Глава 1. Информационное общество в Российской Федерации

§ 1.1. История становления и развития информационного общества в России

Термин «информация» происходит от латинского «informatio», что означает разъяснение, осведомление, изложение. С рационалистической позиции информация есть отражение реального мира с помощью сообщений. Сообщение – это форма представления каких-либо сведений в виде речи, текста, изображения, цифровых данных, графиков, таблиц и т. п.

В статье 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» содержится следующее определение: информация – сведения (сообщения, данные) независимо от формы их представления[1].

Становление любого информационного общества берет свое начало с момента фиксации информации на каком-либо носителе с целью ее сохранения и возможности передачи. Постепенное развитие технологий совершенствовало процесс хранения, обработки и передачи информации, но с появлением вычислительной техники и развитием средств передачи данных ситуация изменилась кардинальным образом. Сейчас практически невозможно представить общество без современных средств связи, несмотря на то, что в массовый обиход они вошли сравнительно недавно.

Особую актуальность тема «информационного общества» обрела в 1990-е годы с развитием так называемой «новой экономики», «экономики знания», «цифровой экономики» и т. п. Понятие «информационное общество» приобрело новый статус после принятия в 2000 году странами «Большой восьмерки» документа под названием «Окинавская хартия глобального информационного общества»[2]. Термин «информационное общество» был использован для обозначения цели, которая может быть достигнута в ходе глобального освоения информационно-коммуникационных технологий (ИКТ). Результатом этого глобального процесса станет обеспечение устойчивого экономического роста, повышение общественного благосостояния, укрепление социального согласия, реализация потенциала большинства стран мира в области развития демократии и, в конечном счете, обеспечение международной стабильности и ответственного управления в мировом сообществе.

---

[1] Об информации, информационных технологиях и о защите информации: Федер. закон Рос. Федерации от 27 июля 2006 г. № 149-ФЗ: ред. от 13 июля 2015 г . // Рос. газ. 2006. 29 июля. № 165.

[2] Окинавская хартия глобального информационного общества: принята на о. Окинава 22 июля 2000 г. // Дипломатический вестник. 2000. № 8. С. 51 – 56.

Информатизация общества – это глобальный социальный процесс, особенность которого состоит в том, что доминирующим видом деятельности в сфере общественного производства являются сбор, накопление, обработка, хранение, передача и использование информации, осуществляемые на основе современных средств вычислительной техники, а также на базе разнообразных средств информационного обмена.

В деятельности органов власти по разработке и реализации государственной политики в области развития информационного общества в России можно выделить несколько этапов.

На первом этапе (1991 – 1994 гг.) формировались основы в сфере информатизации.

Второй этап (1994 – 1998 гг.) характеризовался сменой приоритетов от информатизации к выработке информационной политики.

Третий этап (1998 г. – настоящее время) связан с формированием политики в сфере построения информационного общества.

В 2002 году Правительством Российской Федерации была принята Федеральная целевая программа «Электронная Россия 2002 – 2010 гг.», которая дала мощный толчок развитию информационного общества в российских регионах. В рамках программы формировались стандарты в сфере ИКТ, создавались методическая основа и рекомендации по совершению сделок в электронной форме, начата работа по обеспечению систематического представления информации федеральных органов исполнительной власти в сети Интернет, также начата реализация опытных проектов по предоставлению информационных услуг гражданам органами государственной власти субъектов Российской Федерации через федеральную государственная информационную систему «Единый портал государственных и муниципальных услуг (функций)».

С целью обеспечения единой технологической и телекоммуникационной инфраструктуры информационного взаимодействия существующих и создаваемых государственных и муниципальных информационных систем и иных информационных систем, участвующих в процессах оказания государственных и муниципальных услуг, предоставляемых в электронном виде, а также обеспечения функционирования государственных информационно-аналитических систем Минкомсвязью России создана единая система межведомственного электронного взаимодействия.

В 2008 году была разработана Стратегия развития информационного общества в Российской Федерации[3], в ней определена национальная стратегия, в значительной степени влияющая на развитие нормативного правового регулирования в процессах становления информационного общества. Стратегия представляет собой политический документ, разработанный с

[3] Стратегия развития информационного общества в Российской Федерации: утв. Президентом Рос. Федерации 7 февраля 2008 г. № Пр-212 // Рос. газ. 2008. 16 февр. № 34.

учетом международных актов, который закрепляет цель, принципы и основные направления государственной политики в области использования и развития информационных и телекоммуникационных технологий, науки, образования и культуры для движения страны к современному информационному обществу.

Помимо этого, Стратегия является основой для подготовки и уточнения концептуальных, доктринальных, программных и иных документов, определяющих цели и направления деятельности органов государственной власти, и устанавливает принципы и механизмы их взаимодействия с гражданским обществом в области развития информационного общества в России.

Стратегия подготовлена с учетом международных обязательств Российской Федерации, Доктрины информационной безопасности Российской Федерации, федеральных законов, а также нормативных правовых актов Правительства Российской Федерации, определяющих направления социально-экономического развития, повышения эффективности государственного управления и взаимодействия органов государственной власти и гражданского общества в Российской Федерации.

В Стратегии учтены основные положения Окинавской хартии глобального информационного общества и других международных документов, принятых на высшем уровне, по вопросам развития информационного общества.

Реализация стратегических мероприятий предусматривается по следующим основным направлениям:

1. В области формирования современной информационной и телекоммуникационной инфраструктуры, предоставления на ее основе качественных услуг в сфере информационных и телекоммуникационных технологий и обеспечения высокого уровня доступности для населения информации и технологий, в частности, путем:

– повышения доступности для населения и организаций современных услуг в сфере информационных и телекоммуникационных технологий;

– формирования единого информационного пространства, в том числе для решения задач обеспечения национальной безопасности;

– модернизации системы телерадиовещания, расширения зоны уверенного приема российских телерадиопрограмм;

– предоставления гражданам с низким уровнем доходов льгот и компенсаций на пользование услугами связи, приобретение пользовательских устройств и программного обеспечения, необходимого для получения данных услуг;

– создания системы общественных центров доступа населения к государственным информационным ресурсам, включая создание государственной системы правовой информации.

2. В области повышения качества образования, медицинского обслуживания, системы социальной защиты населения на основе развития и использования информационных и телекоммуникационных технологий посредством:

– расширения использования информационных и телекоммуникационных технологий для развития новых форм и методов обучения, в том числе дистанционного образования;

– внедрения новых методов оказания медицинской помощи населению, а также дистанционного обслуживания пациентов;

– предоставления гражданам социальных услуг на всей территории Российской Федерации с использованием информационных и телекоммуникационных технологий.

3. В области совершенствования системы государственных гарантий конституционных прав человека и гражданина в информационной сфере – путём развития законодательных механизмов.

Направления реализации стратегии развития информационного общества в России определены также в областях:

– развития экономики Российской Федерации на основе использования информационных и телекоммуникационных технологий;

– повышения эффективности государственного управления и местного самоуправления, качества и оперативности предоставления государственных услуг, взаимодействия гражданского общества и бизнеса с органами государственной власти;

– развития науки, технологий, техники и подготовки квалифицированных кадров в сфере информационных и телекоммуникационных технологий;

– сохранения культуры многонационального народа Российской Федерации, укрепления нравственных и патриотических ценностей в общественном сознании, развития системы культурного и гуманитарного просвещения;

– противодействия угрозам использования потенциала информационных и телекоммуникационных технологий для нанесения ущерба национальным интересам России.

В связи с процессами глобализации важное значение в стратегии уделено вопросам международного сотрудничества в области развития информационного общества. К основным направлениям реализации стратегии в рамках международного сотрудничества в этой области развития информационного общества относится участие:

– в разработке международных норм права и механизмов, регулирующих отношения в области использования глобальной информационной инфраструктуры, включая вопросы интернационализации управления сетью Интернет;

– в международном информационном обмене;

– в формировании системы международной информационной безопасности, совершенствовании взаимодействия правоохранительных органов Российской Федерации и иностранных государств в области предупреждения, выявления, пресечения и ликвидации последствий использования информационных и телекоммуникационных технологий в террористических и иных преступных целях;

– в международных исследовательских проектах по приоритетным направлениям развития науки, технологий и техники;

– в разработке международных стандартов в сфере информационных и телекоммуникационных технологий, гармонизации национальной системы стандартов и сертификации в этой сфере с международной системой.

На основании Стратегии развития информационного общества и Концепции долгосрочного социально-экономического развития до 2020 года была разработана государственная программа «Информационное общество (2011 – 2020 годы)»[4]. Она охватывает все отрасли и сферы деятельности и должна повысить его прозрачность и управляемость, обеспечить устойчивость и конкурентоспособность экономики в целом. Работа ведется по множеству направлений: созданию электронного правительства, преодолению цифрового неравенства, развитию новых технологий связи.

Основной принцип программы: результаты должны приносить реальную, ощутимую пользу людям. Повышение качества жизни должно выражаться в простых и доступных сервисах, которыми граждане пользуются почти ежедневно (запись на прием к врачу через Интернет, оплата штрафов с мобильного телефона и т. д.).

Цели и задачи Госпрограммы – повышение качества жизни граждан на основе использования информационных и телекоммуникационных технологий; обеспечение предоставления гражданам и организациям услуг с использованием современных информационных и телекоммуникационных технологий; развитие технической и технологической основы становления информационного общества; предупреждение угроз, возникающих в информационном обществе.

Показателями успешной реализации Программы станут рост индекса Российской Федерации в международном рейтинге стран по уровню развития информационных и телекоммуникационных технологий и увеличение числа граждан, использующих госуслуги в повседневной жизни. К 2020 году планируется увеличить долю населения, пользующегося электронными госуслугами, до 85 %.

---

[4] Об утверждении государственной программы Российской Федерации «Информационное общество (2011 – 2020 годы)»: Постановление Правительства Рос. Федерации от 15 апреля 2014 г. № 313 // Собр. законодательства Рос. Федерации. 2014. № 18 (часть II), ст. 2159.

Таким образом, в Российской Федерации в настоящее время активно идет процесс становления и развития информационного государства и общества посредством выполнения таких задач, как управление развитием информационного общества, развитие электронного правительства, повышение качества государственного управления за счёт создания и внедрения современных информационных технологий, услуг на основе информационных технологий в области медицины, здравоохранения и социального обеспечения, развитие сервисов на основе информационных технологий в области образования, науки и культуры, поддержка региональных проектов в сфере информационных технологий.

§ 1.2. Электронное правительство. Оказание государственных услуг в электронном виде и система межведомственного электронного взаимодействия (СМЭВ)

Реализация мероприятий по развитию электронного правительства Российской Федерации началась в 2002 году с принятием Федеральной целевой программы «Электронная Россия (2002 – 2010 годы)» и продолжилась в рамках государственной программы «Информационное общество (2011 – 2020 годы)».

Электронное правительство – это форма организации деятельности органов государственной власти, обеспечивающая качественно новый уровень оперативности и удобства получения организациями и гражданами государственных услуг и информации о результатах деятельности государственных органов за счет широкого применения информационно-коммуникационных технологий.

Основные принципы развития и использования электронного правительства:

ориентация на пользователя. Электронное правительство должно развиваться с ориентацией на потребности пользователей всех категорий путем их постоянного изучения в различных жизненных и деловых ситуациях, поэтому необходим анализ текущих и будущих требований и ожиданий пользователей, на основании которого электронное правительство будет способно сконцентрировать свои усилия на выполнении текущих требований потребителей и планировать свою деятельность, ориентируясь на их ожидания;

эффективность, включая социальную и экономическую. Информационные системы электронного правительства предоставляют возможности для эффективного решения задач государственного и муниципального управления, в том числе за счет его оптимизации, вовлечения в него граждан, поддержки открытого диалога государства с профессиональными и экспертными сообществами;

всеохватность. Электронное правительство может охватывать своими возможностями все ветви власти, уровни государственного управления и местного самоуправления, а также все виды организаций, включая самоорганизующиеся сообщества, все возрасты и группы населения для предоставления им услуг, удобных способов взаимодействия со службами электронного правительства и между собой, совместного использования информации, поддержки совместной деятельности;

безопасность и доверие. Действия пользователей электронного правительства и их данные защищаются; конфиденциальность, целостность и доступность к сведениям обеспечиваются таким образом, что устанавливается доверие между пользователем и электронным правительством, позво-

ляющее передавать и хранить персональную и иную конфиденциальную информацию;

гибкость и адаптивность. На фоне изменения технологий, социально-экономических условий, организационной и корпоративной культуры органов государственной власти и местного самоуправления электронному правительству требуются гибкость и своевременная реакция на эти изменения;

ориентация на юридические данные. Перестройка работы электронного правительства на основе использования юридически значимых данных позволит сократить межведомственный документооборот, количество услуг и документов обязательного хранения у граждан и организаций;

непрерывность функционирования. Данный принцип подразумевает устойчивость развития возможностей электронного правительства при изменении условий и внедрении новшеств, а также поддержание ранее заданных требований к открытости и оказанию государственных и муниципальных услуг.

Целями внедрения электронного правительства в Российской Федерации являются:

1. Предоставление высококачественных государственных и муниципальных услуг всем категориям пользователей в любое время, в любом месте, с различных устройств преимущественно в режиме реального времени.

2. Повышение обоснованности принимаемых управленческих решений, снижение издержек реализации функций и осуществления полномочий органов государственной власти и местного самоуправления, принятие управленческих решений преимущественно в режиме реального времени.

3. Возможность использования систем и сервисов электронного правительства для поддержки деятельности гражданского общества и бизнеса, вовлечения граждан в процессы государственного и муниципального управления.

Структура электронного правительства представлена на рисунке 1.2.1.

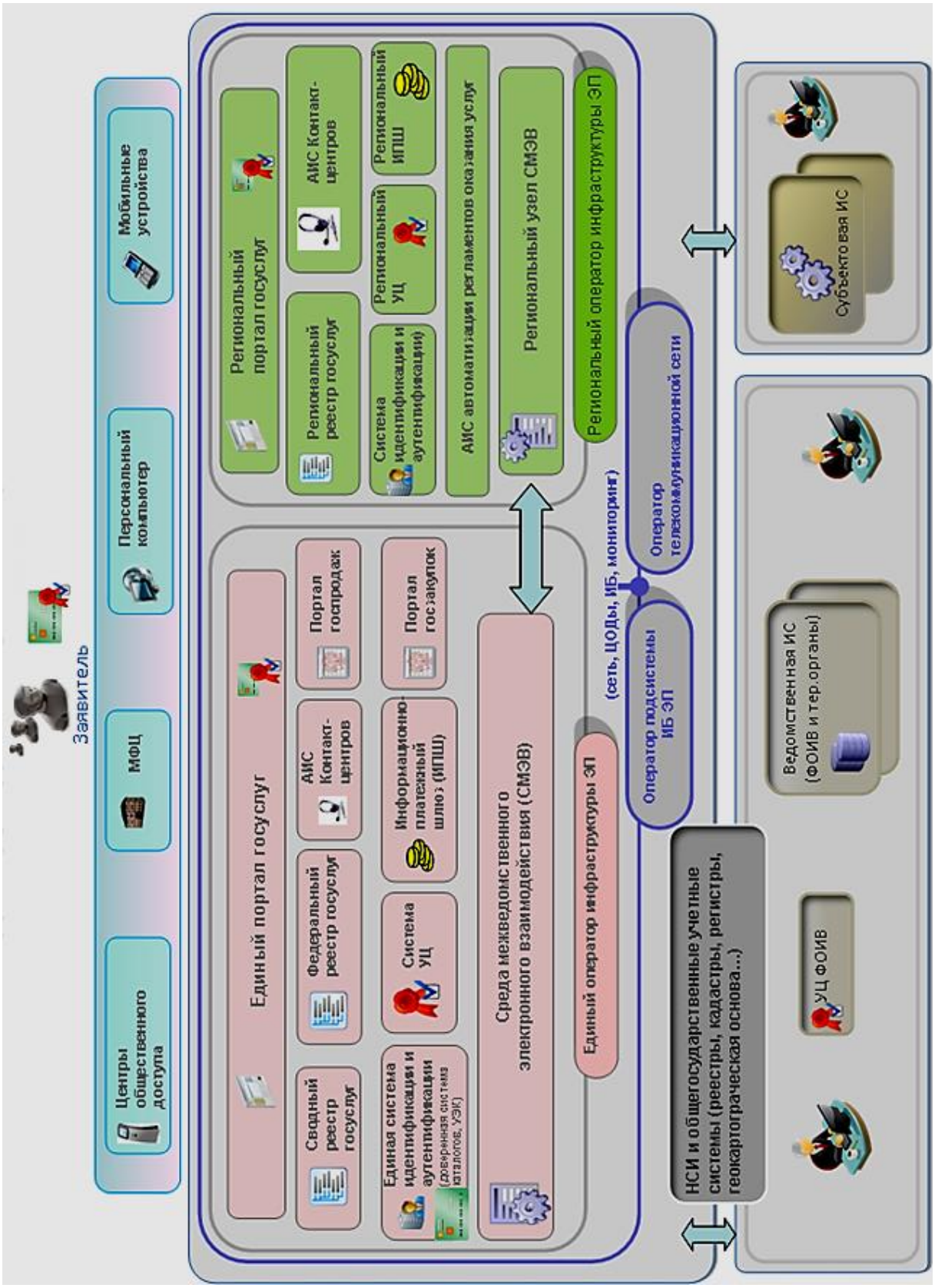

Рисунок 1.2.1. Структура электронного правительства.

Ключевыми элементами национальной инфраструктуры электронного правительства являются:

1. Единый портал государственных и муниципальных услуг (ЕПГУ).

Единый портал государственных и муниципальных услуг (функций) – это федеральная государственная информационная система, обеспечивающая:

– доступ физических и юридических лиц к сведениям о государственных и муниципальных услугах, государственных функциях по контролю и надзору, об услугах государственных и муниципальных учреждений, об услугах организаций, участвующих в предоставлении государственных и муниципальных услуг, размещенных в федеральной государственной информационной системе, обеспечивающей ведение реестра государственных услуг в электронной форме;

– предоставление в электронной форме государственных и муниципальных услуг в соответствии с перечнями, утвержденными Правительством Российской Федерации и высшими исполнительными органами государственной власти субъекта Российской Федерации;

– учет обращений граждан, связанных с функционированием Единого портала, в том числе возможность для заявителей оставить отзыв о качестве предоставления государственной или муниципальной услуги в электронной форме.

Информация на Едином портале государственных и муниципальных услуг (функций) размещается в течение одного рабочего дня из Сводного реестра государственных и муниципальных услуг (функций), формируемого федеральными и региональными органами власти Российской Федерации, органами местного самоуправления, которые несут ответственность за полноту и достоверность сведений об услугах (функциях).

Единый портал доступен любому пользователю информационно-телекоммуникационной сети Интернет и организован таким образом, чтобы обеспечить простой и эффективный поиск информации по государственным или муниципальным услугам.

На Едином портале реализована концепция «личного кабинета» пользователя, обеспечивающая после его регистрации на портале следующие возможности:

– ознакомление с информацией о государственной или муниципальной услуге (функции);

– обеспечение доступа к формам заявлений и иных документов, необходимых для получения государственной или муниципальной услуги (функции), их заполнение и представление в электронной форме;

– обращение в электронной форме в государственные органы или органы местного самоуправления;

– мониторинг хода предоставления государственной или муниципальной услуги или исполнения государственной функции;

– получение начислений и возможность оплаты государственных пошлин, штрафов и сборов;

– хранение реквизитов пользователя;

– получение результатов предоставления государственных или муниципальных услуг в электронной форме на Едином портале, если это не запрещено федеральным законом.

2. Федеральный реестр государственных услуг (ФРГУ).

Из федерального реестра государственных услуг, формируемого федеральными и региональными органами государственной власти Российской Федерации, органами местного самоуправления, которые несут ответственность за полноту и достоверность сведений об услугах (функциях), информация в течение одного рабочего дня размещается на Едином портале государственных и муниципальных услуг (функций).

3. Единая система нормативно-справочной информации (ЕСНСИ).

Единая система нормативно-справочной информации – федеральная государственная информационная система, которая предназначена для обеспечения единой точки доступа к справочной информации, используемой в государственных и муниципальных информационных системах, где все заинтересованные стороны (участники информационного взаимодействия) могут получить описание справочников/классификаторов, базовых государственных информационных ресурсов, а также их актуальные данные.

4. Единая система межведомственного электронного взаимодействия (СМЭВ).

Единая система межведомственного электронного взаимодействия – это федеральная государственная информационная система, предназначенная для организации информационного взаимодействия между информационными системами участников СМЭВ в целях предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме.

СМЭВ является комплексом программно-технических средств и информационных баз данных, выполняющих функцию регламентированной гарантированной передачи сообщений между подключенными к ней информационными системами государственных органов. Используемая при этом технология электронных сервисов позволяет объединить в единую сеть практически любые информационные системы независимо от времени их создания, программной платформы и структуры баз данных. Необходимо подчеркнуть, что СМЭВ – это полностью защищённая среда, обеспечивающая безопасность передаваемой информации от точки подключения отправителя сообщения до точки подключения его получателя.

СМЭВ функционирует на основе защищённой криптографическими средствами сети передачи данных.

Участниками межведомственного электронного взаимодействия являются федеральные органы исполнительной власти, государственные внебюджетные фонды, исполнительные органы государственной власти субъектов Российской Федерации, органы местного самоуправления, государственные и муниципальные учреждения, многофункциональные центры, иные органы и организации.

Целью создания СМЭВ является повышение качества предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций за счет использования общих информационных ресурсов, уменьшения времени на поиск и обработку информации в электронной форме.

Основными функциями системы взаимодействия являются:

– обеспечение передачи запросов, иных документов и сведений, необходимых для получения государственных и муниципальных услуг и поданных заявителями через единый портал в подключенные к системе взаимодействия информационные системы органов и организаций, обязанных предоставить запрашиваемые государственные (муниципальные) услуги;

– обеспечение обмена электронными сообщениями между органами и организациями, информационные системы которых подключены к СМЭВ, при предоставлении государственных и муниципальных услуг и исполнении государственных и муниципальных функций;

– обеспечение передачи на единый портал запросов, иных документов и сведений, обработанных в информационных системах органов и организаций, а также информации о ходе выполнения запросов о предоставлении государственных или муниципальных услуг и результатах их предоставления;

– осуществление мониторинга системы взаимодействия, а также мониторинга соблюдения процедур, предусмотренных техническими требованиями и соглашениями;

– предоставление информационно-методической поддержки органам и организациям в части использования ими системы взаимодействия, а также иных информационных систем, включенных в инфраструктуру, обеспечивающую информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме и подключенных к системе взаимодействия.

В целях исполнения своих функций СМЭВ обеспечивает:

– доступ к электронным сервисам информационных систем, подключенных к СМЭВ;

– возможность использования централизованных баз данных и классификаторов информационными системами, подключенными к СМЭВ;

– получение, обработку и доставку электронных сообщений в рамках информационного взаимодействия участников СМЭВ, обеспечение фиксирования времени их передачи, целостности и подлинности, указания их авторства и возможности предоставления сведений, позволяющих проследить историю движения электронных сообщений;

– защиту передаваемой информации от несанкционированного доступа, искажения или блокирования с момента поступления указанной информации в СМЭВ до момента передачи ее в подключенную к СМЭВ информационную систему;

– ведение реестра электронных сервисов информационных систем, подключенных к СМЭВ.

На рисунке 1.2.2 представлена общая схема оказания государственных услуг в электронной форме, где показано место СМЭВ в этом процессе.

Рисунок 1.2.2. Общая схема оказания государственных услуг в электронной форме.

Физически СМЭВ представляет собой набор узлов, размещенных в центрах обработки данных (ЦОД). Один узел СМЭВ используется федеральными органами власти, и по одному – в каждом регионе. К каждому региональному узлу подключены местные информационные системы (финансовые, медицинские, статистические и др.), порталы госуслуг, единая система идентификации и аутентификации, удостоверяющий центр, си-

стема нормативно-справочной информации и другие компоненты. Таким образом, посредством СМЭВ интегрируются между собой многочисленные федеральные и региональные информационные системы.

5. Единая система идентификации и аутентификации (ЕСИА).

Единая система идентификации и аутентификации является федеральной государственной информационной системой, обеспечивающей информационно-технологический доступ уполномоченных должностных лиц федеральных органов исполнительной власти, государственных внебюджетных фондов, органов исполнительной власти субъектов Российской Федерации, органов местного самоуправления, государственных и муниципальных учреждений, многофункциональных центров, иных органов и организаций и их информационных систем, физических и юридических лиц при формировании базовых государственных информационных ресурсов и при межведомственном информационном взаимодействии с использованием единой системы межведомственного электронного взаимодействия и подключенных к ней региональных систем межведомственного электронного взаимодействия.

ЕСИА является инструментом, подтверждающим права граждан на санкционированный доступ к государственным и муниципальным услугам и права уполномоченных должностных лиц на санкционированный доступ к необходимым сведениям при предоставлении данных услуг, а также на осуществление юридически значимых действий при предоставлении указанных услуг и исполнении государственных и муниципальных функций.

ЕСИА предназначена для обеспечения:

– доступа пользователей к различным информационным системам без необходимости повторной регистрации на основе единых идентификационных параметров с использованием различных носителей (СНИЛС и пароль, электронная подпись, SIM-карта или смарт-карта);

– доступа должностных лиц государственных организаций к базовым ресурсам; осуществления идентификации и аутентификации должностных лиц органов исполнительной власти при межведомственном взаимодействии;

– взаимодействия информационных систем, то есть механизмов идентификации, аутентификации и авторизации информационных систем при взаимодействии с использованием СМЭВ.

Основные функциональные возможности ЕСИА:

1. Идентификация и аутентификация пользователей, в том числе:

– однократная аутентификация (стандарты SAML или OpenID).

SAML (англ. security assertion markup language) – язык разметки декларации безопасности) – открытый стандарт обмена данными аутентификации и авторизации между участниками, в частности между поставщиком учётных записей и поставщиком сервиса.

OpenID – открытый стандарт децентрализованной системы аутентификации, предоставляющей пользователю возможность создать единую учётную запись для аутентификации на множестве не связанных друг с другом информационных ресурсов, используя услуги третьих лиц.

Пользователям ЕСИА это даёт следующее преимущество: пройдя процедуру идентификации и аутентификации в ЕСИА, пользователь может в течение одного сеанса работы обращаться к любым информационным системам, использующим ЕСИА, при этом повторная идентификация и аутентификация не требуется;

– поддержка различных методов аутентификации: по паролю и по электронной подписи;

– поддержка уровней достоверности идентификации (таблица 1.2.1).

Таблица 1.2.1.

Уровни достоверности идентификации

Уровень достоверности идентификации	**Описание**
Уровень 1	Минимальный уровень достоверности идентификации. Данный уровень присваивается учетным записям пользователей, личность которых не подтверждена. Предполагается использование данного уровня в ИС, которым требуется осуществлять взаимодействие с пользователями в рамках определенного контекста. При этом отсутствует необходимость гарантии, что данные о пользователе соответствуют реальной личности и что пользователь действительно является этой личностью.
Уровень 2	Данный уровень присваивается учетным записям пользователей, личность которых подтверждена со стандартным уровнем гарантии (проверяется реальное существование физического лица с помощью сервисов органов исполнительной власти, осуществляется подтверждение соответствия личности пользователя посредством отправки регистрируемого почтового отправления с кодом активации Почтой России или выдачи кода активации в центре регистрации). Для аутентификации используется пароль.

Уровень достоверности идентификации	Описание
Уровень 3	Данный уровень присваивается учетным записям пользователей, личность которых подтверждена с повышенным уровнем гарантии (проверяется реальное существование личности при персональном посещении пользователем центра регистрации – офиса уполномоченной организации). Для аутентификации используется электронная подпись.
Уровень 4	Максимальный уровень достоверности идентификации. Данный уровень присваивается учетным записям пользователей (к таким пользователям, например, относятся пользователи с ролью должностного лица органа власти), регистрация которых выполняется только уполномоченным сотрудником органа исполнительной власти (оператором). Самостоятельная регистрация указанных пользователей исключена.

2. Управление идентификационными данными, а именно ведение регистров физических, юридических лиц, органов и организаций, должностных лиц органов и организаций и информационных систем.

3. Авторизация уполномоченных лиц органа исполнительной власти (ОИВ) при доступе к следующим функциям ЕСИА:

– ведение регистра должностных лиц ОИВ в ЕСИА;

– ведение справочника полномочий ИС и предоставление пользователям ЕСИА (зарегистрированным в ЕСИА как должностные лица ОИВ) полномочий по доступу к ресурсам ИС, зарегистрированным ЕСИА;

– делегирование вышеуказанных полномочий уполномоченным лицам нижестоящих ОИВ.

4. Ведение и предоставление информации о полномочиях пользователей в отношении информационных систем.

Сценарий идентификации и аутентификации заявителей выглядит следующим образом (рисунок 1.2.3):

Рисунок 1.2.3. Сценарий идентификации и аутентификации заявителей.

1. Пользователь обращается к защищённому ресурсу ИС, например, ведомственному или региональному порталу государственных услуг.

2. Информационная система направляет в ЕСИА запрос на аутентификацию.

3. ЕСИА проверяет наличие у пользователя открытой сессии и, если активная сессия отсутствует, проводит его аутентификацию. Для этого ЕСИА направляет пользователя на веб-страницу аутентификации ЕСИА. Заявитель проходит идентификацию и аутентификацию, используя доступный ему метод аутентификации.

4. Если пользователь успешно аутентифицирован, то ЕСИА передаёт в информационную систему набор утверждений, содержащих идентификационные данные пользователя, информацию о контексте аутентификации, в том числе данные об уровне достоверности идентификации.

5. На основании полученной из ЕСИА информации ИС авторизует заявителя на доступ к защищаемому ресурсу.

Базовый сценарий авторизации должностных лиц ОИВ при межведомственном взаимодействии (доступе к ресурсам ИС, операторами которых являются другие ОИВ) представлен на рисунке 1.2.4 и выглядит так:

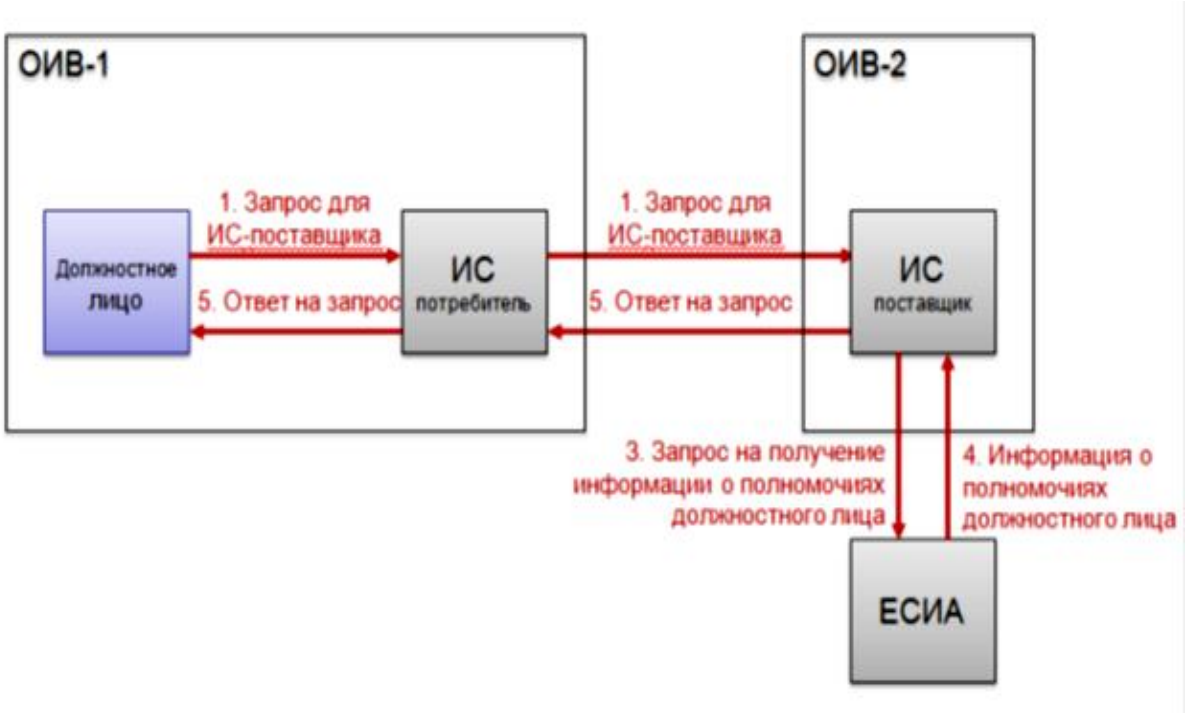

Рисунок 1.2.4. Базовый сценарий авторизации должностных лиц ОИВ при межведомственном взаимодействии.

1. Пользователь (должностное лицо) с использованием ИС-потребителя направляет запрос ИС-поставщику.

2. ИС-поставщик извлекает из запроса сведения о пользователе, отправившем запрос:

– идентификатор пользователя как физического лица – СНИЛС;

– идентификатор ОИВ, в котором пользователь является должностным лицом;

– основной государственный регистрационный номер (ОГРН).

3. ИС-поставщик направляет в ЕСИА запрос на предоставление информации о полномочиях пользователя в отношении ИС-поставщика. Для отправки запроса ИС-поставщик использует электронный сервис ЕСИА.

4. ЕСИА передаёт в ИС-поставщик данные о действующих полномочиях должностного лица.

5. ИС-поставщик на основании полученных из ЕСИА данных о полномочиях должностного лица авторизует запрос пользователя.

6. Единое пространство доверия (ЕПД).

Единое пространство доверия – это совокупность взаимосвязанных доверенных сервисов, в которой обеспечивается признание подлинности электронной подписи при электронном взаимодействии федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, иных государственных органов, государственных

внебюджетных фондов, органов местного самоуправления, организаций и физических лиц.

Единое пространство доверия включает в себя головной удостоверяющий центр (ГУЦ), информационную систему удостоверяющих центров ЕПД, а также множество аккредитованных и присоединенных к ЕПД удостоверяющих центров, обеспечивающих поддержку процессов управления сертификатами электронной подписи.

Инфраструктура ЕПД представлена на рисунке 1.2.5.

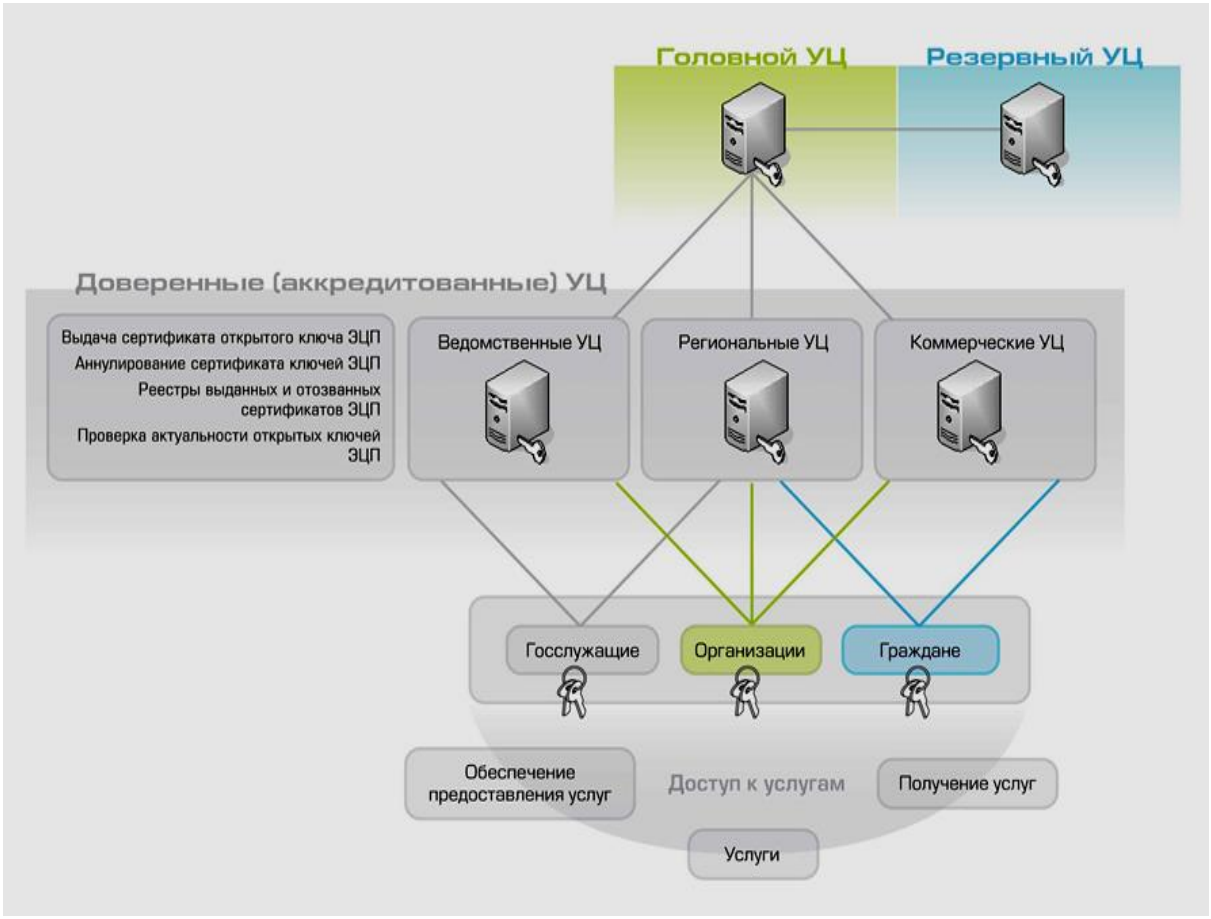

Рисунок 1.2.5. Инфраструктура ЕПД.

Информационная система удостоверяющих центров ЕПД предназначена для обеспечения информационно-технологической поддержки отношений по использованию электронных подписей, возникающих между субъектами, в том числе в процессах формирования и оказания электронных государственных и муниципальных услуг с помощью инфраструктуры электронного правительства.

Информационно-технологическая поддержка реализуется путем предоставления сторонам – субъектам отношений и взаимодействующим информационным системам – совокупности сервисов проверки и подтверждения аутентичности электронных подписей, для чего используются удо-

стоверяющие центры, входящие в ЕПД. Структура информационной системы удостоверяющих центров ЕПД представлена на рисунке 1.2.6.

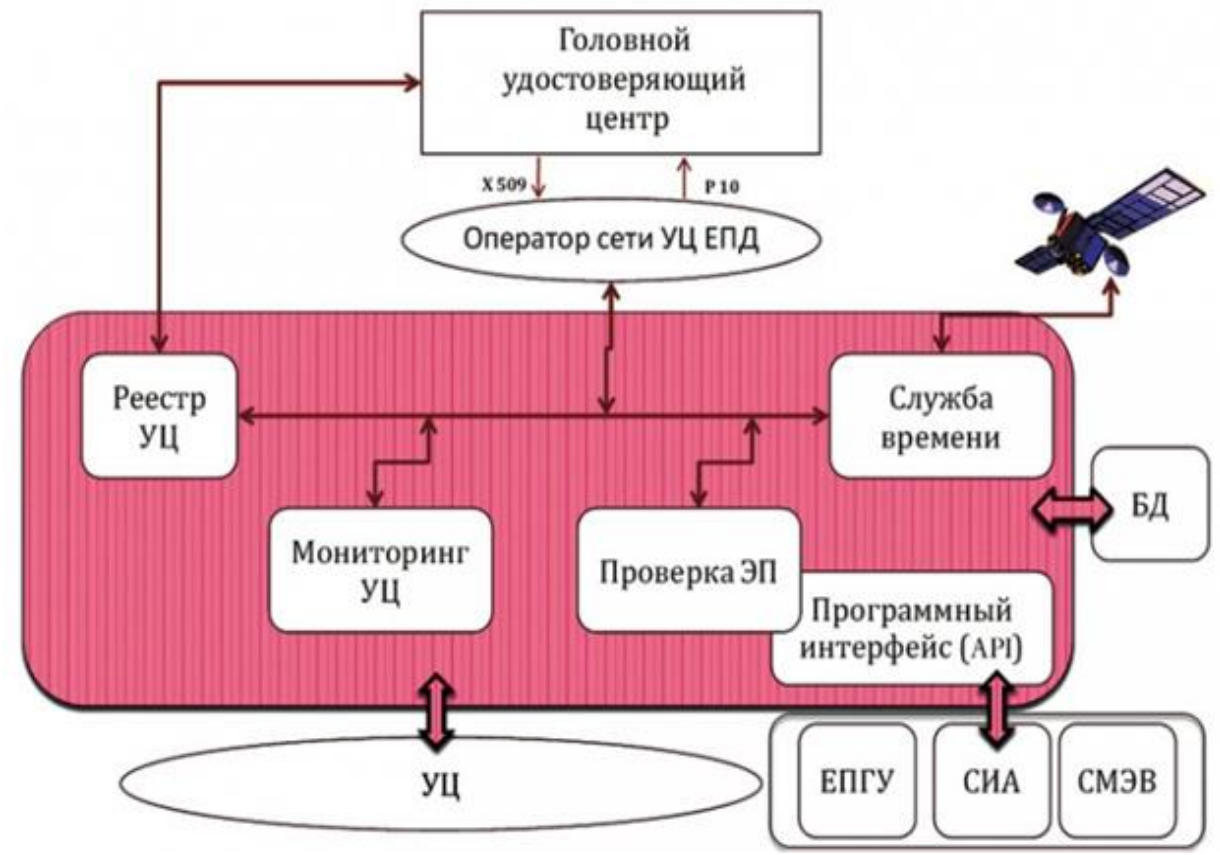

Рисунок 1.2.6. Структура информационной системы удостоверяющих центров ЕПД.

Электронная подпись (ЭП) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию[5].

ЭП представляет собой комбинацию символов, которая формируется в результате математического преобразования исходного документа при помощи специального программного обеспечения. ЭП добавляется к исходному документу при пересылке, и любое изменение исходного документа делает эту ЭП недействительной. Таким образом, ЭП безошибочно указывает на подлинность и авторство, не переносится с одного документа на другой документ, защищает подписанный документ от подделки, а также от изменения или искажения информации.

[5] Об электронной подписи: Федер. закон Рос. Федерации от 6 апреля 2011 г. № 63-ФЗ: ред. от 30 декабря 2015 г. // Собр. законодательства Рос. Федерации. 2011. № 15, ст. 2036.

ЭП основана на асимметричном криптографическом алгоритме. Особенностью такого алгоритма является то, что используются два разных ключа: один ключ для зашифрования информации, а второй, который специальным образом получен из первого и отличен от него, – для ее расшифрования.

Ключ электронной подписи – уникальная последовательность символов, предназначенная для создания электронной подписи.

Первый ключ является секретным – закрытым (личным) ключом, он известен только лицу, подписывающему документ. Второй ключ несекретный – открытый ключ, он может быть известен любому получателю электронного документа.

Открытый ключ публикуется на сайте удостоверяющего центра, услугами которого пользуется владелец ключа, а закрытый ключ он хранит со всеми возможными мерами предосторожности.

УЦ является системой управления ключами в рамках криптографической системы на основе инфраструктуры открытых ключей (закрытый ключ известен только его владельцу).

УЦ создает сертификат открытого ключа и таким образом удостоверяет этот ключ.

УЦ подтверждает или опровергает принадлежность открытого ключа лицу, которое владеет соответствующим закрытым ключом. Удостоверяющий центр – это организация, которая выпускает сертификаты ключей проверки ЭП и отвечает за управление криптографическими ключами пользователей. Открытые ключи и другая информация о пользователях хранится удостоверяющими центрами в виде цифровых сертификатов.

Сертификат – это электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи[6].

Выдавая сертификат, УЦ удостоверяет подлинность связи между открытым ключом пользователя УЦ и информацией, его идентифицирующей. И ключ, и сертификат хранятся в файлах. Для того, чтобы никто, кроме владельца подписи, не мог воспользоваться закрытым ключом, его обычно записывают на съемный носитель ключа (например, «Рутокен»). Для дополнительной защиты его снабжают PIN-кодом. Для создания электронной подписи необходимо ввести правильное значение PIN-кода. Сертификат содержит всю необходимую информацию для проверки электронной подписи. Данные сертификата открыты и публичны. Поэтому обычно

[6] Об электронной подписи: Федер. закон Рос. Федерации от 6 апреля 2011 г. № 63-ФЗ: ред. от 30 декабря 2015 г. // Собр. законодательства Рос. Федерации. 2011. № 15, ст. 2036.

сертификаты хранятся в хранилище сертификатов операционной системы. И, конечно, все сертификаты всегда хранятся в УЦ[7].

В МВД России введена в эксплуатацию Система удостоверяющих центров органов внутренних дел Российской Федерации (СУЦ ОВД). СУЦ ОВД – автоматизированная система, предназначенная для реализации возможностей средств электронной подписи в подразделениях системы МВД России. Целью СУЦ ОВД является предоставление ее пользователям возможностей использования электронной подписи.

Основными задачами СУЦ ОВД являются:

1. Обеспечение сотрудников ОВД средствами электронной подписи.

2. Обеспечение проверки электронной подписи электронного документа и статуса (действительности) сертификатов ключей проверки электронной подписи пользователей.

3. Реализация в СУЦ ОВД методов по обеспечению функционирования средств защиты информации от несанкционированного доступа с целью осуществления сохранности конфиденциальной информации, обрабатываемой в СУЦ ОВД.

4. Обеспечение возможности реализации механизмов строгой аутентификации при доступе пользователей к информационным ресурсам.

5. Обеспечение возможности формирования электронной подписи электронного документа в целях подтверждения его целостности и авторства и обеспечения юридической значимости.

СУЦ ОВД взаимодействует с единой системой информационно-аналитического обеспечения деятельности МВД России (ИСОД МВД России).

7. Государственная информационная система о государственных и муниципальных платежах (ГИС ГМП).

В соответствии с Федеральным законом от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»[8] с 1 января 2013 года органы, предоставляющие государственные услуги, не вправе требовать от заявителей документы, подтверждающие факт внесения платы за услугу, в том числе об оплате государственной пошлины, взимаемой за предоставление государственных и муниципальных услуг. Для подтверждения этого факта они должны использовать сведения, содержащиеся в ГИС ГМП.

ГИС ГМП представляет собой централизованную систему, обеспечивающую прием, учет и передачу информации между ее участниками,

---

[7] Султанов Р. А. Электронная подпись в системе МВД России // Информационные технологии, связь и защита информации МВД России – 2015: тематический сборник. Москва, 2015. С. 66-69.

[8] Об организации предоставления государственных и муниципальных услуг: Федер. закон Рос. Федерации от 27 июля 2010 г. № 210-ФЗ: ред. от 15 февраля 2016 г. // Рос. газ. 2010. 30 июля. № 168.

которыми являются администраторы доходов бюджета, организации по приему платежей, порталы, многофункциональные центры, взаимодействие которых с ГИС ГМП производится через систему межведомственного электронного взаимодействия.

Основные цели ГИС ГМП:

– предоставление гражданам и организациям единого источника сведений о начисленных и уплаченных платежах за государственные (муниципальные) услуги и о платежах в бюджетную систему Российской Федерации по принципу «одного окна»;

– получение платных государственных и муниципальных услуг без истребования с заявителя документов, подтверждающих оплату.

– Создание, ведение, развитие и обслуживание ГИС ГМП осуществляет Федеральное казначейство.

Государственные и муниципальные учреждения после осуществления начисления суммы, подлежащей оплате заявителем за предоставляемые услуги, а также иных платежей в случаях, предусмотренных федеральными законами, обязаны незамедлительно направлять информацию, необходимую для её уплаты, в ГИС ГМП.

Участники ГИС ГМП:

– Федеральное казначейство – осуществляет функции по созданию, ведению, развитию и обслуживанию ГИС ГМП;

– администраторы доходов – сообщают о начислениях (ГИБДД, ФНС, предприятия ЖКХ и другие ведомства);

– агенты, принимающие платежи, – сообщают об оплате платежей (банки, платёжные терминалы, отделения Почты России);

– портал государственных услуг, многофункциональный центр – предоставляют гражданам информацию о начислениях и платежах.

Схема взаимодействия ГИС ГМП представлена на рисунке 1.2.7.