной власти, затрагивающие права, свободы и обязанности человека и гражданина, устанавливающие правовой статус организаций, имеющие межведомственный характер и некоторые другие подлежат государственной регистрации в Министерстве юстиции Российской Федерации и последующему официальному опубликованию.

Помимо актов федеральных органов исполнительной власти государственной регистрации также подлежат акты, имеющие нормативный характер, издаваемые Центральным банком Российской Федерации, Пенсионным фондом Российской Федерации, Федеральным фондом обязательного медицинского страхования, Фондом социального страхования Российской Федерации.

Федеральные органы исполнительной власти определили десятки источников официального опубликования. Обязанность публикации на своих официальных сайтах нормативных правовых актов, относящихся к полномочиям федеральных органов исполнительной власти, установлена законодательством Российской Федерации, однако такие публикации, будучи официальными, не связаны с вступлением актов в силу. Кроме того, де-факто публикуется малая часть нормативных правовых актов, значительная часть опубликованных актов не актуальна.

Некоторые акты Президента Российской Федерации и Правительства Российской Федерации, федеральных органов исполнительной власти публикуются не в полном объеме (например, без приложений), что делает их фактически недоступными для граждан и организаций. Таким образом, в настоящее время имеет место неполное и плохо доступное опубликование нормативных правовых актов федеральных органов исполнительной власти. В Российской Федерации роль общепринятого источника информации о содержании нормативных правовых актов играют правовые базы, информация в которых не носит официального характера, и доступ к которым имеет ценовые и технологические ограничения.

Основные требования к внедрению официального опубликования нормативных правовых актов в электронном виде таковы:

- электронное опубликование должно носить официальный характер и происходить согласно нормативно закрепленной процедуре, обеспечивая вступление акта в законную силу, включая выполнение существующих для отдельных категорий нормативных правовых актов специфических процедур (например, государственной регистрации нормативных правовых актов федеральных органов исполнительной власти в Министерстве юстиции Российской Федерации);
- электронное опубликование должно осуществляться органом власти или по волеизъявлению органа власти, принявшего нормативный правовой акт;
- электронное опубликование должно выполнять информационную функцию, заключающуюся в обнародовании содержания и текста правового акта;

- электронное опубликование должно обеспечивать неизменность как самих актов после их официального опубликования, так и места и времени их опубликования (реквизитов публикации);
- должна обеспечиваться эквивалентность официальной электронной и бумажной публикации (в период их совместного существования);
- должна обеспечиваться возможность получения официальных выписок (текстов) в электронном виде;
- тексты опубликованных актов должны быть доступны для ознакомления и получения в электронном виде круглосуточно без взимания платы неограниченному кругу лиц;
- должна быть обеспечена технологическая, программная, лингвистическая и организационная доступность пользования официальными сайтами — источниками официального опубликования нормативных правовых актов.

В среднесрочной перспективе необходимо обеспечить:

- Изменение порядка официального опубликования законодательных и подзаконных нормативных правовых актов, предусматривающего обязательное опубликование нормативных правовых актов в электронном виде на государственном информационно-правовом портале (далее — ГИПП) и на официальных сайтах федеральных органов исполнительной власти.
- Разработку порядка формирования и ведения ГИПП.
- Разграничение компетенции по размещению нормативных правовых актов на государственном информационно-правовом портале различных участников законотворческой и нормотворческой деятельности (операторов портала).
- Разработку ГИПП, содержащего бесплатный доступ к нормативным правовым актам, а также поисковую систему, классификаторы нормативной правовой информации, программно-аппаратные интерфейсы для автоматизированного взаимодействия с внешними ИС, в том числе Сводным реестром государственных функций и услуг, государственным реестром нормативных правовых актов федеральных органов исполнительной власти, поисковыми системами Интернет.
- Обязательную публикацию на официальных сайтах федеральных органов исполнительной власти нормативных правовых и индивидуальных правовых актов федеральных органов исполнительной власти, не нуждающихся в государственной регистрации в Минюсте России, обеспечивающую их вступление в силу.
- Изменение статуса федерального регистра нормативных правовых актов субъектов Российской Федерации, федерального регистра муниципальных нормативных правовых актов, публикацию текстов нормативных правовых актов субъектов Российской Федерации, муниципальных нормативных правовых актов на ГИПП.
- Проведение регулярного мониторинга доступности и бесплатности законодательных и подзаконных нормативных правовых актов, размещенных на ГИПП и на официальных сайтах федеральных органов исполнительной власти.

Выводы и предложения, связанные с реализацией полномочий федеральных органов исполнительной власти в электронном виде

На основе анализа текущего порядка исполнения государственных функций и предоставления государственных услуг, а также их целевого состояния, связанного с их переводом в электронный вид, проведенного в предыдущих разделах, можно сформулировать следующие основные мероприятия:

- Разработка и утверждение нормативных правовых актов, необходимых для предоставления государственных услуг и исполнения государственных функций с помощью информационных и коммуникационных технологий;
- Планирование перевода государственных полномочий, функций, услуг в электронный вид;
- Создание юридически значимого и систематизированного учета государственных полномочий федеральных органов исполнительной власти;
- Проведение технологических и организационных мероприятий в части модернизации Единого портала государственных функций (государственных услуг) и официальных сайтов органов исполнительной власти.
- Определение типовой последовательности действий федерального органа исполнительной власти при переходе к исполнению полномочий в электронном виде.
- Создание государственного информационно-правового портала.

4. Перевод в электронный вид государственной учетной деятельности

Государственная учетная деятельность (государственный учет) — деятельность исполнительного органа государственной власти в рамках законодательно установленных полномочий по сбору, хранению, обработке и предоставлению гражданам, организациям, органам государственной власти, местного самоуправления сведений об объектах, субъектах, юридически значимых событиях и действиях. Аналогичным образом может быть определена муниципальная учетная деятельность (муниципальный учет).

Учетная деятельность лежит в основе реализации практически любого разрешительного или контрольно-надзорного полномочия, которое можно рассматривать как последовательность обращений к ряду государственных учетных систем с целью получения сведений о правах и обязанностях граждан (организаций) или иных сведений о них. Реализация полномочия завершается принятием решения о возможности или невозможности изменения прав или обязанностей гражданина (организации) с внесением соответствующей записи в определенную учетную систему.

Проблемы, связанные с ведением государственной учетной деятельности

В настоящее время государственная учетная деятельность не рассматривается как специфический объект регулирования, к которому могут быть выдвинуты единые требования. Отсутствует унифицированный и нормативно закрепленный состав требований к процедурам формирования, ведения, обработки и хранения юридически значимых событий и действий в ходе осуществления разрешительных и контрольно-надзорных полномочий. Не установлены единые принципы осуществления исполнительными органами государственной власти учетной деятельности, которые значительно облегчили бы ее перевод в электронный вид.

В настоящее время на федеральном и региональном уровнях можно обнаружить факты ведения учетной деятельности органами власти в отсутствие соответствующих законодательно установленных полномочий (например, ведение базы данных детей, уклоняющихся от посещения школы). Отдельные информационные системы, обеспечивающие ведение учетной деятельности в электронном виде, существуют вне нормативного пространства, статус данных в них является неопределенным, а порядок ведения учетной деятельности на их базе - произвольным.

Имеют место случаи незаконного обращения данных из учетных систем. Существование электронных учетных систем, сведения в которых носят исключительно справочный характер, не защищенных должным образом и не имеющих под собой должной нормативной правовой базы, приводит к утечкам данных за пределы органа власти. При

этом отсутствует возможность однозначного установления ответственных за это государственных служащих. Близкой к указанной проблеме является проблема взимания платы за сведения, предоставляемые из государственных учетных систем, при отсутствии правовых оснований.

Неопределенность правового статуса данных в государственных электронных учетных системах приводит к невозможности информационного обмена между ними. Юридической значимостью обладают только данные, представленные на бумажных носителях, поэтому обмен данными, представленными в электронном виде, может осуществляться только в справочных целях.

Направления деятельности по упорядочиванию государственного учета

Необходимо решить следующие задачи, связанные с совершенствованием нормативного и методического обеспечения государственной учетной деятельности в контексте подготовки к переходу предоставления государственных услуг и исполнению государственных функций в электронном виде:

- Рассматривая государственную (муниципальную) учетную деятельность как специфический объект регулирования, выработать единые принципы ведения государственной учетной деятельности.
- Выработать и закрепить нормативно требования к порядку ведения государственной (муниципальной) учетной деятельности.
- Легализовать ведение государственной (муниципальной) учетной деятельности в электронном виде, сформулировать и закрепить нормативно требования к государственным электронным учетным системам.
- Выдвинуть и закрепить нормативно требования, устанавливающие порядок взаимодействия учетных систем.
- Провести инвентаризацию государственных учетных систем и определить сроки и приоритеты реализации перечисленных выше требований применительно к конкретным государственным учетным полномочиям.

Единые принципы ведения государственной учетной деятельности

Упорядочение ведения государственной (и муниципальной) учетной деятельности и переход к ведению учетной деятельности в электронном виде потребует внесения изменений в федеральные законы и подзаконные нормативные правовые акты.

Ключевые принципы ведения государственной учетной деятельности необходимо зафиксировать на уровне федерального закона «О государственной и муниципальной учетной деятельности»:

Принцип законности ведения государственной (муниципальной) учетной деятельности

Нормативная правовая база реализации всякого учетного полномочия должна однозначно устанавливать:

- Объект учета и состав учетных данных.
- Организатора или организаторов учета.
- Операторов или порядок определения операторов учетной системы.
- Полномочия органов государственной власти или местного самоуправления, исполнение которых осуществляется с обращением к учетным данным.
- Права и обязанности, возникающие, изменяющиеся или прекращающиеся в связи с правоустанавливающими учетными событиями; права и обязанности, возникновение, изменение или прекращение которых должно быть отражено правоподтверждающими учетными событиями.

- Права и обязанности организатора учета и операторов в части сроков и условий внесения в учетную систему собранных (полученных) данных, оснований для отказа во внесении данных и запроса дополнительных данных.
- Права и обязанности организатора учета и операторов в части предоставления доступа к учетным данным; права и обязанности различных категорий лиц в части получения доступа к учетным данным. Порядок предоставления доступа к учетным данным.
- Порядок взимания платы за сведения, предоставляемые из государственной учетной системы, и за регистрационную запись в государственной учетной системе, а также порядок и объем взимаемой платы.

Принцип законности обращения учетных данных

Требования, которые обеспечат выполнение указанного принципа:

- При ведении учетной деятельности не допускается передача данных между учетными системами, обеспечивающими реализацию различных учетных полномочий, за исключением случаев, установленных федеральным законом, нормативным правовым актом Президента Российской Федерации или Правительства Российской Федерации, или прямого дозволения гражданина или организации, заинтересованных в такой передаче.
- Хранение данных, содержащихся в учетной системе, осуществляется не дольше, чем установлено в нормативных правовых актах, регламентирующих осуществление реализации конкретного учетного полномочия.
- Возможность отождествления объектов учетов, сведения о которых включены в различные учетные системы, может быть реализована только на основании требований федерального закона.

Принцип необходимости и достаточности состава учетных данных

Состав учетных данных должен включать все данные, необходимые для реализации полномочий органов государственной власти или органов местного самоуправления, осуществляемой с обращением к учетным данным. В составе учетных данных не должно быть данных, которые не являются необходимыми для реализации указанных полномочий.

Принцип обеспечения достоверности учетных данных

Организатор учетной деятельности обязан принять нормативные, организационные и технические меры, направленные на обеспечение достоверности учетных данных.

Средства обеспечения достоверности учетных данных должны, позволять определить:

- состояние учетных данных на конкретную дату;
- время внесения изменений в данные;
- лиц, принимавших решения о внесении изменений в данные, а также лиц, вносивших изменения в данные;
- лиц, получавших доступ к данным.

Принцип юридической значимости учетных данных в электронном виде

Данный принцип предполагает обеспеченную нормативно, организационно и технологически возможность непосредственного использования учетных данных в электронном виде для установления прав и обязанностей, юридических фактов или статусов без выполнения иных юридических действий по проверке или подтверждению данных, кроме проверки источника их получения.

Легализация ведения государственной (муниципальной) учетной деятельности в электронном виде

Для того чтобы легализовать ведение государственной и муниципальной деятельности в электронном виде, необходимо:

- Создать инфраструктуру обеспечения юридической значимости данных в электронном виде.
- Внести изменения в правовые акты, регулирующие реализацию учетных полномочий органами государственной власти и местного самоуправления.

Требования к государственным и муниципальным электронным учетным системам

Требования к государственным и муниципальным учетным системам, реализующие сформулированные выше принципы, должны быть установлены нормативными правовыми актами Правительства Российской Федерации, Президента Российской Федерации, субъектов Российской Федерации.

Кроме того, необходимо организовать учет государственных и муниципальных учетных систем, для чего создать регистр государственных и муниципальных учетных систем. Организация такого учета является необходимым условием для автоматизированного межведомственного взаимодействия, поскольку без идентификации учетных систем и их привязки к единому адресному и семантическому пространству невозможно регламентное обнаружение необходимых учетных данных и обращение к ним.

Приоритеты

Необходимо осуществить инвентаризацию государственных учётных систем, выделить ограниченный круг (10–15) наиболее востребованных для оптимизации межведомственного взаимодействия приоритетных учетных систем и запланировать приведение их в соответствие сформулированным принципам и требованиям. Данный перечень может включать: Единый государственный реестр юридических лиц; Единый государственный реестр налогоплательщиков; Единый государственный реестр индивидуальных предпринимателей; Единый государственный реестр прав на недвижимое имущество и сделок с ним; Государственный кадастр недвижимости и др.

5. Информационно-технологические и инженерные компоненты электронного правительства

Вводные положения

ИКТ-системы электронного правительства можно классифицировать следующим образом:

- Прикладные государственные ИС, эксплуатируемые федеральными органами исполнительной власти, органами государственной власти субъектов Российской Федерации и органами местного самоуправления в рамках своих полномочий.
- Информационно-технологическая инфраструктура электронного правительства.
- Инженерная (телекоммуникационная и аппаратная) инфраструктура.

В состав информационных систем электронного правительства входит программно-аппаратное, нормативно-методическое, правовое, кадровое, финансовое и другие виды обеспечения. На рис. 5.1 показана взаимная связь прикладных, инфраструктурных государственных и негосударственных ИС, инженерной инфраструктуры, ИС граждан и организаций.

Прикладные государственные информационные системы

Прикладные государственные ИС автоматизируют исполнение государственных функций и предоставление государственных услуг федеральными органами исполнительной власти, органами государственной власти субъектов Российской Федерации и органами местного самоуправления. Для целей формирования электронного правительства выделяются следующие типы прикладных информационных систем:

- Учетные системы: обеспечивают сбор, учет и предоставление правоустанавливающих и правоподтверждающих юридических фактов в отношении граждан, организаций и объектов (реестры).
- Информационно-правовые системы: используются для раскрытия информации, факт публикации которой в силу закона порождает правовые последствия.
- Информационно-справочные системы: используются для официальной публикации информации. Факт публикации информации в таких системах не порождает правовых последствий, однако является обязательным в силу закона.
- Аналитические системы: используются для хранения, обработки, предоставления и визуализации агрегированных и статистических данных с целью поддержки принятия управленческих решений.
- Обеспечивающие системы: используются для автоматизации типовой деятельности органов исполнительной власти, неспецифичной относительно полномочий конкретного ведомства (управление персоналом, электронный документооборот, учет обращений граждан и т. п.).

Информационно-технологическая инфраструктура электронного правительства

Распоряжением Правительства Российской Федерации от 2.08.2009 № 1231-р ОАО «Ростелеком» определен единственным исполнителем работ в рамках мероприятий ФЦП «Электронная Россия (2002-2010 гг.)» в части проектирования и создания инфраструктуры электронного правительства, а распоряжением Правительства Российской Федерации от 15.10.2009 № 1475-р ОАО «Ростелеком» определен единственным исполнителем работ по эксплуатации инфраструктуры электронного правительства - Единым национальным оператором инфраструктуры электронного правительства.

При этом иные правовые акты не определяют понятие «инфраструктура электронного правительства», не устанавливают ее состава, не содержат критериев отнесения к ней государственных ИС, не устанавливают полномочий и ответственности Единого национального оператора и не определяют операторов иных объектов инфраструктуры электронного правительства (связанных с обеспечением режима государственной тайны, а также не включенных в перечень мероприятий Распоряжения № 1231-р).

Для обеспечения регламентации процессов эксплуатации инфраструктуры электронного правительства необходима разработка постановления Правительства Российской Федерации, устанавливающего:

- положение о едином национальном операторе инфраструктуры электронного правительства, определение его полномочий и сферы ответственности;
- порядок эксплуатации инфраструктуры электронного правительства;
- порядок отнесения ИС к инфраструктурным;
- требования к государственным инфраструктурным ИС;
- порядок разработки и введения в эксплуатацию государственных инфраструктурных ИС.

Определение информационно-технологической инфраструктуры электронного правительства

Под информационно-технологической инфраструктурой электронного правительства понимается совокупность государственных ИС, целевым назначением которых является обеспечение автоматизированного взаимодействия:

- государственных ИС, участвующих в исполнении государственных функций или предоставлении государственных услуг;
- государственных ИС с ИС, используемыми гражданами и организациями для доступа к сервисам электронного правительства.

Для решения отдельных инфраструктурных задач, связанных с формированием электронного правительства, привлекаются также негосударственные организации и эксплуатируемые ими ИС (поисковые системы сети Интернет, провайдеры телекоммуникационных услуг, нотариальные конторы и др.).

Критерии выявления инфраструктурных функций

Для придания регламентированного характера процедуре отнесения ИС к инфраструктурным должны быть закреплены нормативно следующие принципы:

1. К инфраструктурным системам электронного правительства относятся ИС, без создания и эксплуатации которых обеспечение взаимодействия ИС электронного правительства невозможно. Эти системы выполняют следующие функции:
 - Обеспечение надежного, достоверного, юридически значимого информационного взаимодействия в электронной форме, в том числе идентификации участников взаимодействия.
 - Регистрация и обнаружение участников взаимодействия, информационных объектов, данных. Функции реализуются с помощью электронных каталогов, реестров, поисковых систем.
2. К инфраструктурным системам электронного правительства могут относиться ИС, без создания и эксплуатации которых обеспечение взаимодействия информационных систем электронного правительства возможно, однако экономически неэффективно. К функциям, выполняемым такими системами, относятся:
 - Интеграционные функции и функции преобразования (шлюзования) данных, обеспечивающие передачу информации между специфическими сегментами телекоммуникационных сетей и прикладными информационными системами.
 - Вспомогательные функции, необходимые для обеспечения современного технологического уровня, удобства и комфорта использования ИС.
3. Поддерживаемая инфраструктурной системой функция должна выполняться единообразно при решении однотипных задач, связанных с взаимодействием ИС.
4. Выполнение любой инфраструктурной функции должно быть установлено правовым актом.

Инженерная инфраструктура

Инженерная инфраструктура выполняет хорошо стандартизованные инфокоммуникационные функции: организация и предоставление каналов связи, предоставление доступа к сети Интернет, поддержка центров обработки данных, формирование открытых и защищенных контуров компьютерных сетей, поддержка функционирования общесистемного программного обеспечения, обеспечение информационной безопасности и т. п.

Требования к прикладным государственным информационным системам

Действующее законодательство фрагментарно регулирует порядок создания прикладных государственных ИС. Выдвижение единой системы требований к ним необходимо для:

- Упорядочивания (легализацией) деятельности, связанной с электронной формой ведения государственных информационных систем.
- Обеспечения взаимной совместимости государственных информационных систем.
- Обеспечения обнаружения, в том числе автоматизированного, сервисов государственных ИС, участвующих в информационном обмене.
- Обеспечения эффективности бюджетных расходов на ИКТ.

Для достижения указанных целей необходимо:

- Установить в нормативных правовых актах Правительства Российской Федерации и соответствующих нормативно-правовых актах субъектов Российской Федерации и муниципальных образований правила создания государственных ИС, включающие требования к стадиям их жизненного цикла, в том числе порядок планирования и бюджетирования; порядок осуществления закупок и введения в эксплуатацию; ответственность за действия, совершаемые автоматически или автоматизировано без участия государственных служащих, и их последствия; порядок вывода ИС из эксплуатации.
- Создать реестр государственных ИС, в том числе установить порядок его ведения и состав учитываемых в нем объектов.
- Определить очередность приведения ИС органов государственной власти к вновь вводимым требованиям, утвердить соответствующий план.

Требования к инфраструктурным информационным системам электронного правительства

Требования, предъявляемые к инфраструктурным ИС электронного правительства, подлежат правовому закреплению Правительством Российской Федерации:

Общность использования. Реализация инфраструктурной ИС должна обеспечивать взаимодействие неопределенного круга ИС, в том числе неизвестных заранее (ее реализация не должна зависеть от ИС, взаимодействие которых она обеспечивает).

Использование открытых стандартов. Инфраструктурная ИС должна обеспечивать доступ к предоставляемым ею сервисам посредством единообразных интерфейсов, отвечающих критериям открытых стандартов.

Технологическая нейтральность. Инфраструктурная ИС не должна требовать от прикладных и иных инфраструктурных ИС использования какой-либо конкретной технологии, программного обеспечения или аппаратной платформы.

Стабильность. Неизменность основных характеристик, форматов, регламентов функционирования инфраструктурной ИС должна обеспечиваться в течение продолжительного времени.

Преемственность. В случае модернизации ИС должна быть обеспечена продолжительная поддержка функционирования замещаемых протоколов, форматов, спецификаций, предоставление сервисов по замещаемым регламентам.

Повсеместная доступность. Инфраструктурная ИС должна обеспечивать доступность своих сервисов на всей территории Российской Федерации и — в случаях, установленных законодательством, — за ее пределами.

Постоянная работоспособность. Инфраструктурная ИС должна обеспечивать доступность своих сервисов круглосуточно без перерывов и отказов в обслуживании.

Нагрузочная способность и способность к масштабированию. Инфраструктурная ИС должна обладать достаточным запасом по пропускной способности и вычислительной нагрузке, в том числе в условиях прогнозируемых пиковых нагрузок.

Типовые решения

Одним из способов автоматизации функций, единообразно выполняемых федеральными и региональными органами власти, органами местного самоуправления, является создание новых или доработка существующих решений до уровня типовых программных решений (типовых ИС). Содержание плана по формированию и внедрению типовых решений, а также других компонентов инфраструктуры электронного правительства представлено на рисунке 5.2.

ИС должны удовлетворять ряду требований, являющихся условием их эффективного использования:

- **Общность функциональности и использования:** автоматизируемая с помощью типовой ИС деятельность, требования к ней и к квалификации персонала должны быть формализуемыми и типизированными.
- **Открытость:** типовая ИС должна использовать интерфейсы, отвечающие критериям открытых стандартов, обеспечивать «прозрачное» межведомственное и межуровневое взаимодействие, быть исчерпывающе документирована и снабжена справочными руководствами.
- **Стабильность функционирования и наличие технической поддержки:** массовое внедрение типового решения должно предваряться пилотными проектами, подтверждающими качество типовой ИС и возможность стабильной поддержки.
- **Тиражируемость:** в типовых решениях преимущественно должно использоваться свободно лицензируемое ПО, обеспечивающее органам власти и их поставщиками права на свободное тиражирование и модификацию. Отступление от данного принципа подлежит обоснованию в каждом таком случае.

Для каждой типовой ИС должен быть определен орган исполнительной власти - функциональный заказчик работ по разработке, развитию и поддержке типовой ИС. Функциональный заказчик определяется, исходя из отраслевой и функциональной направленности типовой ИС. Функциональный заказчик:

- Определяет потребность в создании типовой ИС, проводя переговоры с заинтересованными органами власти на всех уровнях.
- Определяет прогнозный объем тиражирования типовой ИС, подкрепляя его соглашениями с заинтересованными органами власти о совместной разработке и последующей эксплуатации типовой ИС.
- Исходя из объема тиражирования, вырабатывает требования к типовой ИС и согласует их с заинтересованными в создании типового решения заказчиками.
- Формирует смету проекта, учитывающую весь жизненный цикл существования типовой ИС, определяет совместно с заинтересованными заказчиками порядок и источники финансирования типовой ИС.
- Определяет правила подтверждения соответствия типовой ИС требованиям (правила сертификации и включения в реестр типовых ИС).

Общие требования, предъявляемые к типовым ИС, раскрывающие приведенные выше принципы, регламенты принятия решения о разработке типовых ИС, порядок их разработки и эксплуатации, выбор пилотных зон утверждаются уполномоченным федеральным органом исполнительной власти (Минкомсвязи России) совместно с заинтересованными органами власти. Уполномоченный орган также ведет реестр типовых ИС, определяет принципы признания в качестве типовой ИС ранее разработанных систем,

в том числе коммерческих разработок, в случае если они удовлетворяют действующим требованиям. Межведомственной рабочей группой по вопросам сокращения различий между субъектами Российской Федерации по уровню информационного развития совместно с Минкомсвязи России и регионами в рамках проекта «Электронный регион» разработана оптимальная карта информации. Ведется отбор и анализ программно-технических решений регионов в целях признания их типовыми. Уполномоченный орган осуществляет предварительную инвентаризацию потребностей федеральных и региональных органов власти, органов местного самоуправления в типовых ИС и предлагает ведомствам (регионам, муниципалитетам) выступить в качестве функционального заказчика типовой ИС.

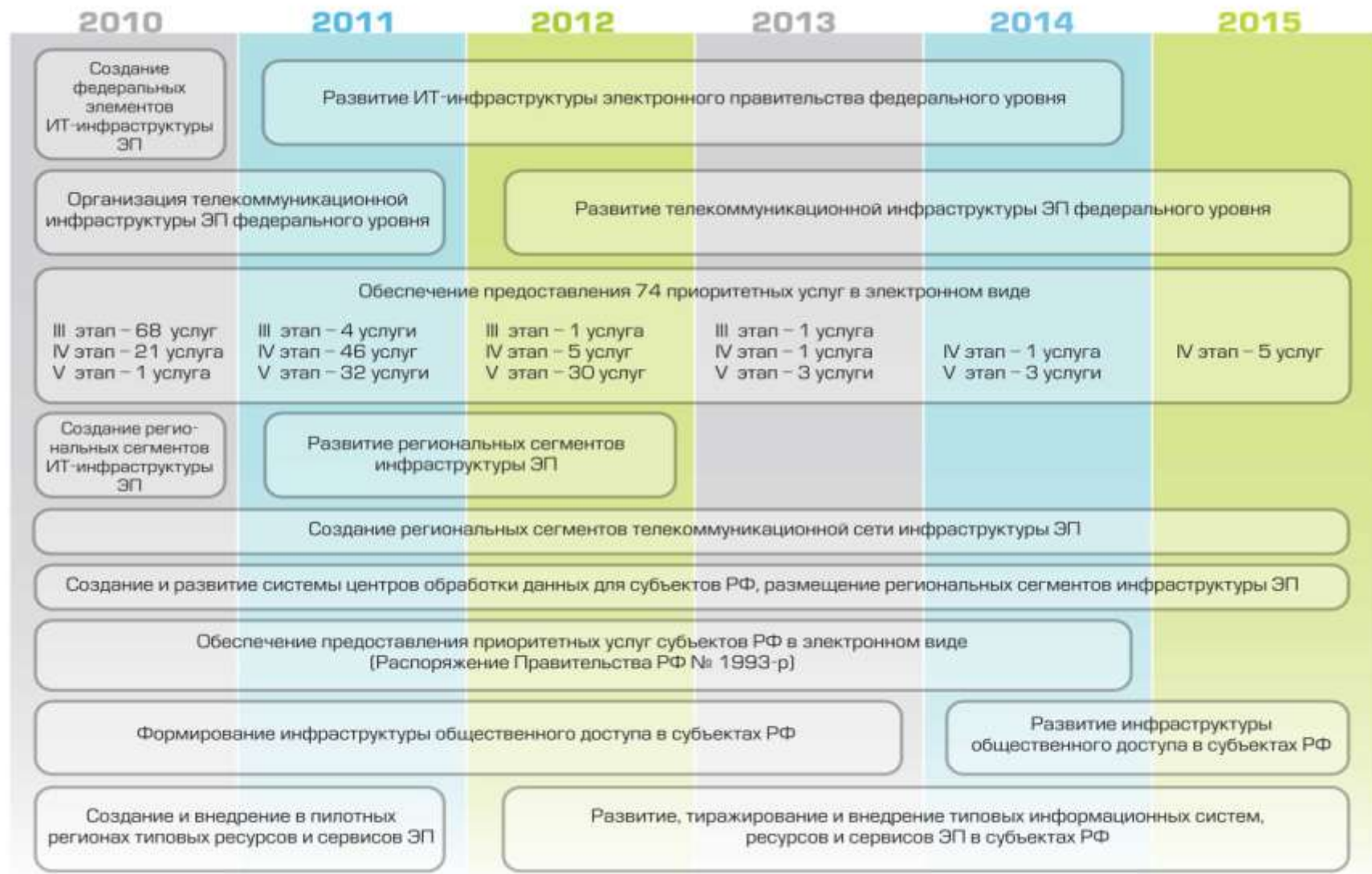


Рисунок. 5.2. План формирования отдельных компонентов инфраструктуры.

6. Решение первоочередных проблем и формирование ключевых инфраструктур электронного правительства

Существенным фактором, оказывающим значительное влияние на положение дел в информационной области вообще, и в сфере защиты информации, в частности, является то, что до начала 90-х годов нормативное регулирование в данной области оставляло желать лучшего. Некоторые ключевые для электронного правительства вопросы в данной области не решены до сих пор.

Из изложенного в предыдущих разделах ясно, что в основе деятельности электронного правительства лежит электронное взаимодействие государственных организаций и органов власти всех уровней как между собой, так и иными физическими и юридическими лицами. Кроме того, в различного рода электронных реестрах и базах данных накапливается, обрабатывается, систематизируется разного рода информация, принадлежащая как собственно государству, так и отдельным органам власти, муниципальным образованиям, государственным и муниципальным учреждениями, ведомствами, государственными организациями, так и частным лицами. В подобных условиях, принципиальное значение при разрешении коллизий и конфликтных ситуаций, возникающих вследствие, в связи или в процессе реализации функций электронного правительства между государственными организациями и иными физическими и юридическими лицами, а также между последними, приобретает правильное категорирование сведений, хранимых, обрабатываемых и передаваемых между всеми участниками электронных взаимодействий.

С учетом того, что рассмотрение взаимодействий, связанных с обработкой, хранением и передачей по каналам связи информации, содержащей сведения, составляющие государственную тайну, выходит за рамки настоящей работы, при реализации функций электронного правительства можно выделить следующие основные категории информации:

1. Сведения, составляющие служебную тайну государственных организаций и органов государственной власти.
2. Сведения, составляющие коммерческую тайну отдельных физических и юридических лиц.
3. Сведения, составляющие профессиональную или иную охраняемую законом тайну,
4. Персональные данные отдельных граждан.
5. Открытые неконфиденциальные сведения, подмена, искажение или уничтожение которых может нанести ущерб интересам отдельных лиц, организаций, обществу и государству в целом.

Существующие в настоящее время нормативные акты законодательного уровня регулируют в той или иной степени оборот в информационных системах сведений, относящихся ко 2-ой, 3-ей и 4-ой категориям, полностью оставляя открытым вопросы оборота и защиты сведений, которые отнесены данной классификацией к пп. 1 и 5.

Вместе с тем, оборот в ИС государственных органов сведений I категории поднимает вопросы как по обеспечению конфиденциальности сведений, отнесенных к I категории, так и по обеспечению их аутентичности, целостности и доступности для легальных пользователей. Что касается защиты информации, то до настоящего времени порядок защиты подобных сведений не определен. Согласно Руководящим документам ФСТЭК России до принятия закона, определяющего порядок обращения с подобной информацией в государственных органах и организациях России, защиты этих сведений должна осуществляться тем же порядком, что и информации, составляющей государственную

тайну с грифом «секретно», что практически исключает возможность обработки, хранения и передачи подобного рода сведений или иных данных, связанных с ними в открытых или общедоступных ИС. Однако, единственный действующий в настоящее время нормативный акт, определяющий порядок оборота служебной несекретной информации в государственных организациях,² относит к служебной тайне любую информацию, которая касается деятельности организаций, и ограничения на распространения которой диктуются служебной необходимостью. Поэтому без законодательного закрепления статуса информации, содержащей сведения, составляющие служебную тайну государственных организаций, а также нормативов защиты подобной информации, исполнение основных функций электронного правительства, описанных в предыдущих разделах, будет в значительной мере либо затруднено, либо практически невозможно.

В качестве источников угроз могут выступать как субъекты (личность), так и объективные проявления. Источники угроз могут находиться как внутри объекта информатизации – внутренние, так и вне его – внешние. Все источники угроз делятся на классы, обусловленные типом носителя угрозы (источника угрозы).

- обусловленные действиями субъекта (Антропогенные источники угроз).
- обусловленные техническими средствами (Техногенные источники угроз).
- обусловленные природными явлениями (Стихийные источники угроз).

К классу антропогенных источников угроз относятся субъекты, действия которых могут быть квалифицированы как умышленные или случайные преступления.

К классу техногенных источников угроз относятся источники, определяемые технократической деятельностью человека и развитием цивилизации.

К классу стихийных источников угроз относятся стихийные бедствия или иные обстоятельства, которые невозможно предусмотреть или возможно предусмотреть, но невозможно предотвратить при современном уровне человеческого знания и возможностей³.

Основными угрозами электронного документооборота (взаимодействия отправителя и получателя электронного документа) являются:

- нарушение конфиденциальности электронного документа;
- нарушение целостности электронного документа;
- нарушение неотказуемости электронного документа;
- нарушение адекватности отображения электронного документа;
- нарушение доступности электронного документа.

Существующие нормативные правовые акты регулируют, в основном, вопросы нарушения конфиденциальности электронной информации. Федеральный закон «Об информации, информационных технологиях и о защите информации» устанавливает, что защита информации может быть направлена на обеспечение защиты от неправомерного доступа, уничтожения, модифицирования и блокирования доступа к информации. Однако никаких подзаконных нормативных актов, регламентирующих технические нормативы обеспечения целостности, аутентичности и адекватности отображения электронных документов не разработано. Таким образом, до сих пор остаются законодательно и нормативно неурегулированными вопросы защиты несекретной информации, аутентичность, целостность или доступность которой является важной с точки зрения интересов личности, общества и государства. Вместе с тем, анализ законодательства ведущих развитых государств показывает, что уполномоченные государственные органы довольно жестко регулируют информационную сферу, особенно там, где речь идет об информационной безопасности. В частности, законодательством США установлен

² Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти»

³ Румянцев О. Г., Додонов В.Н., Юридический энциклопедический словарь, М., 1997 г., изд. «ИНФРА-М»

приоритет национальных интересов при решении вопросов безопасности информации (в том числе и частной). Законодательные акты, например, декларируют, что требования государственных органов по обеспечению необходимого уровня защиты информации могут быть распространены на любую информацию, несанкционированное изменение режима доступа к которой, уничтожение или изменение, содержащихся в ней данных и несанкционированный доступ к этим сведениям может привести к нежелательным последствиям для национальных интересов. При этом требования государственных органов по обеспечению необходимого уровня защиты информации распространяются на любую «важную информацию, потеря которой или ее неправильное использование, несанкционированное изменение и т.д., может привести к нежелательным воздействиям на национальные интересы». Очевидно, что без законодательного закрепления аналогичных нормативов в России вопрос нормального функционирования электронного правительства не может быть решен в полной мере.

Работа любого учреждения или предприятия не возможна без организации не только обмена документами в электронной и/или традиционной форме, но и организации так называемого «документооборота». Очевидно, что само понятие «документооборот» имеет более широкий смысл, чем понятие обмен документированной информацией. Собственно под документооборотом обычно подразумевается процесс, описывающий весь жизненный цикл документа, начиная с момента его создания до момента его уничтожения или сдачи в архив на вечное хранение. Если процессы создания, обработки, обмена и временного хранения документов в электронной форме в той или иной форме регламентируются действующими нормативными актами, то вопросы архивного хранения документированной информации регулируются законодательством об архивном деле в Российской Федерации, которое ориентировано в настоящее время исключительно на учет и хранение документов в бумажной форме. Без внесения соответствующих изменений в данные нормативные акты полноценное функционирование электронного правительства также невозможно.

Кроме того, в краткосрочной перспективе (2010–2012 гг.) в приоритетном порядке, должны быть созданы юридические и технические предпосылки формирования следующих ключевых инфраструктур:

1. Инфраструктура обеспечения юридической значимости электронного взаимодействия. К основным составляющим инфраструктуры относятся единая сеть удостоверяющих центров (заверение цифровой подписи), служба третьей доверенной стороны (заверение времени и иных значимых фактов, связанных с волеизъявлением), а также механизмы идентификации, авторизации и аутентификации участников взаимодействия. Необходимость первоочередного формирования данной инфраструктуры обусловлена невозможностью в ее отсутствие предоставления государственных услуг в электронном виде и осуществления без участия заявителей сбора документов, необходимых для получения услуги и выдаваемых третьими лицами (подведомственными организациями, иными органами исполнительной власти и др.).
2. Инфраструктура обеспечения совместимости государственных ИС. К основным составляющим этой инфраструктуры относятся единые реестры нормативного и справочного характера, необходимые для обеспечения способности ИС к автоматизированному взаимодействию и доступа к ним граждан и организаций. Приоритетность инфраструктуры обусловлена тем, что унаследованные системы разрабатывались без учета возможности их совместной работы.
3. Инженерная и информационно-технологическая инфраструктуры. Технологическое обеспечение предоставления государственных услуг в электронном виде, функционирование инфраструктурных компонентов электронного правительства осуществляется с помощью федерального и региональных сегментов инфраструктуры (см.

рисунок 6.1). В состав федерального сегмента входят такие инфраструктурные ИС, как Единый портал государственных и муниципальных услуг (функций), Сводный и федеральный реестры государственных услуг, система идентификации и аутентификации пользователей, корневой (головной) УЦ, резервные программно-аппаратные мощности, центральные узлы Системы межведомственного электронного взаимодействия (далее – СМЭВ) и информационно-платежного шлюза, реестры технологических стандартов и нормативно-справочных данных, реестр ИС электронного правительства, подсистемы обеспечения информационной безопасности, контроля и мониторинга работоспособности элементов инфраструктуры электронного правительства и предоставляемых с ее помощью сервисов и др. Помимо инфраструктурных ИС федеральный и региональные сегменты инфраструктуры могут обеспечивать функционирование прикладных учетных, информационно-справочных и информационно-правовых ИС.

Типовой региональный сегмент инфраструктуры обеспечивает функционирование региональных сегментов перечисленных выше федеральных ИС (системы идентификации и аутентификации, УЦ, информационно-платежных шлюзов, СМЭВ, систем автоматизации регламентов оказания госуслуг в электронном виде и др.), региональных и муниципальных порталов и реестров государственных услуг, иных прикладных ИС, систем обеспечения информационной безопасности, систем контроля и мониторинга работоспособности элементов инфраструктуры и предоставляемых на ее базе сервисов. На базе региональных сегментов инфраструктуры органам государственной власти субъектов Российской Федерации, органам местного самоуправления предоставляются сервисы (услуги) по обеспечению технологических процессов предоставления в электронном виде государственных и муниципальных услуг (например, услуги по интеграции ИС или хостинг-услуги). Типовые региональные сегменты инфраструктуры могут размещаться в центрах обработки данных Единого национального оператора инфраструктуры электронного правительства в субъектах Российской Федерации.

При описании состава базовых функциональных элементов инфраструктуры электронного правительства необходимо отметить особое функциональное назначение Системы межведомственного электронного взаимодействия.

СМЭВ представляет собой центральный интеграционный элемент инфраструктуры электронного правительства, иерархическую, территориально-распределенную информационную систему, реализующую инфокоммуникационную среду обеспечения не только процессов оказания госуслуг в электронном виде, но и решения задач информационного обмена непосредственно в интересах ведомств.

Межведомственное электронное взаимодействие осуществляется через территориально распределенную телекоммуникационную инфраструктуру электронного правительства путем использования потребителями электронных сервисов, предоставляемых единой информационной системой межведомственного электронного взаимодействия. При этом межведомственное информационное взаимодействие органов государственной власти с Администрацией Президента Российской Федерации, Аппаратом Правительства Российской Федерации, Администрацией Президента Российской Федерации, палатами Федерального собрания Российской Федерации осуществляется на базе информационно-телекоммуникационной сети специальной связи и информации Федеральной службы охраны Российской Федерации.

Для обеспечения возможности обмена в автоматизированном режиме электронными почтовыми сообщениями между Администрацией Президента Российской Федерации, Аппаратом Правительства Российской Федерации, федеральными органами исполнительной власти и иными федеральными органами государственной власти используется система межведомственного электронного документооборота (система МЭДО). Система МЭДО не является элементом СМЭВ. Оператор системы МЭДО определяется отдельным нормативным правовым актом Российской Федерации.

Система межведомственного электронного взаимодействия создается с целью решения следующих задач:

- Использование единых правил (стандартов, интерфейсов) для обеспечения взаимодействия между системами (стандартизация и унификация).
- Обеспечение возможности независимого развития информационных ресурсов без необходимости переделки всех связанных с ним систем.
- Обеспечение однократного подключения ресурса к системе взаимодействия и последующего многократного использования ресурса в деловых процессах.
- Повышение степени контролируемости процесса взаимодействия за счет централизации администрирования и мониторинга.
- Централизация хранения описаний ресурсов для ускорения разработки информационных систем, взаимодействующих с ресурсами.

Таким образом, на концептуальном уровне, СМЭВ, выступая в роли интеграционной шины и/или интеграционного брокера, не отвергает концепции автоматизации деловых процессов (для государственных органов, работающих преимущественно с документом – создания систем документооборота), а является дополнительной к ней. Система электронного документооборота реализует сквозной процесс предоставления государственной услуги, система межведомственного электронного взаимодействия обеспечивает участие в этом процессе ранее несвязанных ресурсов, предоставляя транспортную и логическую среду для обмена стандартизованными сообщениями между системой документооборота (системой исполнения деловых процессов) и внешними информационными ресурсами. При этом за счет выбора в качестве транспорта системы обмена сообщениями, базирующейся на открытых стандартах, к СМЭВ могут быть подключены как вновь создаваемые информационные системы, так и существующие информационные системы, созданные на различных программно-аппаратных платформах.

Использование СМЭВ в качестве единственного средства предоставления информационных ресурсов для системы исполнения бизнес-процессов позволяет обеспечить независимость информационных ресурсов органов государственной власти и систему исполнения деловых процессов. При этом оба этих элемента (система документооборота и информационные ресурсы) могут изменяться независимо. Модификации при этом будут подвергаться только отдельные элементы СМЭВ – адаптеры к информационным ресурсам.

Наличие централизованно поддерживаемых адаптеров к информационным ресурсам позволяет не разрабатывать заново программный код, обеспечивающий доступность информационных ресурсов, а использовать комбинацию уже имеющихся возможностей – формировать комплексные сервисы, позволяя увеличить скорость формирования новых деловых процессов.

Необходимо отметить, что при реализации задач межведомственного документооборота в рамках оказания госуслуг так или иначе необходимо решать задачи взаимодействия с различными информационными ресурсами. Решение этой задачи потребует реализовать функции взаимодействия, обнаружения ресурсов, поддержания списка доступных ресурсов, разработку стандартов взаимодействия и т.п., что, в конечном итоге, приведёт либо к созданию отдельной подсистемы межведомственного взаимодействия либо к взаимодействию систем по принципу «точка-точка». Последний вариант приводит к неконтролируемому росту затрат на внедрение новых регламентов оказания госуслуг и огромной избыточности реализуемых функций.

СМЭВ необходима для:

- технологического обеспечения эффективного межведомственного информационного взаимодействия за счет повышения надежности, скорости и безопасности межведомственного информационного взаимодействия;

- обеспечения регламентированного доступа граждан и представителей организаций к государственным, муниципальным и иным информационным системам, а также автоматизации обмена данными между отдельными государственными, муниципальными и иными информационными системами.

Функционирование электронных сервисов СМЭВ обеспечивается за счет: использования электронных служб, предоставляемых Поставщиками; реализации логической последовательности вызовов электронных служб Поставщиков на технологических средствах СМЭВ с целью получения результата исполнения электронного сервиса.

Доступ потребителей к электронным сервисам СМЭВ должен осуществляться:

- с использованием механизмов аутентификации Участников, в том числе с использованием электронной цифровой подписи;

- с помощью обмена потребителями информации и СМЭВ, поставщиков информации и СМЭВ электронными сообщениями установленного формата и структуры.

Принципами, на основе которых должна создаваться СМЭВ, являются:

- обеспечение технологической возможности информационного взаимодействия существующих и вновь создаваемых государственных информационных систем, муниципальных информационных систем и иных информационных систем, предназначенных для выполнения государственных задач (далее - информационные системы);

- обеспечение технологической независимости структуры СМЭВ и регламента ее работы от проводимых технических, административных, организационных и иных изменений в информационных системах, подключенных к СМЭВ;

- применение единых технологий, форматов, протоколов межведомственного информационного взаимодействия, унифицированных программно-технических средств; правомерное использование программного обеспечения, использование сертифицированных программно-технических средств и средств связи;

- обеспечение защиты информации путем принятия организационных и технических мер, направленных на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

- минимизация финансовых и временных издержек при передаче и получении информации;

- однократный ввод и многократное использование информации в информационных системах, подключенных к СМЭВ;

- обеспечение функционирования в реальном режиме времени; соблюдение прав граждан при автоматизированной обработке информации, содержащей персональные данные.

Достоверность предоставляемой информации обеспечивается каждым из поставщиков информации в рамках его зоны ответственности. При этом инфраструктура электронного правительства должна обеспечивать прием запросов, безошибочную маршрутизацию и неискаженную передачу информации между потребителями и участниками.

СМЭВ должна предусматривать возможность осуществления мониторинга межведомственного информационного взаимодействия со стороны уполномоченных государственных органов.

Инфраструктура электронного правительства

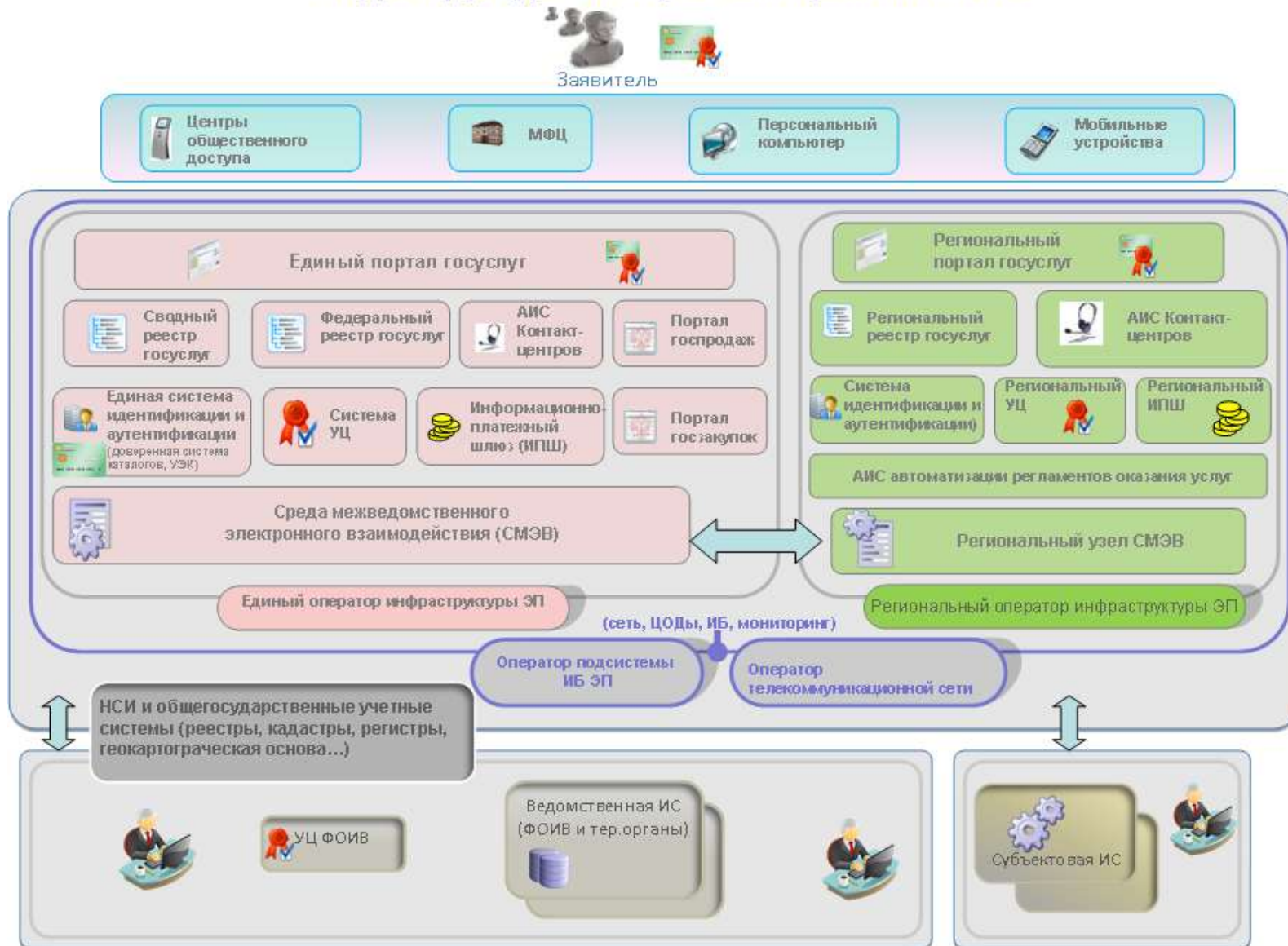


Рисунок. 6.1. Ключевые компоненты инфраструктуры электронного правительства в составе федерального и регионального сегментов.

Инфраструктура обеспечения юридической значимости электронного взаимодействия

Для обеспечения электронного взаимодействия органов власти, граждан и организаций требуется создание общественных институтов, эквивалентных используемым в традиционном очно-бумажном взаимодействии.

Юридическая значимость электронного документа

Несмотря на функциональную тождественность бумажных и электронных документов (информация на материальных носителях, зафиксированная и оформленная в установленном порядке), существуют принципиальные различия в способах обеспечения их аутентичности, адресности и неотказуемости, обусловленные техническими и культурными причинами.

Это определяет необходимость законодательного определения правового статуса электронных документов, в том числе:

- Необходимо установить правовые критерии признания электронного документа юридически значимым (см. ниже). Не следует устанавливать общих требований к методам обеспечения юридической значимости электронных документов. Необходимым условием признания юридической значимости электронного документа в общем случае не может являться использование цифровой подписи, наличие сертификата ключа подписи определенного вида, определенный тип используемых программно-аппаратных устройств, использование сертифицированных средств и т. п.
- Необходимо предусмотреть ответственность за умышленное уничтожение электронных документов или их реквизитов, обеспечивающих качество юридической значимости электронного документа.
- Необходимо определить и стандартизировать основные типы файлов, используемых для обработки, хранения и передачи документированной электронной информации в целях обеспечения их адекватного отображения у всех участников электронного документооборота и взаимного обмена документированной информацией в рамках деятельности электронного правительства. Данный перечень должен носить открытый характер. Законодательно должны быть предусмотрены меры, направленные на обеспечение доступности к информации в случае исключения каких-либо файловых типов из данного перечня.
- Необходимо разработать и закрепить законодательно порядок осуществления третьей независимой стороной процедур перевода документов из традиционной бумажной формы в электронную и наоборот, в том числе, и в случаях, когда документ изначально был создан и существовал до момента перевода исключительно в электронной форме.

Качество юридической значимости в рамках очно-бумажного документооборота реализуется через систему реквизитов (неотъемлемых составляющих документа), обеспечивающих фиксацию и сохранность юридических фактов, сведения о которых зафиксированы в документах, а также возможности их использования в качестве доказательств. Реквизиты, независимо от того, какими техническими, правовыми и организационными средствами они реализуются, обеспечивают следующие необходимые составляющие правового содержания документов и данных:

1. Подтверждение волеизъявления субъекта правоотношений как правило, реализуется собственноручной подписью или цифровой подписью (далее — ЦП) как ее аналогом. Помимо собственноручной подписи или ее аналога допустимо использование иных законных способов, позволяющих надежно установить факт волеизъявления.
2. Фиксация правомочности субъекта права. В общем случае качеством правомочности обладают все граждане Российской Федерации, однако правомочность субъекта права может иметь ограничения (заключенные, недееспособные, не достигшие определенного возраста и др.). В приложениях электронного правительства в кратко- и среднесрочной перспективе необходимо опираться на современную практику, когда централизованного учета правомочий не осуществляется.
3. Фиксация полномочий должностных лиц. Необходимо вести электронные реестры уполномоченных лиц, которым выдан сертификат ключа цифровой подписи, а также обеспечивать своевременный отзыв сертификатов.
4. Фиксация правового статуса органов власти — в бумажных документах реализуется, например, в форме углового штампа с гербом Российской Федерации, указанием контактных данных, проставлением штампа или гербовой печати ведомства. В электронной форме адекватным аналогом является ведение электронных реестров органов государственного и муниципального управления.
5. Подтверждение места и времени издания документа. Для поддержания данного реквизита необходимо наличие выделенного субъекта — доверенной третьей стороны.

Целевое состояние инфраструктуры обеспечения юридической значимости электронного взаимодействия

Для обеспечения всех атрибутов юридической значимости зафиксированного в установленном порядке юридического факта (электронного документа или записи в электронной базе данных), для целей взаимодействия неопределенного круга лиц необходимы следующие взаимодополняющие структуры:

1. Единая общенациональная инфраструктура удостоверения открытых ключей цифровой подписи (инфраструктура цифрового доверия), обеспечивающая идентификацию субъектов информационного взаимодействия и целостность содержания сообщений.
2. Инфраструктура доверенной третьей стороны, предназначенная для удостоверения доверенного времени, а также иных существенных для юридической значимости документа фактов, а также апостильного и нотариального заверения. Как правило, реализуется на основе инфраструктуры цифрового доверия.
3. Электронные учетные системы участников информационного взаимодействия (органов и организаций, уполномоченных лиц органов и организаций, физических и юридических лиц), обеспечивающие подтверждение их правового статуса, правомочий, полномочий, права подписи и др. В электронном правительстве реализуются, как правило, на ведомственном уровне.

Инфраструктура цифрового доверия

Инфраструктура цифрового доверия (далее — ИЦД) включает в себя удостоверяющие центры, входящие в единый домен цифрового доверия, и обеспечивает единое пространство использования и признания цифровой подписи. Вместе с тем, в настоящее время в России отсутствует единое национальное пространство доверия. Существующие корпоративные, ведомственные и региональные системы не обладают признаками инфраструктурности за пределами собственного сегмента, как правило, соответствующего

корпорации, отрасли, ведомства или региона. Возможная реализация инфраструктуры цифрового доверия приведена на рис. 6.2.

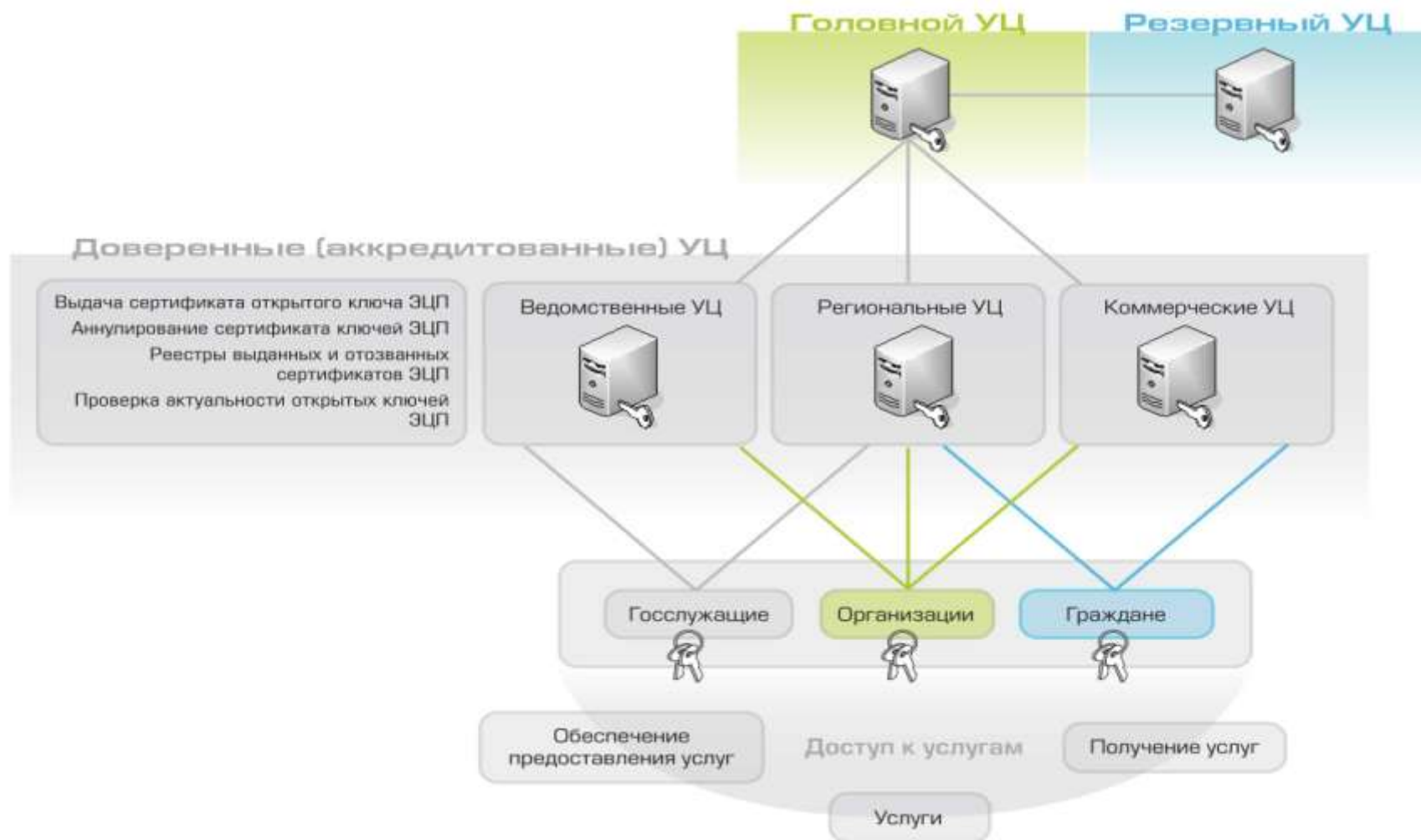


Рисунок 6.2. Вариант реализации инфраструктуры цифрового доверия в рамках проекта «Электронное правительство»

Существуют три основные модели построения инфраструктуры открытых ключей:

- Иерархическая,
- Браузерная,
- Сетевая.

Сравнительные характеристики различных моделей организации инфраструктуры открытых ключей.

	<i>Иерархическая</i>	<i>Браузерная</i>	<i>Сетевая</i>
Описание	<p>Характеризуется прямой иерархией доверительных отношений, регистрируемых на уровне единого (федерального, регионального, корпоративного и т.п.) корневого УЦ, который выпускает сертификаты УЦ уровнем ниже. Они в свою очередь выпускают сертификаты УЦ следующего уровня и т.д. до сертификатов конечных пользователей. Все образующие домен сертификаты в данной модели связаны в строгом иерархическом порядке и образуют древовидную структуру.</p>	<p>Пользователь входит сразу в несколько иерархических доменов РКІ, для чего используются т.н. «списки доверенных удостоверяющих центров», публикуемые той или иной организацией для облегчения проверки сертификатов пользователей из других доменов. В данных списках представляются те УЦ, которым можно доверять при определенных условиях (нередко разные типы взаимодействия подразумевают использование услуг разных УЦ).</p>	<p>Каждый из УЦ является независимым. Для установления доверия между центрами, каждая пара центров формирует кросс-сертификат, содержащий два объекта: сертификат открытого ключа первого УЦ, подписанный вторым УЦ, и сертификат второго УЦ, подписанный первым УЦ. В результате взаимной сертификации формируется сетевая топология доверия, основанная на связи двух УЦ. В сетевой схеме для взаимной проверки сертификатов двух пользователей может возникнуть несколько путей.</p>

<p>Достоинства</p>	<ol style="list-style-type: none"> 1. Существенно упрощает вопросы по обеспечению взаимодействия пересылаемых информационных блоков ЭЦП и сертификатов внутри домена. Проверка подлинности приходящего сертификата происходит по ясно выстроенной иерархической «цепочке доверия» – пути следования сертификата. 2. Аналогична существующим управляющим структурам. 3. Может быть легко наложена на иерархическое дерево имен. 4. Определяет простой алгоритм поиска, построения и верификации цепочек сертификатов для всех взаимодействующих сторон. 	<p>Ввиду удобства использования получила широкое распространение среди пользователей сети Интернет.</p>	<ol style="list-style-type: none"> 1. Более гибкая, чем иерархическая. 2. Конечный пользователь должен доверять, только центру, издавшему его сертификат. 3. Возможна непосредственная кросс-сертификация различных УЦ, пользователи которых часто взаимодействуют между собой, что сокращает процесс верификации цепочек.
--------------------	--	---	---

Недостатки	<p>1. Для обеспечения взаимодействия конечных пользователей, пользователи должны входить в домен одного корневого УЦ;</p> <p>2. Компрометация секретного ключа корневого УЦ приостанавливает работу всего домена и требует защищенной доставки нового сертификата до каждого конечного пользователя.</p>	Наличие рисков при определении списков доверенных УЦ, обеспечении защиты доверенных списков (публикуемых обычно через веб-браузеры) от несанкционированного изменения.	<p>Алгоритм поиска и построения цепочек сертификатов для всех взаимодействующих сторон очень сложный</p> <p>Пользователь не может предоставить цепочку, которая обеспечивает проверку его сертификата всеми остальными пользователями.</p>
------------	--	--	--

Источником «первичного доверия» в иерархической архитектуре формирования единого домена цифрового доверия является корневой УЦ, создаваемый или контролируемый государством. Корневой УЦ выдает сертификаты прочим УЦ, которые, в свою очередь, выдают сертификаты гражданам и организациям.

Иным вариантом формирования единого домена цифрового доверия является использование браузерной модели национальной инфраструктуры открытых ключей, в которой построение доверительных отношений осуществляется с помощью ведения реестров доверенных УЦ и сертификатов их открытых ключей. При этом пользователи, входящие в различные субдомены доверия, доверяют друг другу в силу включения их УЦ в число доверенных (аккредитованных, присоединяемых). При этом для данной модели организации национального пространства доверия, необходимо обеспечить распространение сведений реестра доверенных УЦ по доверенным каналам связи. Также необходимо решать вопрос обеспечения оперативного доступа пользователей к спискам отозванных сертификатов, ведущихся УЦ, входящими в различные субдомены доверия.

Источником «доверия» в сетевой модели архитектуры формирования единого национального домена цифрового доверия является множество независимых корневых УЦ, каждый из которых формирует свой «домен доверия» и обеспечивает «парное» доверительное взаимодействие с любым другим УЦ, входящим в исходное множество корневых УЦ. При этом в указанное множество корневых УЦ на национальном уровне могут входить предприятия различных организационно-правовых форм.

В настоящее время в мире не существует единого подхода к выбору и реализации способа организации национальной инфраструктуры открытых ключей. В ряде стран, например, таких как Эстония и Канада используется иерархический способ построения национальной инфраструктуры открытых ключей. В других, например, в США для построения национального пространства доверия используется сетевая модель, включающая на общенациональном уровне несколько равноправных корневых УЦ (конкретно в США – 4).

В настоящее время в Российской Федерации действует свыше сотни УЦ, которые созданы в различных регионах, министерствах ведомствах, отраслях промышленности, крупных предприятиях. Существуют сегменты доверия, основанные на парных кросс-сертификациях, входящих в эти сегменты УЦ. Максимальный домен доверия образован объединением 7 удостоверяющих центров, различной организационно-правовой формы,

«Портал доверенных услуг», поддерживающий свыше 500 000 действующих сертификатов ключей подписи. Данное объединение носит открытый характер, и правила присоединения к нему опубликованы.

Хотя собственно системный проект не предусматривает выбора конкретного варианта для реализации национальной инфраструктуры цифрового доверия, необходимо учитывать, что при любом сценарии формирования единого домена доверия не допускается отказ от включения в него любых легально существующих и удовлетворяющих требованиям законодательства УЦ. По этой причине неотъемлемой частью инфраструктуры цифрового доверия является совокупность нормативных правовых, технических и организационных актов, исчерпывающе определяющих порядок присоединения УЦ к единому национальному домену.

Идентификация при электронном взаимодействии

Действующее законодательство регламентирует вопросы идентификации и аутентификации участников электронного взаимодействия исключительно в контексте использования электронной цифровой подписи, оставляя без должного нормативного обеспечения иные мотивы. Вместе с тем, на практике существует потребность осуществлять идентификацию пользователей и приложений в значительно более широком потребительском спектре. Естественно строгость идентификации и аутентификации как пользователей, так и приложений, а также стоимость их реализации существенно зависят от реализуемых механизмов.

Базовые сценарии идентификации граждан в приложениях электронного правительства

Базовые варианты идентификации при удаленном доступе граждан и организаций к сервисам электронного правительства перечислены ниже в порядке возрастания надежности:

1. Нестрогая идентификация на основе НИК или его аналогов без аутентификации (например, адресом электронной почты)
2. Идентификация на основе многоцветных логина и пароля, выбранных пользователем.
3. Идентификация, основанная на информации (знаниях), известных только идентифицируемому лицу (например, данные банковского счета, биографии пользователя, учетных данных мобильного оператора и др.).
4. Одноразовый пароль с использованием аппаратного токена, смарт-карты, одноразовый пароль, выдаваемый гражданину после установления его личности, одноразовый пароль, передаваемый по независимым каналам связи.
5. Идентификация на основе инфраструктуры открытых ключей с хранением закрытого ключа подписи на незащищенном носителе.
6. Идентификация на основе инфраструктуры открытых ключей с хранением закрытого ключа подписи на защищенном от чтения носителе.

Уровень защиты участников электронного взаимодействия определяется через компромисс между рисками и издержками на защиту от них применительно к конкретным услугам.

Универсальные электронные карты и идентификация граждан

В зависимости от используемых технологий и поддерживаемых функций универсальная электронная карта (далее — УЭК) может выполнять роль универсального или ограниченного удостоверения личности:

- Универсальные смарт-карты, приравненные по статусу к удостоверению личности гражданина и обеспечивающие его надежную идентификацию с помощью технологии цифровой подписи.
- Специализированные карты, которые используются в ограниченном числе случаев (карты социального обеспечения, медицинского страхования, водительское удостоверение, далее — социальные карты), позволяющие осуществить идентификацию держателя карты с ограниченной надежностью с целью:
 - Подтверждения прав держателя карты на получение отдельных видов социальной помощи или доступа к определенной информации.
 - Зачисления на банковские счета дотаций, пенсий, пособий и др.
 - Снятия наличных денежных средств, безналичной оплаты товаров и услуг и др.

Отдача от применения УЭК определяется развитостью инфраструктуры ее поддержки, к которой относятся:

- Сеть терминальных устройств, позволяющих принимать карту в местах ее использования (банковские терминалы, рабочие станции государственных служащих и домашних хозяйств и др.).
- Центр обработки данных, интегрированный с электронными учетными системами, платежными системами.
- Каналы связи, позволяющие терминалам связываться с центрами обработки данных и электронными учетными системами в режиме реального времени.

Для расширения сети обслуживания карты УЭК должна быть совместима со стандартами международных платежных систем, что позволит использовать процессинговую банковскую сеть, имеющую собственную развитую инфраструктуру.

Выпущенные в значительных количествах на региональном уровне УЭК относятся к типу специализированных карт. Социальные сервисы, которые возможно поддержать с помощью такой карты, сконцентрированы преимущественно на региональном и муниципальном уровнях.

По мере увеличения числа сервисов электронного правительства и коммерческого рынка, требующих от граждан обладания цифровым удостоверением личности, будет увеличиваться количество пользователей, имеющих потребность в таком инструменте. Поэтому в числе приоритетных задач необходимо определить разработку и утверждение на государственном уровне единых требований к УЭК, а также организации процессов эмиссии, персонализации, обращения карт и их использования в рамках процессов предоставления в электронном виде госуслуг на базе инфраструктуры электронного правительства.

Служба доверенного времени

Служба предоставления доверенного эталонного времени должна обеспечивать высоконадежную и доступную синхронизацию во времени локальных часов участвующих во взаимодействии ИС, в том числе служб третьей доверенной стороны.

Электронный нотариат

Значительная часть унаследованных правоустанавливающих и правоподтверждающих документов существует в бумажном виде, и для их перевода в электронный вид требуются технологические (сканирование, распознавание и др.) и организационно-правовые процедуры, сохраняющие качество их юридической значимости.

Традиционно такого рода правовые действия выполняются институтом нотариата, в связи с чем необходимо сформировать соответствующие институты и практику, обобщив законодательство Российской Федерации о нотариате на случай электронных документов.

Необходимо также закрепить на уровне федерального закона возможность заверения эквивалентности бумажных и электронных копий документов по месту работы или проживания, с помощью удостоверяющих центров сертификатов ЦП, органами государственной власти, а также гражданином или организацией самостоятельно (механизм ответственного декларирования гражданином определенных юридических фактов). Необходимо на уровне правительственного акта закрепить формы заверения (ответственного декларирования) эквивалентности бумажных и электронных копий документов, допустимые в зависимости от правового содержания документов.

Необходимо изучить возможность хранения электронных копий бумажных документов в электронном виде у самих граждан и организаций (виртуальный личный сейф). Виртуальный сейф представляет собой государственную или частную ИС, позволяющую гражданам или организациям хранить в электронной форме заверенные электронные копии документов, а также предоставлять доступ к ним органам власти, коммерческим организациям, третьим лицам для проверки наличия у гражданина или организации определенных юридически значимых статусов.

Обеспечение совместимости информационных систем электронного правительства

К инструментам обеспечения семантической и технологической совместимости ИС электронного правительства относятся нормативные, технические и организационные средства, рассматриваемые в данном разделе.

Семантическая совместимость информационных систем электронного правительства

Основным средством обеспечения семантической совместимости ИС электронного правительства является создание единого нормативного источника информации о способах представления электронных данных (схемах данных), применяемых при взаимодействии государственных ИС друг с другом, а также с системами граждан и организаций — единого реестра схем данных (далее — РСД).

Основными задачами создания реестра схем данных являются:

- Снижение затрат на организацию информационного взаимодействия с государственными информационными системами за счет упрощения доступа к информации о семантике используемых при этом структур данных; обеспечения частичной или полной автоматизации процедур разработки конверторов данных;
- Снижение зависимости от поставщиков (разработчиков) информационных систем для государственных заказчиков и субъектов, взаимодействующих с государственными информационными системами.

Возникновение обязанности органа власти по регистрации схем данных

Обязательной регистрации в РСД подлежат схемы, описывающие данные, которые в ходе взаимодействий, предусмотренных функциональными возможностями ИС и регламентами обмена информацией, пересекают границы органов власти, в том числе передаются в ИС другого ведомства, подведомственного учреждения, предоставляются для доступа граждан, организаций или принимаются от них для обработки. Взаимодействие федерального органа исполнительной власти с его территориальным органом рассматривается как внутриведомственное за исключением случая, когда территориальный орган имеет двойное подчинение. В системах, эксплуатируемых несколькими ведомствами, регистрации подлежат схемы данных для всех случаев взаимодействия со смежными системами.

Статус реестра схем данных

С правовой точки зрения РСД является:

- официальным источником требований по семантической совместимости информационных систем;
- средством контроля над соответствием требованиям по семантической совместимости государственных ИС.

Основными документами, на основании которых осуществляется деятельность реестра, являются:

- нормативный правовой акт, устанавливающий статус реестра, определяющий ответственный за его ведение орган;
- регламент ведения реестра;
- технические требования к регистрируемым схемам данных.

С момента полного введения регулирования в области применения схем данных во вновь внедряемых или модернизируемых системах не допускается использование для межведомственного информационного обмена, а также при обмене данными с гражданами и негосударственными субъектами незарегистрированных схем данных и схем данных, не соответствующих техническим требованиям.

Все схемы, зарегистрированные в РСД, должны быть доступны всем заинтересованным лицам.

Концепция правового и нормативно-технического регулирования использования схем данных

Нормативная конструкция, определяющая требования к описанию используемых при электронном взаимодействии данных, которая должна быть разработана и введена в действие в 2010-2012 гг., выглядит следующим образом:

- формирование единого нормативного источника сведений о данных, используемых при электронном взаимодействии (РСД);
- установление технических требований к схемам данных;
- установление обязанностей органов исполнительной власти по регистрации схем в РСД;
- установление обязанностей органов исполнительной власти по использованию стандартизованных схем данных при реализации внешних интерфейсов информационных систем;
- установление рекомендательного характера использования стандартизованных схем данных региональными и муниципальными органами власти при реализации внешних интерфейсов информационных систем.

Технологическая совместимость информационных систем электронного правительства

В разделе описан комплекс взаимоувязанных подходов к принципам выбора технологий при создании ИС электронного правительства, в том числе инструменты стандартизации интерфейсов информационных систем путем принятия требований к форматам данных и протоколам взаимодействия, которые должны учитываться при разработке и закупке программного обеспечения для государственных нужд.

Государственный реестр стандартизованных спецификаций

Основным средством обеспечения технической совместимости информационных систем электронного правительства является создание единого нормативного источника информации об унифицированных (стандартизованных) способах реализации интерфейсов, используемых при взаимодействии государственных информационных

систем друг с другом, а также с другими информационными системами — государственного реестра стандартизированных спецификаций (далее — РСС).

Требования к регулированию интерфейсов информационных систем

Неудачный или обусловленный коммерческими интересами выбор технологии электронного взаимодействия с гражданами и организациями может приводить к их дискриминации. Пользователи безосновательно принуждаются приобретать и использовать конкретные программные продукты или технологические платформы, что ограничивает их права, снижает доступность государственных услуг, подрывает конкурентные стимулы для развития рынка информационных технологий и создает предпосылки для его монополизации. С другой стороны, попытка удовлетворить абсолютно любые технологические потребности граждан-пользователей информационных систем может привести к чрезмерным расходам на поддержку редких или устаревших технологий.

Для преодоления этих проблем необходимо определение круга унифицированных и пригодных для многократного использования технологических решений, которым должно отдаваться предпочтение при построении государственных информационных систем. При этом политика государства в области унифицированных спецификаций:

- не должна носить запретительного характера, то есть препятствовать внедрению новых, более прогрессивных технологий в качестве дополнения к консервативным унифицированным спецификациям;
- не должна дискриминировать разработчиков программного обеспечения, предписывая использование конкретных программ для реализации унифицированных спецификаций.

Принципы регулирования интерфейсов информационных систем

Обобщение мирового и отечественного опыта позволяет выделить несколько принципов, которые на современном этапе применяются во всех странах, использующих стандартизацию интерфейсов государственных информационных систем:

- Принцип зрелости спецификаций и их поддержки рынком. Для реализации интерфейсов государственных информационных систем допускаются только те спецификации, которые не несут риска потери государственных инвестиций по причине бесперспективности спецификации.
- Принцип минимума обременений. Приоритет получают те спецификации, использование которых накладывает минимум ограничений на пользователей, не принуждают их к приобретению конкретного ПО.
- Принцип приоритетности открытых стандартов. В случаях, когда для решения определенной технологической задачи существует открытый стандарт, предпочтение должно отдаваться ему, а не нестандартной технологии.

Запрещение использования закрытых технологий, как таковых, нецелесообразно по экономическим и техническим причинам. Необходимо и достаточно ограничить использование закрытых технологий в случаях, когда это препятствует информационному взаимодействию — при реализации внешних интерфейсов.

Регламент формирования перечня форматов и протоколов, включаемых в реестр стандартизированных спецификаций, должен базироваться на полной открытости предусмотренных в нем процедур, включая гласность исполнения регламента и принятия решений и возможность участия в процедурах, предусмотренных регламентом, любого заинтересованного лица.

Требования к стандартизованным спецификациям

Необходимо установить следующие обязательные критерии отбора спецификаций, подлежащих реализации в интерфейсах государственных информационных систем:

- Стандарт должен быть опубликован в виде документа, содержащего информацию, достаточную для независимой от разработчика стандарта реализации описанной в нем технологии.
- Условия использования стандарта и связанных с ним документов не должны предусматривать платежей за реализацию технологии, а также иных ограничений, ставящих пользователей стандарта в зависимость от его разработчиков: требования о получении разрешений на использование, запрет на использование в определенных отраслях и т. п.
- Стандарт не должен включать в себя, в том числе посредством ссылок, спецификации, которые не удовлетворяют требованиям документированности и отсутствия ограничений использования.
- Предпочтение при выборе форматов и спецификаций должно отдаваться стандартам, утвержденными ведущими международными и отраслевыми организациями по стандартизации (ISO, IETF, W3C, OASIS).

Типология взаимодействий в приложениях электронного правительства

В подразделе рассмотрены типы взаимодействий информационных систем электронного правительства с внешними информационными системами, а также ситуации, в которых они применяются. Всего допускается три типа взаимодействий и семь способов их реализации.

1. Типы взаимодействий:
 - Взаимодействие с гражданами.
 - Взаимодействие с организациями.
 - Межведомственное взаимодействие.
2. Способы реализации межсистемного взаимодействия:
 - Межсистемный обмен с использованием веб-сервисов (основной способ).
 - Интерактивное взаимодействие с использованием веб-браузера (основной способ).
 - Загрузка-выгрузка файлов при браузерном взаимодействии.
 - Интерактивное взаимодействие с использованием модулей криптографической защиты или ЭЦП.
 - Прием информации на машинных носителях.
 - Использование «толстого клиента».
 - Асинхронный обмен с использованием электронной почты.

Для каждого из трех типов взаимодействий необходимо установить требования по конкретным стандартизованным спецификациям, указанным в РСС, которые должны поддерживать (реализовывать) конкретный способ межсистемного взаимодействия.

Возникновение обязанности по соответствию информационных систем требованиям по стандартизации

Соответствие требованиям по стандартизации является обязательным для всех ИС, которые задействованы в предоставлении государственных услуг или исполнении государственных функций и данные которых могут использоваться внешними информационными системами. Требование касается как разрабатываемых в рамках государственного заказа информационных систем, так и при поставке готовых программ.

Концепция нормативного правового и нормативно-технического регулирования интерфейсов информационных систем

Регулирование, вводящее обязательность реализации интерфейсов государственных информационных систем стандартизованным способом решает следующие задачи:

- Установление наиболее важных типов информационного взаимодействия и соответствующих им интерфейсов, которые должны реализовываться с использованием открытых стандартов.
- Установление стандартизованных спецификаций, которые должны использоваться для реализации этих интерфейсов и обязательности их применения для реализации интерфейсов ИС электронного правительства.

Формирование инженерной инфраструктуры

В состав инженерной инфраструктуры электронного правительства входят:

- Каналы связи.
- Защищенная транспортная сеть.
- Интранет-сеть, обеспечивающая межведомственное и межуровневое взаимодействие, а также открытый контур ведомственных сетей.
- Межведомственные (надведомственные) центры обработки данных (вычислительные мощности) и иная аппаратная инфраструктура.

Внутренние телекоммуникационные сети и внутриведомственная инженерная инфраструктура (центры обработки данных, системное и специализированное программное обеспечение, персональные компьютеры, серверы и т.п.) органов государственной власти и организаций, участвующих в предоставлении государственных услуг, формируются ведомствами в пределах сфер их компетенции.

В Российской Федерации созданы и активно развиваются частные и государственные телекоммуникационные сети, которые должны использоваться при формировании общегосударственной телекоммуникационной инфраструктуры, исходя из соображений экономической эффективности. Для этого необходимо:

1. Произвести инвентаризацию унаследованных ведомственных, отраслевых, телекоммуникационных сетей, сетей подведомственных организаций, а также иных объектов инженерной инфраструктуры, включая центры обработки данных и информационные центры (далее — объекты инженерной инфраструктуры).
2. Сформировать опорную телекоммуникационную сеть и определить оператора (операторов), осуществляющего (осуществляющих) ее эксплуатацию и предоставление телекоммуникационных сервисов конечным потребителям.
3. Установить на уровне постановления Правительства Российской Федерации перечень объектов инженерной инфраструктуры электронного правительства, а также порядок владения, пользования и распоряжения объектами инженерной инфраструктуры электронного правительства.
4. Установить на уровне постановления Правительства Российской Федерации обязательные требования к объектам инженерной инфраструктуры по информационной, технологической безопасности, а также формы оценки соответствия (сертификация, декларирование).
5. Разработать порядок присоединения частных и государственных телекоммуникационных сетей к опорной сети, включая механизмы управления единой сетью, политику обеспечения безопасности и качества обслуживания.
6. Разработать порядок бюджетного финансирования и порядок привлечения финансирования из внебюджетных источников, необходимого для эксплуатации объектов инженерной инфраструктуры электронного правительства.
7. Разработать порядок доступа к сети связи (порядок оказания услуг), включая размер тарифов на услуги и работы, а также порядок тарификации.

8. Произвести инвентаризацию потребности федеральных органов исполнительной власти, их территориальных подразделений и подведомственных организаций, участвующих в предоставлении государственных услуг, в телекоммуникационной инфраструктуре (далее — объекты подключения), произвести ранжирование объектов подключения по приоритетности подключения к телекоммуникационной инфраструктуре, сформировать соответствующий план.
9. Определить порядок использования органами государственной власти и организациями, участвующими в предоставлении государственных услуг, объектов инженерной инфраструктуры электронного правительства, коммерческих сетей связи.

Информационная безопасность

Деятельность электронного правительства уже в краткосрочной перспективе будет способствовать значительному расширению использования государственных ИС для целей управления, увеличению обмена информацией и, одновременно с этим, повысит уровень информационных рисков, несанкционированной утечки, искажения, уничтожения и снижения доступности хранимой, обрабатываемой и передаваемой информации. Существенному повышению возможности несанкционированного использования или модификации информации, блокированию процесса получения информации, введению в оборот ложной информации, приводящей к принятию ошибочных решений и, как следствие, к значительному материальному ущербу, способствуют:

- увеличение объемов обрабатываемой, передаваемой и хранимой в ИС информации;
- сосредоточение в базах данных информации различного уровня важности и конфиденциальности;
- расширение круга пользователей, имеющих доступ к государственным информационным ресурсам России;
- увеличение числа удаленных рабочих мест, появление мобильных рабочих мест;
- широкое использование для связи пользователей глобальной сети Internet и различных каналов связи.

Одним из направлений государственной политики в сфере информатизации является формирование и защита информационных ресурсов государства, как национального достояния⁴. Гражданский кодекс Российской Федерации определяет информацию как объект права⁵.

Информационные ресурсы, являясь объектом отношений физических, юридических лиц и государства, подлежат обязательному учету и защите как всякое материальное имущество собственника⁶ наряду с другими ресурсами. При этом собственнику предоставляется право самостоятельно, в пределах своей компетенции, устанавливать режим защиты информационных ресурсов и доступа к ним.

Защите подлежат только те сведения (сообщения, данные) независимо от формы их представления неправомерное обращение с которыми может нанести ущерб гражданам, обществу или государству в целом. Степень защиты информации определяет собственник информации, с учетом, в необходимых случаях, рекомендаций уполномоченных государственных органов. Любые нормативы на степень защиты информации, устанавливаемые регулирующими государственными органами должны базироваться на требованиях феде-

⁴ Указ Президента РФ № 170, 1994 г., «Об основах государственной политики в сфере информатизации» (ред. от 09.07.97 г.)

⁵ Гражданский Кодекс Российской Федерации, часть I, ст. 128

⁶ Федеральный Закон «Об информации, информационных технологиях и о защите информации»

рального законодательства. Ответственность за выполнение мер защиты лежит не только на собственнике информации, но и на любом владельце и пользователе.

Конфиденциальной считается такая информация, доступ к которой ограничивается в соответствии с законодательством. Федеральное законодательство содержит либо прямую норму, согласно которой какие-либо сведения относятся к категории конфиденциальных и ограничивается доступ к ним, либо определяет признаки, которым должны удовлетворять эти сведения. Законодательством определяются признаки служебной и коммерческой тайны как особого объекта гражданских прав⁷.

Согласно существующему подходу к служебной тайне государственных организаций и органов государственной власти всех уровней относятся сведения, не являющиеся государственной тайной, содержащие служебную информацию (сведения) о деятельности государственных органов, доступ к которой ограничен в соответствии с Гражданским кодексом РФ и федеральными законами. Таким образом, органы государственной власти Российской Федерации любого уровня в пределах своей компетенции вправе отнести определенного рода информацию к категории служебной тайны и установить режим ее защиты. Исключение составляют только сведения, доступ к которым не может быть ограничен в принципе. Например, правовые акты, устанавливающие статус этих органов власти и государственных организаций России, описание его структуры, функций, направлений и форм деятельности, его адрес, порядок рассмотрения и разрешения заявлений физических и юридических лиц, сведения о чрезвычайных ситуациях, опасных природных явлениях, экологическая, гидрометеорологическая, гидрогеологическая, демографическая, санитарно-эпидемиологическая информация.

Информационные ресурсы государственной организации и органа государственной власти также могут представлять коммерческую ценность и быть товаром⁸, за исключением случаев, предусмотренных законодательством. Несанкционированные действия и использование такой информации может нанести ущерб интересам не только непосредственно данной организации, но и Российской Федерации в целом. Однако при этом, режим защиты информации, представляющей коммерческую ценность, определяется именно такой организацией или органом власти как собственником этих ресурсов.

Таким образом, субъектами правоотношений в процессе защиты информации при реализации функционала электронного правительства являются:

- Российская Федерация, как собственник информационных ресурсов.
- Государственный орган или организация, уполномоченные Правительством РФ на распоряжение переданными информационными ресурсами.
- Иные федеральные органы государственной власти, органы власти субъектов Российской Федерации, муниципальных образований, организации, учреждения, юридические и физические лица, как совладельцы и пользователи информационных ресурсов.
- Должностные лица и сотрудники структурных подразделений учреждений, организаций, воинских формирований и подразделений, иных федеральных органов государственной власти, органов власти субъектов Российской Федерации, муниципальных образований, организаций, учреждений, юридических лиц, а также физические лица, как пользователи информационных ресурсов.
- Юридические и физические лица, сведения о которых накапливаются в информационных ресурсах государственного органа, как собственники (владельцы) этой информации;
- Подразделения, обеспечивающие эксплуатацию технических средств обработки информации;
- Другие юридические и физические лица, причастные к созданию и функционированию технических средств обработки информации.

⁷ Гражданский Кодекс Российской Федерации, часть I, ст. 139

⁸ Федеральный Закон «Об информации, информатизации и защите информации», № 24-ФЗ, 1995 г., ст. 6.6

Объектом защиты информации в данном контексте являются сведения, содержащиеся в информационных ресурсах государственной организации, зафиксированные на материальном носителе с реквизитами, позволяющими их идентифицировать, участвующие в процессах сбора, обработки, накопления, хранения и распространения информации, доступ к которой ограничивается. Таким образом, в рамках реализации функций электронного правительства основными объектами защиты могут быть:

- Информационные ресурсы органов государственной власти, региональных органов управления и муниципальных образований.
- Информационные и программные ресурсы (прикладное программное обеспечение, системное программное обеспечение, инструментальные средства и утилиты) ИС, чувствительные по отношению к случайным и несанкционированным воздействиям, содержащие технологическую информацию управления автоматизированными системами и транспортной сетью.
- Служебные информационные ресурсы ИС (базы данных и файлы данных, системная документация, руководства пользователя) содержащие сведения о служебной, технологической и управляющей информации.
- Информационные ресурсы подсистем обеспечения безопасности информации, содержащие сведения о структуре, принципах и технических решениях защиты информации.

В перечисленных условиях обеспечение безопасности информации в системах и ресурсах электронного правительства должно быть направлено, в первую очередь, на исключение нанесения или существенное уменьшение ущерба перечисленным выше субъектам правоотношений, защиту конституционных прав личности, на сохранение личной тайны и персональных данных.

Обеспечить информационную безопасность систем электронного правительства предлагается путем создания защищенной сети передачи данных (ЗСПД) и построения подсистем обеспечения информационной безопасности (ПОИБ) для основных информационно-технических компонентов электронного правительства: портала государственных услуг (ПГУ); информационно-платежного шлюза (ИПШ), региональных ЭП; прикладных государственных информационных систем ФОИВ. Архитектура информационной безопасности представлена на рисунке 6.3.

Обеспечение информационной безопасности систем ЭП

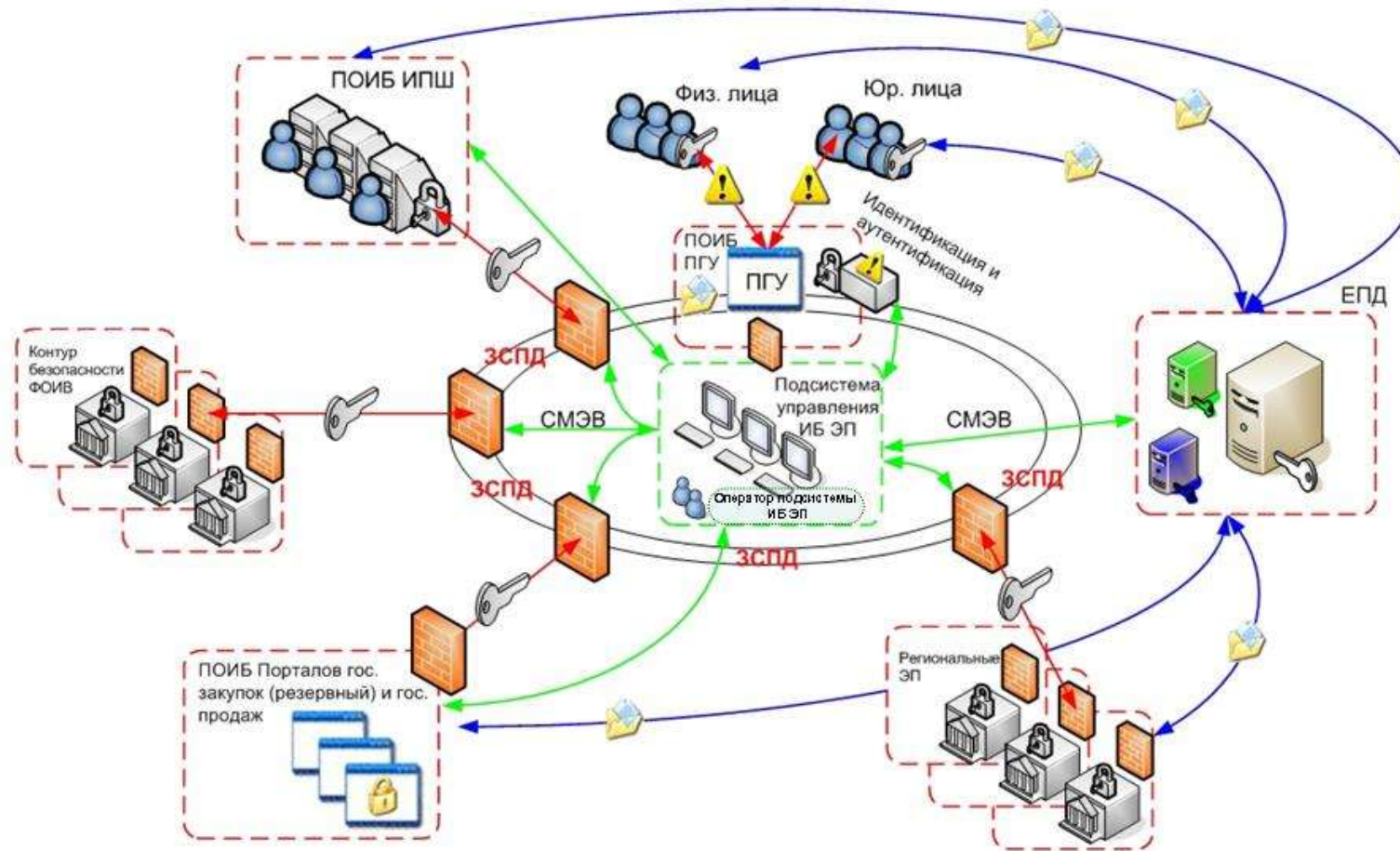


Рисунок 6.3. Схема обеспечения информационной безопасности систем электронного правительства.

В ходе разработки, внедрения, эксплуатации государственных ИС, субъектам правоотношений может быть причинен следующий ущерб:

- материальный ущерб от разглашения защищаемой информации;
- материальный, моральный ущерб от любых неправомерных действий с объектами защиты;
- моральный, физический, материальный ущерб личности, от разглашения персональных данных;
- моральный, материальный ущерб от нарушения конституционных прав и свобод личности;
- материальный ущерб от необходимости восстановления нарушенных прав и объектов защиты;
- моральный и материальный ущерб от дезорганизации деятельности;
- материальный ущерб от уничтожения (утраты) *объектов защиты* и средств их обработки;
- материальный, моральный ущерб от несвоевременного поступления информации потребителям;
- моральный, материальный ущерб деловой репутации;
- материальный ущерб от невозможности выполнения обязательств перед третьей стороной;
- материальный, моральный ущерб от нарушении международных обязательств.

При этом причиненный ущерб может квалифицироваться как состав преступления, предусмотренный уголовным правом, или сопоставляться с рисками утраты, предусмотренными гражданским, административным или арбитражным правом.

Основными угрозами безопасности информации при разработке, создании, развитии и эксплуатации государственных ИС России являются:

- для нарушения конфиденциальности информации:
 - хищение (копирование) информации и средств ее обработки
 - утрата (неумышленная потеря, утечка) информации, средств ее обработки
- для нарушения целостности информации:
 - модификация (искажение) информации
 - отрицание подлинности информации
 - навязывание ложной информации
- для нарушения доступности информации:
 - блокирование информации
 - уничтожение информации и средств ее обработки

Для достижения целей защиты и нейтрализации угроз информационной безопасности при осуществлении деятельности электронного правительства должно быть обеспечено эффективное решение задач:

- защита от вмешательства в процесс функционирования государственных ИС со стороны пользователей, иных неуполномоченных и посторонних лиц, в том числе легальных пользователей этих ресурсов;
- обеспечение полноты, достоверности и целостности сведений, содержащихся и вносимых в указанные ИС;
- обеспечение физической сохранности технических средств и программного обеспечения ИС и защита их от действия техногенных и стихийных источников угроз;

регистрация событий, влияющих на безопасность информации, обеспечения полной подконтрольности и подотчетности выполнения всех операций, которые могут оказать влияние на состояние информационной безопасности ИС и циркулирующей в них информации;

своевременное выявление, оценка и прогнозирование источников угроз безопасности информации, причин и условий, способствующих нанесению ущерба интересам субъектов правоотношений, нарушению нормального функционирования и развития государственных ИС;

анализ рисков реализации угроз безопасности информации и оценка возможного ущерба, предотвращение неприемлемых последствий нарушения безопасности информации, циркулирующей в ИС, создание условий для минимизации и локализации наносимого ущерба;

обеспечение возможности восстановления актуального состояния ИС при нарушении безопасности информации и ликвидации последствий этих нарушений;

формирование целенаправленной политики в области обеспечения безопасности информации при разработке, внедрении, эксплуатации и совершенствовании ИС.

Основные принципы обеспечения безопасности информации в государственных информационных системах, вовлеченных или связанных с деятельностью электронного правительства.

- Принцип законности. Проведение защитных мероприятий должно быть согласовано с действующим законодательством в области информации, информатизации и защиты информации с применением всех дозволенных методов обнаружения и пресечения нарушений при работе с информацией.
- Принцип максимальной дружелюбности и прозрачности. Противодействие угрозам безопасности информации всегда носит недружелюбный характер по отношению к пользователям и обслуживающему персоналу ИС, так как меры по защите информации всегда налагают ограничения на работу организационного и технического характера. Поэтому принимаемые меры должны максимально совмещаться с используемыми операционной и программно-аппаратной структурой ИС, а также должны быть понятны и оправданы для пользователей.
- Принцип превентивности. Меры по защите информации и внедряемые СЗИ должны быть нацелены, прежде всего, на недопущение (пресечение) реализации угроз безопасности информации, а не на устранение последствий их проявления.
- Принцип оптимальности и разумной разнородности. Для сокращения расходов на создание систем обеспечения безопасности должен осуществляться оптимальный выбор соотношения между различными методами и способами противодействия угрозам безопасности информации. Дополнительно внедряемые средства защиты должны дублировать основные функции защиты, уже используемые в программно-аппаратной среде ИС, и по возможности иметь другое происхождение, чем сама эта среда, что позволяет существенно затруднить процесс преодоления защиты за счет иной логики построения защиты.
- Принцип адекватности и непрерывности. Решения, реализуемые системами защиты информации, должны быть дифференцированы в зависимости от важности защищаемой информации и вероятности возникновения угроз ее безопасности. Безопасность информации в государственных информационных системах должна обеспечиваться непрерывно в течение всего жизненного цикла систем.

- Принцип адаптивности. Системы обеспечения информационной безопасности должны строиться с учетом возможного изменения конфигурации ИС, роста числа пользователей, изменения степени конфиденциальности и ценности информации.
- Принцип доказательности и обязательности контроля. Должны реализовываться организационные меры внутри сети и применение специальных аппаратно-программных средств идентификации, аутентификации и подтверждения подлинности информации. Должна обеспечивать обязательность, своевременность и документированность выявления, сигнализации и пресечения попыток нарушения установленных правил защиты.
- Принцип самозащиты и конфиденциальности самой системы защиты информации.
- Принцип многоуровневости и равнопрочности. ИС должна реализовывать защиту информации на всех уровнях своей жизнедеятельности (технологическом, пользовательском, локальном, сетевом). Защита должна строиться эшелонировано, и иметь несколько последовательных рубежей таким образом, чтобы наиболее важная зона безопасности находилась внутри других зон. Все рубежи защиты должны быть равнопрочными к возможности реализации угрозы.
- Принцип простоты применения и апробированности защиты. Должны применяться средства защиты, для которых формально или неформально возможно доказать корректность выполнения защитных функций, проверить согласованность конфигурации различных компонентов, а их применение пользователями и обслуживающим персоналом должно быть максимально простым, чтобы уменьшить риски, связанные с нарушениям правил их использования. По той же причине целесообразно использовать средства защиты информации допускающие возможность централизованного администрирования.
- Принцип преемственности и совершенствования. Система защиты информации должна постоянно совершенствоваться на основе преемственности принятых ранее решений и анализа функционирования ИС.
- Принцип персональной ответственности и минимизации привилегий для пользователей всех уровней. Принимаемые меры должны определять права и ответственности каждого уполномоченного лица. Распределение прав и ответственности должно в случае любого нарушения позволять определить круг виновных. Система обеспечения информационной безопасности должна обеспечивать разделение прав и ответственности между пользователями.

Принцип персональной ответственности и минимизации привилегий для пользователей всех уровней. Система обеспечения информационной безопасности должна обеспечивать разделение прав и ответственности между пользователями и минимизацию привилегий, позволяя, в случае любого нарушения, определить круг виновных.

7. Обеспечение доступности государственных услуг и инфраструктуры электронного правительства

Доступность — совокупность свойств государственной услуги, обеспечивающих:

- полноту и актуальность информирования заявителей о порядке предоставления услуги;
- легкость обнаружения услуги;
- получение услуги с минимальными временными и финансовыми затратами.

Недостаточный уровень доступности услуги может создать трудности для граждан и организаций, вплоть до фактической невозможности ее получения. Если не обеспечен достаточный уровень доступности электронного канала взаимодействия, граждане предпочитают получать услугу в традиционной форме, а государственные инвестиции в формирование электронного правительства оказываются неэффективными.

В настоящее время число государственных услуг, предоставляемых в электронном виде, невелико. В то же время имеющиеся примеры демонстрируют типичные проблемы, воспроизводящиеся в различных сферах государственного управления.

Наиболее критичными рисками, связанными с плохой доступностью услуг, являются:

- высокая стоимость доступа к сети Интернет;
- реализация государственных услуг в опоре на закрытые и платные для пользователей технологии;
- невостребованность реализации конкретной государственной услуги в электронном виде (малое число потенциальных пользователей);
- игнорирование потребностей различных категорий граждан, препятствующее реализации их законных прав.

Доверие получателей государственных услуг определяется следующими факторами:

- функциональная целостность и надежность информационных систем электронного правительства;
- гарантированность целевого использования персональных данных пользователя, предоставленных им в ходе получения услуги;
- выполнение ожиданий пользователей в отношении временных и ресурсных затрат, связанных с получением услуги в электронном виде.

Принципы обеспечения доступности государственных услуг: целевое состояние

Принципы, обеспечивающие доступность электронных государственных услуг, подлежащие нормативному закреплению, изложены ниже и сгруппированы по трем направлениям: принципы качественного правового регулирования, принципы качественного информирования и принципы технологической нейтральности.

Принципы качественного правового регулирования

1. Полнота правового регулирования

Нормативные правовые акты, регулирующие порядок предоставления государственных услуг, должны предусматривать все возможные ситуации, в которых граждане обращаются за получением услуги. Если заявитель не может реализовать свое право на получение государственной услуги в рамках действующего порядка ее предоставления⁹, но в соответствии с вышестоящими нормативными правовыми актами имеет право на ее получение, в нормативных актах должен быть описан правовой механизм оперативной реализации законных прав заявителей.

2. Регламентированное взаимодействие учетных систем

⁹ Как, например, жители Приднестровья и Абхазии, имеющие российское гражданство, но ввиду неопределенности своего правового статуса, часто не имеющие возможности получения государственных услуг.

Органы, участвующие в предоставлении государственных услуг, не вправе требовать от заявителей актуальную и законно имеющуюся в их распоряжении информацию (или могущую быть законно полученной).

Получатели государственных услуг должны иметь возможность уполномочить орган, участвующий в предоставлении государственной услуги, обратиться в другие органы государственной власти и иные организации для получения сведений, необходимых для предоставления услуги.

Факты регламентированного доступа органов власти и уполномоченных лиц к сведениям, относящимся к гражданам и организациям, должны автоматически протоколироваться.

3. Представительство интересов

В случаях, когда это не противоречит законодательству, должны быть предусмотрены возможности опосредованного (через законного представителя) получения государственных услуг для граждан, которые не могут реализовать свое право получения услуги самостоятельно.

4. Право на дистанционное взаимодействие

Нормативные правовые акты, регулирующие порядок предоставления государственных услуг (функций), должны предусматривать возможность:

- доступа граждан к относящимся к ним данным, учитываемым федеральными органами исполнительной власти и участвующими в предоставлении услуг организациями, и в случае выявления в них ошибок, их оперативного исправления;
- уплаты государственной пошлины через электронные и мобильные системы платежей.
- подачи заявления, инициирующего предоставление государственной услуги, и необходимых для этого документов, а также получения результатов предоставления государственной услуги в электронном виде;

5. Многоканальность предоставления государственной услуги

Заявители вправе самостоятельно определять, в каком виде — бумажном и/или электронном — они будут выполнять те или иные процедуры при получении государственной услуги. Использование электронного канала взаимодействия как единственного для получения государственной услуги следует считать исключительным случаем. Пользователям, не имеющим возможности получения услуги в электронном виде (например, не имеющим навыков использования ИКТ), должен быть обеспечен традиционный способ получения услуги.

6. Принцип повышения эффективности электронного взаимодействия

Переход к предоставлению государственной услуги в электронном виде не должен приводить к усложнению для получателей услуг процедур, увеличению сроков рассмотрения и принятия решения, росту издержек.

7. Законность использования ИС

ИС, используемые федеральными органами исполнительной власти и участвующими в предоставлении услуг организациями, должны в полной мере реализовывать требования нормативных правовых актов, устанавливающих порядок предоставления этих услуг. На случай если заявитель не может реализовать свое право на получение государственной услуги в электронном виде в силу несовершенства ИС (отсутствие функциональности, неработоспособности и т. п.), в соответствующих нормативных правовых актах должен быть описан механизм оперативной реализации законных прав заявителя.

8. Ответственность за действия, совершаемые автоматически или автоматизированно

Все юридически значимые действия, включая фиксацию юридических фактов, предоставление справок и выписок и т. п., совершаемые автоматизировано с помощью ИС, должны совершаться от имени конкретного должностного лица, которое несет персональную ответственность за наступающие последствия.

9. Отсутствие произвольных ограничений доступа к государственным услугам

Идентификация пользователей, запрос у них персональных или иных данных, заключение лицензионных или иных соглашений с пользователями допустимо только в случаях, прямо предусмотренных законодательством. К любой открытой информации государства, в том числе связанной с порядком и ходом предоставления государственных услуг, должен предоставляться немедленный бесплатный доступ.

10. Протоколирование действий государственных служащих

В ИС, используемых для предоставления государственных услуг, должна отсутствовать техническая возможность нецелевого использования информации, связанной с заявителями. ИС должны предусматривать автоматическое ведение протоколов, фиксирующих момент совершения всех юридически значимых действий с помощью ИС, состав действий и субъекта их совершившего. Регламенты эксплуатации ИС, технические средства должны предусматривать использование операторами и государственными служащими индивидуальных средств их идентификации.

Принципы качественного информирования

1. Доступное для понимания информирование

Органы государственной власти информируют получателей услуг доступным для них способом без использования специальной терминологии:

- о существовании услуги, предоставляемой в электронном виде и о порядке ее получения;
- об отличиях (в том числе преимуществах и недостатках) процедур получения услуги в электронном и традиционном виде;
- о правовых последствиях, потенциальных рисках и проблемах, связанных с получением услуги в электронном виде;
- о требованиях к квалификации заявителей, к используемым ими программно-техническим (форматы данных, коммуникационные протоколы) и телекоммуникационным (ширина канала связи и др.) средствам, средствам идентификации, использование которых обязательно для получения услуги.

2. Широкое информирование

Пользователи электронного правительства имеют возможность найти информацию об услуге:

- с использованием распространенных средств поиска в сети Интернет;
- на официальных сайтах органов власти с использованием встроенных средств поиска и навигационных средств;
- на Едином портале государственных услуг с использованием встроенных средств поиска и навигационных средств;
- на информационных стендах в местах получения услуги в традиционной форме.

Принципы технологической нейтральности

1. Открытость внешних интерфейсов государственных ИС

Все внешние интерфейсы ИС, используемых для предоставления информации или государственных услуг, должны быть реализованы посредством открытых стандартов и быть официально опубликованы органами исполнительной власти, отвечающими за эксплуатацию этих ИС.

Реализация внешних интерфейсов ИС с использованием закрытых технологий и технологий, требующих для их использования заключения лицензионных, а также иных соглашений, допускается только в качестве дополнительных возможностей, использование которых остается на усмотрение получателя услуги.

2. Запрет на технологическую дискриминацию

Органы государственной власти обеспечивают доступ к государственной услуге посредством всех электронных каналов взаимодействия, востребованных пользователями электронного правительства, не ограничивая круг получателей услуги владельцами конкретных видов аппаратного и программного обеспечения, использованием услуг конкретных поставщиков услуг на рынке, в том числе операторов связи. Если действующие нормативные правовые акты не позволяют выполнить данное требование, орган исполнительной власти, предоставляющий соответствующую государственную услугу, обязан инициировать процедуру их корректировки.

3. Основные каналы взаимодействия электронного правительства

Основными способами взаимодействия в ходе предоставления государственных услуг в электронной форме являются веб-браузер и электронная почта. Взаимодействие через веб-браузер и электронную почту, если предоставление какой-либо услуги технически осуществимо с их использованием, должны реализовываться в обязательном порядке. Другие каналы взаимодействия и программное обеспечение, требующее специальной установки на компьютеры заявителя только для целей предоставления услуги, могут использоваться только в качестве дополнительных способов взаимодействия после реализации основных.

4. Разумность требований к компетентности пользователей

Предоставление государственных услуг не должно требовать от пользователя навыков, превышающих базовые (использование веб-браузера, электронной почты и текстового процессора, а также средств идентификации). Если для осуществления какой-либо процедуры требуются знания и навыки, выходящие за рамки базовой компетенции пользователей, в интерфейсе веб-сайтов и программного обеспечения должны быть реализованы общая и контекстная справки. При этом должны быть предусмотрены мероприятия по формированию у граждан актуальных компетенций получения государственных и муниципальных услуг в электронном виде, включая подготовку соответствующих методических рекомендаций, разработку и предоставление возможности бесплатного использования посредством сети Интернет электронных учебных курсов по наиболее востребованным направлениям применения ИКТ (информационная безопасность, основы ЭЦП, работа с типовыми государственными программно-техническими решениями).

5. Наличие единой точки доступа к сервисам электронного правительства

При проектировании и введении в эксплуатацию ИС, используемых для предоставления информации или государственных услуг, должны быть предусмотрены средства интеграции с Единым порталом государственных услуг, а также, в случаях, предусмотренных законодательством, средства идентификации пользователей.

6. Наличие у ИС электронного правительства программных интерфейсов

ИС, используемые для предоставления информации, должны помимо визуального (пользовательского) доступа к информации обеспечивать сервисы автоматизированного (пакетного) получения данных через стандартизированные программные интерфейсы с помощью ИС пользователя (стандартные межмашинные интерфейсы).

7. Учет интересов особых категорий пользователей электронного правительства

ИС, используемые для предоставления информации или государственных услуг, должны обеспечивать учет интересов граждан, имеющих ограниченные возможности:

- лиц с острыми недостатками зрения, для которых должна быть предусмотрена возможность увеличения кегля, которым набран текст, и повышения контрастности;
- слепых, использующих синтезаторы речи или дисплеи для шрифта Брайля;
- лиц с нарушениями функций опорно-двигательного аппарата, которые не имеют возможности пользоваться графическим манипулятором (мышью);
- лиц, страдающих эпилепсией и чувствительных к быстро изменяющимся изображениям.

Направления деятельности по обеспечению доступности услуг электронного правительства

Чтобы обеспечить практическое применение перечисленных принципов, необходимы следующие шаги:

- Разработка и утверждение нормативных правовых актов, устанавливающих требования, касающиеся доступности государственных услуг, предоставляемых в электронном виде.
- Формирование методологии обеспечения доступности государственных услуг, предоставляемых в электронном виде.
- Формирование организационных механизмов обеспечения доступности государственных услуг, предоставляемых в электронном виде.

Также необходимо обеспечить увеличение доступности сети Интернет, компьютерной техники и рыночных услуг в сфере ИКТ, в том числе путем создания центров общественного доступа к сети Интернет.

Разработка и утверждение нормативных правовых актов, устанавливающих требования по доступности государственных услуг, предоставляемых в электронном виде

Принципы обеспечения доступности государственных услуг, предоставляемых в электронном виде, изложенные в предыдущем разделе, должны быть закреплены нормативно на уровне федерального регулирования ввиду того, что они в равной мере применимы к федеральным, региональным и муниципальным услугам.

На уровне подзаконных актов необходимо их конкретизировать применительно к стадии проектирования электронного вида предоставления государственных услуг, в частности определить:

- порядок оценки целесообразности перевода предоставления государственной услуги в электронный вид (исходя из числа потенциальных пользователей и их готовности к электронному виду взаимодействия, дополнительных издержек заявителей, организационной сложностью перевода);
- категории граждан и организаций, являющихся потенциальными получателями разрабатываемой электронной услуги, каналы электронного взаимодействия в привязке к этапам предоставления услуги;
- формализованное описание порядка предоставления государственной услуги в электронном виде, включая описание каналов предоставления государственной услуги;
- порядок финансово-экономического обоснования перевода предоставления государственной услуги в электронный вид и др.
- целевые показатели эффективности.

Формирование методологии обеспечения доступности государственных услуг, предоставляемых в электронном виде

В настоящее время опыт методической поддержки деятельности в системе государственного управления России практически отсутствует. Необходимо разработать и поддерживать в актуальном состоянии корпус рекомендательных материалов, которые должны дополнять и детализировать нормативные правовые документы, облегчая органам власти практическую работу по переводу деятельности в электронный вид.

Формирование организационных механизмов обеспечения доступности государственных услуг, предоставляемых в электронном виде

К числу организационных механизмов обеспечения доступности государственных услуг, предоставляемых в электронном виде, относятся:

- Формирование и публикация на этапе проектирования перевода государственной услуги в электронный вид совокупности индикаторов, описывающих ее целевое состояние.
- Организация регулярного мониторинга текущих результатов формирования электронного правительства и его публикация для всеобщего сведения. Мониторинг должен осуществляться независимо от ответственных за внедрение конкретных услуг органов исполнительной власти
- Стимулирование федеральных органов власти через проведение конкурсов, составление и публикацию рейтингов, награждение органов власти, обеспечивших наибольшую доступность электронных государственных услуг.

Увеличение доступности товаров и услуг в сфере ИКТ

Снятие цифрового барьера, отделяющего пользователей от современных цифровых технологий, не может быть осуществлено посредством государственных инвестиций и посредством создания специализированных пунктов доступа к сети Интернет. Необходимое для этого финансирование является чрезмерной нагрузкой для государственного бюджета. Государственные инвестиции уступают по эффективности частным, что усугубляется наличием в стране административно управляемого рынка и неразвитой конкуренции. Опыт финансовой поддержки отдельных рынков показывает, что уровень конечных цен вследствие государственных расходов изменяется незначительно, а выделенные бюджеты в основном остаются в распоряжении посредников.

Основным способом повышения доступности информационно-коммуникационных технологий для граждан и организаций следует считать институциональные меры, обеспечивающие развитие конкуренции в сфере ИКТ. Необходимо создать в стране благоприятные законодательные условия для предпринимательской деятельности и обеспечить соответствующую правоприменительную практику. Необходимо снятие межрегиональных антирыночных барьеров, преференций поставщикам услуг, использование административного ресурса при управлении рынком и др.

- Необходимо произвести обследование требований действующего регулирования отрасли ИКТ и правоприменительной практики, определить основные препятствия для конкуренции поставщиков товаров и услуг в сфере ИКТ и сформировать пакет предложений по следующим направлениям:

Лицензирование отрасли связи. Лицензирование отрасли связи регулируется в основном федеральным законом «О связи» и подзаконными актами, налагающими в настоящее время на операторов связи излишнее бремя регулирования, что приводит к повышению барьеров для входа на рынок, снижению конкуренции и росту конечных цен для потребителей. Количество лицензируемых видов деятельности в области связи избыточно и должно быть сокращено.

Распределение радиочастотного спектра. Совершенствование систем распределения спектра должно осуществляться в соответствии со следующими мировыми тенденциями:

- платность использования спектра для всех категорий пользователей;
- сохранение существующей системы выделения спектра в тех диапазонах, где это требуют соображения безопасности и международной гармонизации;
- выделение диапазонов для нелицензируемого использования («открытый спектр») в соответствии с потребностями современных перспективных технологий;
- первичное распределение спектра на аукционах с одновременным созданием вторичного рынка прав, допускающего их объединение и дробление, возможность смены пользователя.

Импорт компьютерной и телекоммуникационной техники. Необходимо сократить или ликвидировать тарифные и нетарифные ограничения на импорт средств ИКТ (за исключением случаев, подпадающих под требования технического регулирования). Первоочередной мерой является присоединение к Соглашению по информационным технологиям ВТО, которое предусматривает отмену пошлин на ряд товаров отрасли ИКТ, включая мобильные телефоны.

Рыночные механизмы на рынке телекоммуникаций. Мерой повышения доступности ИКТ для населения является увеличение роли рыночных механизмов на рынке телекоммуникаций, реализуемое в форме отказа государства от участия в капитале и коммерческой деятельности крупных инфраструктурных операторов связи, имеющих доминирующее положение на российском и региональных рынках. Должен быть обеспечен свободный доступ к телекоммуникационной инфраструктуре, созданной на средства государственного бюджета.

8. Обеспечение эффективности бюджетных расходов на формирование электронного правительства

Текущее состояние

Расходы на информатизацию отрасли осуществляются преимущественно целевым образом в рамках соответствующих программ, проектов, выделенных комплексов мероприятий. Автоматизация деятельности в интересах органов государственной власти и подведомственных организаций не упорядочена и для нее характерен ряд проблем:

- большое количество проектов, заканчивающихся концепциями, макетами, пилотными решениями, т.е. результатами, реально не внедряемыми в текущую деятельность и не находящих отражения в конкретных информационных системах;
- практически полное отсутствие на федеральном уровне информационных систем, автоматизирующих комплексные государственные услуги (функции), наличие положительных примеров только в сфере фискальных интересов государства (налоговое, таможенное оформление, пограничный контроль и т.п.) и систем безопасности (милицейские функции, контроль внешней миграции);
- дублирование существующих ИС и разработка новых систем «с нуля» без учета имеющихся наработок, осуществляемые как при изменении полномочий органа государственной власти, так и при смене ответственного заказчика или ответственного пользователя;
- многократная последовательная «доработка» существующих ИС без автоматизации новых сфер деятельности, а также разработка систем, автоматизирующих одни и те же виды деятельности, под различными названиями;

- отсутствие контроля расходов на внедрение ИКТ в подведомственной сфере (функции государственного заказчика переданы подведомственным учреждениям);
- отсутствие должного финансирования эксплуатации созданных ИС, обучение пользователей, техническую поддержку, в результате чего многие системы либо не используются, либо используются неэффективно.

Результаты ежегодного мониторинга развития и использования ИКТ в деятельности федеральных органов исполнительной власти, проведенного во втором квартале 2009 года, показывают, что общие затраты на информатизацию федеральных органов исполнительной власти (по данным 46 ведомств) в 2008 году составили 30,31 млрд. рублей.

Большая часть средств, затраченных на реализацию мероприятий в сфере использования ИКТ в деятельности федеральных органов исполнительной власти, была направлена на приобретение аппаратного обеспечения и сетевого оборудования (41,56% всего бюджета на информатизацию). По сравнению с данными 2007 года (43,58%) доля данной статьи расходов значительно не изменилась.

Согласно прогнозным показателям увеличилась доля расходов на содержание и техническую поддержку закупленного оборудования, созданной информационно-коммуникационной инфраструктуры и действующих информационных систем с 13,22% в 2007 году до 20,51% в 2008 году. В дальнейшем данный показатель будет только расти.

Существует также набор специфических проблем, прямо влияющих на степень эффективности бюджетных расходов, например:

- отсутствие методологии передачи знаний о внедренных ИКТ ответственным пользователям;
- необходимость увязки бюджетного процесса, связанного с внедрением ИКТ, автоматизируемых полномочий и процесса регистрации государственных ИС.

Целевое состояние системы управления расходами на внедрение ИКТ

Целевое состояние системы управления государственными расходами на внедрение ИКТ характеризуется созданием системы финансового менеджмента в сфере расходов на ИКТ, состоящей из:

- определения приоритетов в области информатизации (Правительство Российской Федерации);
- планирования мероприятий по информатизации и расходов на них;
- координации мероприятий по информатизации и их экспертная оценка на этапе планирования (Минкомсвязь России), разработки и принятия федерального закона о федеральном бюджете, исходя из запланированных мероприятий и объемов финансирования;
- реализации мероприятий по информатизации и экспертной оценки конкурсной документации для особо крупных, стратегических или значимых проектов информатизации;
- учета полученных результатов;
- отчетов по результатам реализации мероприятий;
- оценки эффективности реализации мероприятий информатизации.

Первым шагом на пути достижения заданного целевого состояния стало принятие постановления Правительства Российской Федерации от 24 мая 2010 г. № 365 «О координации мероприятий по использованию информационно-коммуникационных технологий в деятельности государственных органов».

Данный документ разработан в целях повышения эффективности планирования, создания и использования ИКТ в деятельности федеральных органов государственной власти, иных государственных органов, государственных внебюджетных фондов (далее – государственные органы), а также расходования средств федерального бюджета на соответствующие мероприятия по информатизации, и предусматривает комплекс мероприятий по планированию разработки и внедрения ИКТ в деятельности государственных органов, основной формой реализации которых выступает экспертиза документов, используемых в рамках планирования, создания и использования ИКТ в деятельности государственных органов.

В целях обеспечения прозрачности процедуры привлечения средств федерального бюджета на реализацию мероприятий в сфере использования ИКТ в деятельности государственных органов устанавливается, что документы, используемые в рамках планирования, создания и использования ИКТ в деятельности государственных органов, в том числе документы, связанные с созданием государственных информационных систем (мероприятия по информатизации), перед их утверждением в установленном порядке подлежат экспертизе.

Предметом экспертизы является определение целесообразности и эффективности привлекаемых финансовых средств, качества предлагаемых технологических решений и их соответствия нормативным правовым актам в области формирования единых правил и подходов к системной организации и реализации процесса внедрения современных ИКТ в деятельность государственных органов, в том числе с учетом уже проводимых в государственных органах мероприятий по информатизации.

Полномочия по организации проведения указанной экспертизы, в частности, утверждение состава экспертной комиссии, определение срока проведения экспертизы, подписание заключений экспертизы, возлагаются на Минкомсвязь России как федеральный орган исполнительной власти, осуществляющий функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере ИКТ.

Организация и проведение экспертизы будут осуществляться с использованием автоматизированной информационной системы.

Технология оценки документов, направляемых на экспертизу (включая перечень нормативных документов, на соответствие которым будут проверяться представляемые на экспертизу документы), требования, предъявляемые к экспертному заключению, права и обязанности экспертов, порядок использования автоматизированной информационной системы будут определяться в Методике проведения экспертизы документов, используемых в рамках планирования, создания и использования ИКТ в деятельности государственных органов, утверждаемой Минкомсвязь России.

Экспертные заключения Минкомсвязь России должны стать обязательным документом, необходимым для принятия в установленном порядке решения о выделении средств федерального бюджета на реализацию мероприятий по информатизации.

Государственные органы при размещении соответствующих заказов на поставки товаров, выполнение работ, оказание услуг для государственных нужд при реализации мероприятий по информатизации также должны учитывать экспертные заключения.

Меры повышения эффективности бюджетных расходов на внедрение ИКТ

Системные меры задают основные требования к процессу планирования и расходования бюджетных средств на внедрение ИКТ, типовые ведомственные меры обеспечивают прозрачность контроля и учета ведомственных расходов на внедрение ИКТ.

Системные меры

1. Увязка процессов создания и регистрации государственных ИС с процессами бюджетного планирования и исполнения бюджета.
2. Оптимизация межбюджетных трансфертов по предоставлению государственных услуг в электронном виде в рамках реализации переданных на реализацию федеральных полномочий.
3. Нормативное закрепление жизненного цикла информационных систем электронного правительства. Закрепление типов государственных контрактов на разработку и внедрение ИС, находящихся на разных жизненных этапах с учетом перехода на федеральную контрактную систему.
4. Внедрение единого порядка координации государственных закупок в сфере ИКТ, включающего единую методологию установления начальной цены государственного контракта на основе нормативов и/или лучших практик, а также систему контроля и мониторинга эффективности работы государственного заказчика.
5. Ограничение расходов на разработку и внедрение ИС, связанных с поддержкой обеспечивающих функций органов государственной власти. Переход на свободное программное обеспечение для реализации обеспечивающих функций и в части общесистемного программного обеспечения.
6. Переход к исключительно программно-целевому принципу управления расходами на создание ИС

Типовые ведомственные меры

1. Утверждение типовой целевой программы ведомства по переводу государственных услуг в электронный вид, включающей в себя реализацию сводного плана ведомства по переводу предоставления государственных услуг и исполнению государственных функций в электронном виде в рамках установленных законодательством объемов бюджетных ассигнований.
2. Снятие функций государственного заказчика по разработке и ведению ИС с подведомственных учреждений.
3. Передача по конкурсу на исполнение функций по сопровождению и техническому обеспечению внедренных ИС негосударственным организациям.
4. Созданий центров компетенций по внедрению ИКТ.
5. Внедрение механизмов финансового менеджмента в части управления расходами на внедрение ИКТ в рамках реализации мероприятий программы Правительства Российской Федерации по повышению эффективности бюджетных расходов.

Целевые индикаторы мероприятий по повышению эффективности бюджетных расходов

Системный уровень

- Доля расходов на разработку и внедрение ИС органами государственной власти, осуществляемых по программно-целевому принципу.
- Удельные расходы (стоимость одного рабочего места пользователя) при внедрении ИС (по типам государственных полномочий), связанных с реализацией основных государственных функций (предоставлением государственных услуг).

- Доля используемых ИС органа государственной власти, зарегистрированных в установленном порядке.
- Наличие в сети Интернет актуального информационного ресурса, содержащего статистику расходов на средства ИКТ по федеральным органам исполнительной власти (телекоммуникационная инфраструктура, зарегистрированные информационные системы).

Типовые ведомственные меры

- Сравнительная статистика расходов на разработку, внедрение и сопровождение зарегистрированных ИС (по этапам жизненного цикла ИС) в разрезе государственных полномочий.
- Доля сотрудников органа государственной власти, прошедших переподготовку (повышение квалификации) в рамках программ по обучению использованию современных средств ИКТ.
- Доля процессов обеспечивающей административно-управленческой деятельности, совершаемых с помощью автоматизированных информационных систем.

Бюджетирование расходов на перевод в электронный вид процессов реализации государственных полномочий

1. Перечень планируемых к созданию в очередном периоде федеральных государственных информационных систем закрепляется в нормативном правовом акте Правительства Российской Федерации. Данный нормативный правовой акт отражается в реестре расходных обязательств каждого из ведомств-участников как отдельное расходное обязательство.
2. Минфин России выделяет один вид расходов «Информационное обеспечение перехода к предоставлению государственных услуг в электронном виде» с указанием необходимости отражения по данному коду всех расходов, связанных с разработкой и внедрением ИС. Альтернативным способом может стать закрепление отдельной целевой статьи расходов для каждого ведомства для ВЦП «Переход к предоставлению государственных услуг в электронном виде».
3. В обоснованиях бюджетных ассигнований ведомства-участники отражают расходы на соответствующие ИС как отдельное бюджетное ассигнование с указанием согласованных с Минкомсвязи России показателей непосредственного и конечного результата.
4. Сведения Реестра федеральных государственных информационных систем используется Минфином России при принятии решений о выделении средств на создание и внедрение информационных систем для оценки обоснованности запрашиваемых объемов финансирования, а также контролирующими органами при проведении проверок. В бюджетном учете расходы на создание, внедрение и эксплуатацию ИС предлагается отражать отдельно.
5. Эффективность перевода государственных услуг в электронный вид рассматривается как степень надлежащего функционирования и востребованности запланированных электронных сервисов по стадиям электронного взаимодействия при условии соблюдения обоснованного объема расходов. В качестве методики расчета степени эффективности бюджетных расходов целесообразно применить вариант определения соответствующих показателей эффективности, утвержденный для оценки карт проектов по реализации Основных направлений деятельности Правительства Российской Федерации на период до 2012 г.

9. Управление формированием электронного правительства

Система управления формированием электронного правительства направлена на достижение установленных целевых индикаторов и реализацию соответствующих мероприятий с максимально эффективным использованием государственных ресурсов.

Планирование и координация деятельности по формированию электронного правительства

Создание электронного правительства предполагает реализацию большого числа ведомственных, региональных, межбюджетных и межведомственных проектов. В связи с этим целесообразно использовать следующий подход к планированию:

- разработать и утвердить государственную программу по созданию информационного общества, сформировать соответствующие разделы в иных программах, находящихся в стадии разработки (согласования), осуществить краткосрочное и среднесрочное планирование необходимых мероприятий на основе целевых программ в составе указанной долгосрочной целевой программы;
- в соответствии с положениями настоящего системного проекта разработать и утвердить технические проекты на создание информационных систем электронного правительства;
- разработать и утвердить программу Правительства Российской Федерации по формированию и поддержке инфраструктуры электронного правительства на региональном уровне, предусмотрев:
 - определение порядка управления и использования информационных и телекоммуникационных систем как объектов государственного имущества Российской Федерации,
 - создание механизмов финансирования расходов, связанных с содержанием указанных объектов;
- завершить ревизию нормативной правовой базы, разработать новые и внести необходимые изменения в действующие нормативные правовые акты в части обеспечения прав заявителей при обращении за получением результата государственной услуги с помощью ИКТ, обеспечении реализации государственных полномочий с помощью ИКТ;
- увязать процессы регистрации и учета государственных информационных систем электронного правительства с процессами бюджетного планирования и исполнения бюджета;
- провести ревизию унаследованных информационных систем на основе данных сформированного реестра федеральных государственных информационных систем, разработать проекты по созданию (модернизации) отдельных компонентов электронного правительства («электронный регион», «электронное здравоохранение», «электронное правосудие» и др.);
- разработать организационно-методическую схему проведения регулярного мониторинга эффективности и результативности создания и использования инфраструктуры электронного правительства для целей предоставления государственных услуг (исполнения государственных функций).

Нормативное закрепление полномочий, функций и ответственности, связанных с формированием электронного правительства

Для успешной реализации положений настоящего системного проекта необходимо четко разграничить права и ответственность всех органов государственной власти, обеспечив

согласованность действий и максимально эффективное использование ресурсов государства.

Текущее состояние системы управления формированием электронного правительства

В настоящее время в Российской Федерации функции планирования, координации и выполнения отдельных мероприятий по формированию электронного правительства распределены по ряду ведомств, а также частично возложены на специально созданные координационные и совещательные органы.

Координаторами процесса формирования электронного правительства является Министерство связи и массовых коммуникаций Российской Федерации и Министерство экономического развития Российской Федерации, отвечающие за постановку задач и контроль их исполнения, обеспечивающие регулируемую и нормотворческую функции в данной сфере. Основой для объединения усилий двух координационных органов Правительства являются распоряжение Правительства Российской Федерации от 03 декабря 2009 г. №1862-р «Об утверждении плана мероприятий по совершенствованию государственного управления в 2009-2010 гг.» и распоряжение Правительства Российской Федерации № 1555-р от 17 октября 2009 г. (перевод государственных услуг в электронный вид).

Заказчиками по отдельным проектам являются федеральные органы исполнительной власти и субъекты Российской Федерации.

В целях организации взаимодействия федеральных органов исполнительной власти, субъектов Российской Федерации, а также обеспечения принятия согласованных решений с учетом позиций указанных субъектов, создана Правительственная комиссия по внедрению информационных технологий в деятельность государственных органов и органов местного самоуправления. Данная Правительственная комиссия обладает наиболее широкими полномочиями в сфере информатизации. В ее состав функционально входят Совет главных конструкторов по использованию информационно-коммуникационных технологий в деятельности федеральных органов исполнительной власти (представители федеральных органов власти) и Совет по региональной информатизации (представители субъектов Российской Федерации).

На региональном уровне формируются координационные органы, ответственные за решение вопросов реализации административной реформы и информатизации субъекта.

Целевое состояние структуры управления

Целесообразно выделить три уровня управления формированием электронного правительства: уровень общей координации, уровень управления «по направлениям», ведомственный уровень.

На верхнем уровне общей координации должно осуществляться средне- и долгосрочное планирование работ, а также оценка эффективности работ. На уровне «управления по направлениям» должны решаться задачи нормативного, методического и финансового обеспечения процессов формирования электронного правительства. Конечный перечень направлений должен быть установлен Советом при Президенте Российской Федерации по развитию информационного общества в Российской Федерации. На ведомственном уровне должно осуществляться управление конкретными проектами (см. рисунок 9.1).

Частно-государственное партнерство

Основным направлением частно-государственного партнерства является создание электронных сервисов, основанных на раскрываемой государством общедоступной

информации. Данные сервисы должны предоставлять пользователям дополнительные возможности поиска, обработки и использования информации.

Управление проектами по формированию электронного правительства

Независимая экспертиза проектов в сфере ИКТ

Организация экспертизы должна предусматривать обязательную публикацию проектной документации и отчетов о реализации проектов, за исключением информации, относящейся к государственной тайне. Результаты экспертизы должны публиковаться в открытом доступе для анализа после окончания срока выполнения проекта. Процедуры экспертизы должны быть формализованы и конкретны, они не должны подменять собой процедуры межведомственного согласования.

Обеспечение методической поддержки, создание центров компетенций для государственных служащих

Опыт формирования электронного правительства в России практически отсутствует, а зарубежный опыт в силу различных обстоятельств не всегда применим. Поэтому особое значение имеет создание центров сбора положительного опыта, полученного при формировании электронного правительства. Такие центры должны обеспечивать распространение лучших практик, типовых документов, типового программного обеспечения, методических и образовательных материалов, на их базе может осуществляться консультационная поддержка государственных служащих.

Кадровое обеспечение формирования электронного правительства

Повышенные требования к уровню квалификации необходимы:

- при разработке базовых элементов информационно-технологической инфраструктуры и нормативной правовой базы электронного правительства;
- при проектировании перехода к реализации государственных полномочий с использованием ИКТ; разработке соответствующей нормативной правовой базы;
- при реализации конкретных государственных полномочий с использованием ИКТ.

Необходимо предусмотреть:

- проведение научно-исследовательских работ в области совершенствования специального, высшего профессионального и последипломного образования с учетом специфики государственной и муниципальной службы;
- проведение массового краткосрочного повышения квалификации государственных и муниципальных служащих;
- распространение лучших практик, в том числе путем проведения конференций.

Разработка и внедрение механизмов повышения мотивации государственных служащих и других участников проектов

Целесообразно предусмотреть разработку механизмов стимулирования государственных служащих, участвующих в реализации государственных полномочий с использованием ИКТ. Такими механизмами могут стать:

- распределение части средств, выделяемых на разработку и внедрение ИКТ при реализации государственных полномочий, на премирование служащих, участвующих в реализации государственных полномочий с использованием ИКТ;

- сохранение общего объема фонда заработной платы ведомства (структурного подразделения), часть служащих которого была высвобождена в результате перехода к реализации государственного полномочия с использованием ИКТ;
- установление запрета на финансирование ведомством каких-либо работ, в т. ч. научно-исследовательских, связанных с проектированием, разработкой и внедрением информационных систем, при наличии невыполненных обязательств по утвержденному плану-графику перехода к реализации государственных полномочий с использованием ИКТ.

Совет при Президенте России по развитию информационного общества	Правительство РФ		Федеральные органы исполнительной власти		
	Правительственная комиссия по административной реформе	Правительственная комиссия по внедрению ИТ	Минкомсвязи России	Минэкономразвития России	Министерства и ведомства
В целом по формированию электронного правительства					
Стратегическая координация, определение полномочий, оценка эффективности	Оптимизация состава полномочий, структуры ФОИВ	Координация создания инфраструктуры ЭП, мониторинг эффективности	Организация мероприятий по формированию ЭП	Координация работ по изменению законодательства	Ведомственные мероприятия по формированию ЭП
Перевод в электронную форму полномочий федеральных органов исполнительной власти					
Стратегическая координация, определение полномочий, оценка эффективности	Перечень государственных услуг (функций) переводимых в электронный вид, определение их целевого состояния	Рассмотрение пакетов нормативных правовых актов для закрепления электронных форм документов	Обеспечение юридической значимости электронного взаимодействия, Общая поддержка Портала госуслуг	Подготовка проектов изменений в федеральное законодательство и подзаконные акты	Перевод государственных функций (услуг) в электронный вид, поддержка ведомственных разделов на Портале госуслуг
Перевод в электронный вид государственной учетной деятельности					
Стратегическая координация, определение полномочий, оценка эффективности	Требования к порядку осуществления государственной учетной деятельности	Приоритетность создания электронных учетных систем	Создание и ведение реестра государственных учетных систем	Изменение законодательства для перевода учетных полномочий в электронный вид	Приведение учетной деятельности к требованиям регулирования
Обеспечение доступности государственных услуг					
Стратегическая координация, определение полномочий, оценка эффективности	Требования по обеспечению доступности государственных услуг	Требования к ИС, обеспечивающим доступность государственных услуг	Контроль исполнения требований законодательства, методическая поддержка	Изменение законодательства для обеспечения доступности государственных услуг	Исполнение плана обеспечения доступности государственных услуг
Развитие информационно-технологических и инженерных компонентов электронного правительства					
Стратегическая координация, определение полномочий, оценка эффективности	Обеспечение увязки бюджетных расходов с целевыми характеристиками ИС	Определение требований к ИТ-компонентам ЭП, Решения о создании ИС, их характеристиках	Установление требований к ИТ-компонентам ЭП, Создание и ведение реестра государственных ИС	Мониторинг использования государственных ресурсов при предоставлении государственных услуг	Исполнение плана развития ИТ-компонентов ЭП, Предоставление данных для внесения в реестр государственных ИС
Формирование инфраструктуры электронного правительства					
Стратегическая координация, определение полномочий, оценка эффективности	Требования к порядку отнесения государственных ИС к инфраструктурным	Решения о разработке инфраструктурных систем, их характеристиках	Изменение законодательства для формирования правовой базы функционирования инфраструктурных ИС	Мониторинг эффективности использования инфраструктуры ЭП	Исполнение плана формирования инфраструктуры ЭП
Обеспечение эффективности бюджетных расходов					
Контроль целевого использования бюджетных средств на внедрение ИКТ	Проект закрепления единого механизма планирования, управления и учета расходов на внедрение ИКТ	Разработка стимулов повышения эффективности бюджетных расходов на внедрение ИКТ	Увязка учета государственных ИС с бюджетным планированием, Единый порядок координации госзакупок в сфере ИКТ	Учета ИС и объектов ИКТ-инфраструктуры ЭП как имущества РФ, Переход к программно-целевому принципу управления расходами на создание ИС	Утверждение целевой программы по переводу государственных услуг в электронный вид

Рисунок 9.1. Проект распределения управленческих функций по направлениям формирования электронного правительства.

Оценка эффективности деятельности по формированию электронного правительства

Оценка качества государственного управления

Наиболее авторитетные международные индексы качества государственного управления составляют Всемирный банк, международная неправительственная организация Transparency International и Всемирный экономический форум.

Индексы развития информационного общества

Индекс готовности стран к сетевому миру (Network Readiness Index) поддерживается Всемирным экономическим форумом совместно с бизнес-школой INSEAD. Рейтинг публикуется ежегодно с 2000 г. и содержит информацию о 134 странах.

Рейтинг готовности стран к электронному правительству ООН составляется ежегодно. Он формируется на основе трех индексов. Индекс развития государственных веб-сайтов составляется по результатам обследования сайтов правительства и пяти основных министерств (образования, здравоохранения, социальной защиты, труда и финансов). Индекс развития телекоммуникационной инфраструктуры оценивает интегральную доступность основных телекоммуникационных услуг населению страны (проникновение фиксированной и мобильной телефонной связи, сети Интернет, телевидения). Для расчета индекса развития человеческого капитала используются данные ЮНЕСКО и Программы развития ООН.

Для указанных выше двух групп индексов необходимо:

- определить целевые показатели для России по каждому из перечисленных индексов на период с 2010 по 2015 г.;
- определить уполномоченный орган, ежегодно докладывающий в Правительство Российской Федерации о показателях России по каждому из указанных индексов.

Оценка качества и доступности государственных услуг

В отличие от интегральных международных индексов качества государственного управления и степени развития информационного общества, характеризующих страну в целом, единых методик оценки доступности государственных услуг в мире не существует.

Систематическая оценка качества и доступности конкретных государственных услуг, предоставляемых в электронном виде, является условием эффективной деятельности по формированию электронного правительства. Мониторинг качества и доступности государственных услуг должен осуществляться в соответствии с методикой мониторинга, утвержденной постановлением Правительства Российской Федерации. Методика должна предусматривать отсутствие у органов, осуществляющих мониторинг, конфликта интересов. Результаты мониторинга подлежат обязательной публикации.

Оценки выполнения утвержденных планов формирования электронного правительства

Инструментами оценки целевых показателей являются:

- Ежегодный мониторинг перехода к предоставлению государственных услуг в электронной форме.
- Ежегодный мониторинг качества и доступности электронных государственных услуг, а также успешности перехода к реализации контрольно-надзорных полномочий в электронной форме, проводимый на основе «контрольных закупок», анализа мнений граждан и организаций.

- Ежегодный мониторинг интенсивности использования ИКТ путем отслеживания и учета случаев обращения к информационным системам органов власти в рамках реализации государственных полномочий.
- Ежегодный мониторинг соответствия электронных учетных систем в федеральных органах исполнительной власти требованиям нормативной правовой базы.
- Ежегодный мониторинг соответствия информационных систем электронного правительства требованиям нормативной правовой базы.

После отработки соответствующих методик указанные ежегодно проводимые мониторинговые обследования должны быть закреплены в федеральном плане статистических наблюдений Росстата. Наряду с этим целесообразно поддерживать следующие механизмы «обратной связи»:

- «Горячая линия» с получателями результатов реализации государственных полномочий с использованием ИКТ.
- Регулярные отчеты ведомств о переходе к реализации государственных полномочий с использованием ИКТ, содержащие, в том числе, сведения об организации и функционирования ведомственной системы контроля за реализацией ведомством государственных полномочий с использованием ИКТ.

Результаты мониторинга, а также отчеты ведомств подлежат обязательной публикации.

Целевые показатели формирования электронного правительства

Целевые показатели формирования электронного правительства приведены в таблицах 9.1-9.8:

Таблица 9.1. Целевые значения показателей перевода в электронный вид разрешительных полномочий федеральных органов исполнительной власти.

Показатели	2010		2011	2012
	Июнь	Дек.		
Инвентаризация и нормативное закрепление перечня разрешительных полномочий для перевода в электронную форму	выполнено			
Доля разрешительных полномочий, по которым реализован 1 этап	90 %	100%		
Доля разрешительных полномочий, по которым реализован 2 этап	10%	50%	100%	
Доля разрешительных полномочий, по которым реализован 3 этап		5%	25%	50%
Доля разрешительных полномочий, по которым реализован 4 этап			10%	20%
Доля разрешительных полномочий, по которым реализован 5 этап				10%

Таблица 9.2. Целевые значения показателей перевода в электронный вид контрольно-надзорных полномочий федеральных органов исполнительной власти.

Показатели	2010		2011	2012
	Июнь	Дек.		
Инвентаризация и нормативное закрепление перечня полномочий, связанных с проверками, для перевода в электронную форму	выполнено			
Доля полномочий, по которым реализован 1 этап		90%	90%	99%
Доля полномочий, по которым реализован 2 этап		50%	60%	70%
Доля полномочий, по которым реализован 3 этап			10%	50%

Таблица 9.3. Целевые показатели приведения учетной деятельности федеральных органов исполнительной власти к требованиям законодательства, на период до 2012 г.

Показатели	2010		2011	2012
	Июнь	Дек.		
Инвентаризация и нормативное закрепление учетных полномочий федеральных органов исполнительной власти	выполнено			
Доля учетных систем, соответствующих требованиям к электронным учетным системам		20%	30%	80%
Доля учетных систем, содержащих общедоступную информацию, информация из которых раскрыта на официальных сайтах органов власти		50%	60%	100%

Таблица 9.4. Целевые значения показателей формирования информационно-технологических и инженерных компонентов электронного правительства на период до 2012 г.

Показатели	2010		2011	2012
	Июнь	Дек.		
Инвентаризация унаследованных информационно-технологических и инженерных компонентов электронного правительства	выполнено			
Приведение государственных информационных систем в соответствие требованиям к государственным информационным системам		10%	50%	70%

Таблица 9.5. Целевые значения показателей, связанных с формированием инфраструктуры обеспечения юридически-значимого электронного взаимодействия

Показатели	2010		2011	2012
	Июнь	Дек.		
Формирование единого домена доверия	Корневой УЦ	20 УЦ	50 УЦ	100 УЦ
Количество удаленных юридически-значимых транзакций, осуществляемых в рамках реализации государственных полномочий (не включая внутриведомственное взаимодействие)	Оценка актуального состояния	+50%	+100%	+100%

Таблица 9.6. Целевые значения показателей, связанных с формированием инфраструктуры обеспечения совместимости государственных информационных систем

Показатели	2010		2011	2012
	Июнь	Дек.		
Создание реестра схем данных	Выполнено			
Количество схем данных, внесенных в реестр		5	20	70
Создание реестра стандартизированных спецификаций	Выполнено			
Доля государственных информационных систем, соответствующих требованиям к интерфейсам информационных систем	10%	20%	50%	80%

Таблица 9.7. Целевые значения показателей обеспечения доступности государственных услуг

Показатели	2010		2011	2012
	Июнь	Дек.		
Изменение удовлетворенности граждан и организаций качеством государственных услуг (включая связанные с контрольно-надзорной деятельностью органов власти)	Оценка актуального состояния	+10%	+30%	+50%
Снижение сроков ожидания результата предоставления услуги	Устанавливается для каждой услуги (функции)			
Снижение времени личного присутствия в органе власти, предоставляющем услугу.	Устанавливается для каждой услуги (функции)			

Таблица 9.8. Целевые значения показателей повышения эффективности бюджетных расходов

Показатели	2010		2011	2012
	Июнь	Дек.		
Доля осуществляемых по программно-целевому принципу расходов на разработку и внедрение	5%	5%	15%	25%

информационных систем органами государственной власти				
Доля информационных систем органов государственной власти, зарегистрированных в установленном порядке	1%	10%	50%	75%
Наличие в сети Интернет обновляемого информационного ресурса, содержащего статистическую информацию о расходах на средства ИКТ по федеральным органам исполнительной власти (телекоммуникационная инфраструктура, зарегистрированные информационные системы)			Выполнено	
Наличие в служебных контрактах и должностных регламентах государственных служащих показателей результативности, связанных с использованием информационно-коммуникационных технологий			Выполнено	
Доля служащих органа государственной власти, прошедших переподготовку (повышение квалификации) в рамках программ по обучению использования современных средств ИКТ			5%	20%
Доля процессов обеспечивающей административно-управленческой деятельности, совершаемых с помощью автоматизированных информационных систем		10%	30%	50%

10. Заключительные положения

В системном проекте содержатся и раскрыты в достаточной мере следующие положения:

- место и роль электронного правительства в макросистеме информационного общества РФ;
- границы электронного правительства и взаимосвязи его основных компонентов;
- система управления формированием электронного правительства и меры по повышению ее эффективности;
- основы информационно-технической политики формирования инфраструктуры электронного правительства и направления работ, необходимые и достаточные для создания электронного правительства в заданные Правительством РФ сроки;
- характеристика текущего и целевого состояния по основным направлениям;
- анализ рисков, предложения по составу и содержанию мероприятий с указанием критичных мер по каждому направлению;
- система мониторинга на основе целевых показателей эффективности процесса формирования электронного правительства.

Таким образом, настоящий документ обеспечивает возможности целенаправленного управления процессом формирования электронного правительства, эффективной координации усилий заинтересованных органов исполнительной власти и организаций, а также осуществления дальнейшего планирования работ по основным направлениям формирования электронного правительства.