ПРАВИТЕЛЬСТВО РЕСПУБЛИКИ ДАГЕСТАН

П О С Т А Н О В Л Е Н И Е

от 26 февраля 2025 г. № 39

г. МАХАЧКАЛА

Об утверждении Положения о Единой государственной системе управления и передачи данных Республики Дагестан

В целях упорядочения обмена информацией в Единой государственной системе управления и передачи данных Республики Дагестан и в локальных вычислительных сетях органов исполнительной власти Республики Дагестан, подведомственных им организаций, органов местного самоуправления муниципальных образований Республики Дагестан и иных заинтересованных организаций Правительство Республики Дагестан **п о с т а н о в л я е т:**

1. Утвердить прилагаемое Положение о Единой государственной системе управления и передачи данных Республики Дагестан.

2. Признать утратившим силу постановление Правительства Республики Дагестан от 5 августа 2011 г. № 268 «О вопросах эксплуатации Единой государственной системы управления и передачи данных Республики Дагестан и локальных вычислительных сетей органов исполнительной власти Республики Дагестан, подведомственных им организаций и органов местного самоуправления муниципальных образований Республики Дагестан» (Собрание законодательства Республики Дагестан, 2011, № 15, ст. 683).

3. Контроль за исполнением настоящего постановления возложить на заместителя Председателя Правительства Республики Дагестан в соответствии с распределением обязанностей.

АДМИНИСТРАЦИЯ ГЛАВЫ И ПРАВИТЕЛЬСТВА РЕСПУБЛИКИ ДАГЕСТАН
УПРАВЛЕНИЕ ДЕЛОПРОИЗВОДСТВА №1

Временно исполняющий обязанности Председателя Правительства Республики Дагестан Р. Алиев

УТВЕРЖДЕНО
постановлением Правительства
Республики Дагестан
от 26 февраля 2025 г. № 39

П О Л О Ж Е Н И Е
о Единой государственной системе управления и передачи данных Республики Дагестан

I. Общие положения

1. Настоящее Положение определяет назначение, структуру и правила функционирования Единой государственной системы управления и передачи данных Республики Дагестан, а также принципы информационного обмена, осуществляемого между участниками.

2. В настоящем Положении используются следующие термины:

Единая государственная система управления и передачи данных Республики Дагестан (далее – ЕГСУПД) – информационно-телекоммуникационная сеть с централизованным управлением, построенная с использованием технологий виртуальных частных сетей и криптографической защиты информации, реализованная на сертифицированных в установленном порядке средствах защиты информации;

технология защищенных виртуальных частных сетей – технология, предназначенная для построения виртуальных защищенных сетей путем использования системы персональных и межсетевых экранов на защищаемых компонентах распределенной сети и объединения защищаемых элементов через виртуальные соединения (туннели), обеспечивающие шифрование сетевого трафика между этими элементами на базе средств криптографической защиты информации (далее – СКЗИ);

центр управления сетью – аппаратные и программные средства для мониторинга, конфигурирования и управления компонентами ЕГСУПД;

компонент ЕГСУПД – сетевые узлы, обеспечивающие функционирование ЕГСУПД и представляющие собой программный или аппаратно-программный комплекс, выполняющий функции межсетевого экрана и криптомаршрутизатора, имеющий сертификат соответствия требованиям безопасности;

абонентский пункт – персональный компьютер, входящий в состав ЕГСУПД, с установленным компонентом ЕГСУПД, поддерживающим возможность работы через зашифрованные каналы связи;

оператор – Министерство цифрового развития Республики Дагестан, организующее предоставление доступа к компонентам ЕГСУПД, осуществляющее координацию действий участников ЕГСУПД, разработку организационно-распорядительных документов;

администратор – государственное автономное учреждение Республики Дагестан «Центр информационных технологий», оказывающее услуги по обслуживанию и технической поддержке ЕГСУПД;

участники – органы государственной власти Республики Дагестан, органы местного самоуправления муниципальных образований Республики Дагестан и подведомственные им государственные и муниципальные учреждения, иные организации, подключенные (подключаемые) к ЕГСУПД;

пользователь – должностное лицо участника ЕГСУПД, использующее для выполнения своих служебных обязанностей информационные системы и ресурсы, входящие в состав ЕГСУПД;

несанкционированный доступ – доступ к информации, хранящейся на различных типах носителей, в базах данных, файловых хранилищах, путем изменения (повышения, фальсификации) своих прав доступа;

ключ, ключевая информация – специальным образом организованный криптографический ключ, представленный в виде компьютерного файла, предназначенный для осуществления криптографической защиты информации в течение определенного срока;

внешняя среда по отношению к СКЗИ – абонентский пункт участника с установленной операционной системой, совместимой с программным обеспечением СКЗИ, подключенный к сети «Интернет», и/или серверная/телекоммуникационная стойка со стабильным и бесперебойным электропитанием.

3. Целью ЕГСУПД является технологическое обеспечение информационного взаимодействия между участниками в соответствии с требованиями законодательства по защите информации.

ЕГСУПД предназначена для решения следующих задач:

обеспечение исполнения государственных и муниципальных функций в электронной форме;

обеспечение предоставления в электронной форме государственных и муниципальных услуг;

обеспечение межведомственного электронного документооборота между участниками;

обеспечение информационного взаимодействия участников в электронной форме при осуществлении процессов подготовки и принятия управленческих решений Главы Республики Дагестан, Правительства Республики Дагестан, в том числе посредством информационно-аналитической поддержки анализа, мониторинга и планирования вопросов социально-экономического развития Республики Дагестан, а также вопросов оперативного реагирования, предотвращения и ликвидации чрезвычайных ситуаций;

обеспечение информационного взаимодействия в электронной форме между органами и организациями в случаях, предусмотренных законами Республики Дагестан, решениями Главы Республики Дагестан, решениями

Правительства Республики Дагестан, протоколами Правительственной комиссии Республики Дагестан по защите информации и Правительственной комиссии Республики Дагестан по использованию информационных технологий для формирования экосистемы цифровой экономики;

обеспечение информационного взаимодействия в электронной форме;

иные задачи, не противоречащие целям создания ЕГСУПД.

В рамках информационного обмена с ЕГСУПД допускается обмен электронными сообщениями, содержащими общедоступную информацию и информацию, доступ к которой ограничивается в соответствии с законодательством Российской Федерации. Обмен между участниками информационного взаимодействия информацией, доступ к которой ограничивается в соответствии с законодательством Российской Федерации, осуществляется при выполнении ими требований по защите такой информации, установленных в отношении информационных систем электронного документооборота.

II. Структура и состав ЕГСУПД

4. ЕГСУПД представляет собой территориально распределенную информационно-телекоммуникационную сеть, объединяющую следующие сегменты:

ядро защищенной сети, представленное комплексом программно-аппаратных средств шифрования и межсетевого экранирования, размещенных в Республиканском центре обработки данных;

центр управления сетью, расположенный в Республиканском центре обработки данных под управлением администратора;

сетевые узлы участников, включающие программно-аппаратные комплексы шифрования и межсетевого экранирования или программные комплексы шифрования и межсетевого экранирования в составе абонентских пунктов.

5. Функционирование ЕГСУПД осуществляется на основе сетей связи общего пользования, в том числе российского государственного сегмента информационно-коммуникационной сети «Интернет», а также выделенных сетей связи, в случае если оператором принято решение о функционировании ЕГСУПД на таких сетях связи.

6. ЕГСУПД обеспечивает подключение органов исполнительной власти Республики Дагестан к российскому сегменту информационно-телекоммуникационной сети «Интернет» (RSNet) в соответствии с требованиями Указа Президента Российской Федерации от 22 мая 2015 г. № 260 «О некоторых вопросах информационной безопасности Российской Федерации».

7. ЕГСУПД обеспечивает межсетевое взаимодействие с другими защищенными виртуальными сетями в рамках определенных настоящим Положением целей и задач.

III. Порядок подключения участников к ЕГСУПД

8. Решение о подключении участников к ЕГСУПД принимается оператором.

9. Подключение участников и пользователей включает в себя следующие этапы:

подача заявки;

рассмотрение заявки;

подключение к ЕГСУПД/направление мотивированного отказа.

10. Участник формирует и направляет оператору заявку о намерении подключиться к ЕГСУПД по форме, приведенной в приложении к настоящему Положению, с указанием цели подключения и перечня пользователей.

11. Оператор в течение 3 рабочих дней с момента получения заявки осуществляет ее рассмотрение и оценивает техническую возможность подключения участника и пользователей.

12. В случае отсутствия технической возможности организации подключения к ЕГСУПД оператор в течение одного рабочего дня с момента рассмотрения заявки уведомляет участника об отказе в подключении с обоснованием причины отказа.

13. В случае положительного результата рассмотрения заявки оператор в течение одного рабочего дня с момента ее рассмотрения передает заявку администратору для проведения работ по подключению участника к ЕГСУПД.

14. На участника распространяются все обязанности по соблюдению требований информационной безопасности, определенные действующим законодательством в области защиты информации, технической и эксплуатационной документации к программным и программно-аппаратным средствам, используемым для работы с ЕГСУПД, и настоящим Положением.

15. Подключение к ЕГСУПД производится за счет средств участника, если иное не установлено актами Правительства Республики Дагестан.

16. Все заявки в рамках взаимодействия направляются в установленном порядке в государственной информационной системе электронного документооборота Республики Дагестан «Дело» (далее – ГИС СЭД РД), а для участников, не имеющих подключение к ГИС СЭД РД, – на официальный адрес электронной почты оператора.

IV. Права и обязанности оператора

17. Оператор обязан:

рассматривать заявления участников на подключение к ЕГСУПД в установленные сроки;

осуществлять на основании заявок и соглашений подготовительные работы по организации предоставления доступа к компонентам ЕГСУПД;

формировать и поддерживать в актуальном состоянии электронный реестр участников, подключенных к ЕГСУПД;

обеспечивать функционирование и развитие ЕГСУПД;

разрабатывать, вводить в действие и предоставлять участникам организационно-распорядительные документы, регламентирующие правила работы участников в ЕГСУПД, проекты соглашений о подключении к ЕГСУПД;

осуществлять мероприятия по модернизации и развитию ЕГСУПД.

18. Оператор имеет право:

информировать руководителей участников о невыполнении их должностными лицами требований информационной безопасности и несоблюдении иных условий по обеспечению бесперебойного функционирования ЕГСУПД;

запрашивать у администратора информацию о компонентах ЕГСУПД;

запрашивать и получать от участников необходимые материалы и сведения об использовании ими ЕГСУПД;

принимать решение об отключении или ограничении доступа к информационным системам ЕГСУПД в случаях нарушения должностными лицами участника требований настоящего Положения;

отказать участнику в подключении к ЕГСУПД.

19. Оператор несет ответственность:

за невыполнение требований настоящего Положения, а также других актов, регулирующих работу ЕГСУПД;

неправомерное использование информации, передаваемой посредством ЕГСУПД, к которой оператор получает доступ в связи с выполнением своих должностных обязанностей.

V. Права и обязанности администратора

20. Администратор обязан:

осуществлять администрирование компонентов ЕГСУПД с учетом требований эксплуатационной документации;

осуществлять техническое обслуживание компонентов ЕГСУПД, используемых участником, при наличии сертификата технической поддержки для компонентов ЕГСУПД, принадлежащих пользователю, в составе работ, предусмотренных данным сертификатом;

своевременно реагировать на поступившие заявки о неисправностях в работе компонентов ЕГСУПД и принимать необходимые меры по их устранению;

периодически проверять состояние ЕГСУПД и своевременно реагировать на попытки несанкционированного доступа;

информировать пользователей ЕГСУПД о порядке работы и ответственности за нарушение настоящего Положения;

информировать оператора и пользователей ЕГСУПД о проводимых работах по обслуживанию и возможных перебоях в работе защищенной сети;

осуществлять поэкземплярный учет СКЗИ и ключевой информации, выданной участникам и относящейся к компонентам ЕГСУПД, в соответствии с требованиями законодательства Российской Федерации;

осуществлять подключение к ЕГСУПД участников и пользователей в соответствии с заявками на подключение;

предоставлять участникам доступ к информационным системам в рамках ЕГСУПД в соответствии с заявками, оформленными в установленном порядке;

предоставлять оператору информацию о компонентах ЕГСУПД;

по требованию оператора производить блокировку или удаление компонентов ЕГСУПД и сетей участников, с которыми организовано межсетевое взаимодействие.

21. Администратор имеет право:

информировать оператора о невыполнении пользователями участников требований информационной безопасности и несоблюдении иных условий по обеспечению бесперебойного функционирования ЕГСУПД;

по согласованию с оператором производить отключение или ограничение доступа к информационным системам ЕГСУПД пользователям участника в случаях нарушения ими требований настоящего Положения.

22. Администратор несет ответственность за действия (бездействие), повлекшее за собой:

невыполнение требований настоящего Положения, а также других актов, регулирующих работу ЕГСУПД;

несвоевременное выявление попыток несанкционированного доступа к ядру защищенной сети, приведших к нарушению требований обеспечения безопасности ЕГСУПД;

несвоевременное устранение неисправностей в работе ядра защищенной сети;

неправомерное использование информации, передаваемой с использованием ЕГСУПД, к которой администратор получает доступ в связи с выполнением своих функций.

VI. Права и обязанности участника и пользователя

23. Ответственность за допуск пользователя к работе в ЕГСУПД и предоставление ему соответствующих полномочий, в том числе за соблюдение пользователем требований по информационной безопасности, несет участник, принявший решение о подключении пользователя к ЕГСУПД.

24. Участник обязан:

осуществлять поэкземплярный учет СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;

осуществлять учет имеющихся у него лицензий и предоставлять их копии по требованию администратора сети ЕГСУПД;

обеспечивать работоспособность программного обеспечения, СКЗИ, необходимых для информационного обмена, подразумевающую выполнение требований к внешней среде по отношению к СКЗИ, позволяющей обеспечить их полнофункциональную эксплуатацию;

принимать меры по пресечению несанкционированного доступа к компонентам ЕГСУПД;

уведомлять оператора ЕГСУПД о случаях нарушений и принятых мерах;

приобретать сертификаты технической поддержки для компонентов ЕГСУПД, принадлежащих пользователю;

производить настройку сетевого оборудования, принадлежащего участнику, для организации доступа пользователей к ЕГСУПД;

обеспечивать безопасность хранения ключевой информации и (или) паролей, переданных администратором для подключения к ЕГСУПД;

обеспечить контроль доступа в помещения, где установлены СКЗИ, согласно действующему законодательству.

25. Пользователь обязан:

знать и соблюдать правила информационной безопасности при работе в ЕГСУПД, определенные настоящим Положением, а также другими актами, регулирующими работу ЕГСУПД;

при выявлении вредоносных программ или признаков нештатного функционирования программного обеспечения немедленно сообщать должностному лицу участника, ответственному за техническую защиту информации, и оператору;

предоставлять свой абонентский пункт администратору для контроля и осуществления технических действий, за исключением случаев запрета на допуск посторонних лиц к абонентскому пункту, установленных участником;

обеспечивать безопасность хранения ключевой информации и (или) паролей, переданных администратором для подключения к ЕГСУПД;

обеспечивать выполнение требований безопасности информации в соответствии с законодательством Российской Федерации на абонентском пункте.

26. Пользователю запрещается:

оставлять свой абонентский пункт во включенном состоянии без контроля и с незаблокированными устройствами ввода и отображения информации;

допускать к подключенному в ЕГСУПД абонентскому пункту посторонних лиц;

самостоятельно проводить изменения в настройках компонентов ЕГСУПД;

передавать пароли и ключевую информацию третьим лицам, а также размещать их в местах, доступных посторонним лицам.

27. Пользователь имеет право:

пользоваться информационными системами, ресурсами и сервисами ЕГСУПД в рамках предоставленных ему полномочий;

обращаться к администратору для решения вопросов использования ЕГСУПД.

28. Пользователь и участник несут ответственность за:

невыполнение требований настоящего Положения, а также других актов, регулирующих работу ЕГСУПД;

неправомерное использование информации, передаваемой посредством ЕГСУПД, к которой пользователь и участник получают доступ в связи с выполнением своих функций.

VII. Организация межсетевого взаимодействия с другими защищенными виртуальными сетями

29. Организация межсетевого взаимодействия с другими сетями, функционирующими на основе технологии защищенных виртуальных частных сетей, включает в себя следующие этапы:

подача заявки;

рассмотрение заявки;

подключение к ЕГСУПД (подписание соглашения о межсетевом взаимодействии) /направление мотивированного отказа.

30. С целью организации межсетевого взаимодействия между ЕГСУПД и сторонней защищенной виртуальной сетью участник сторонней сети в установленном порядке направляет оператору заявку о подключении с указанием цели подключения и контактов должностных лиц, ответственных за организацию такого взаимодействия, по форме согласно приложению к настоящему Положению.

31. Оператор в течение 10 рабочих дней со дня получения заявки совместно с администратором проводит оценку оснований и технической возможности для организации межсетевого взаимодействия.

32. Оператор имеет право отказать в подключении новому участнику межсетевого взаимодействия, при этом проинформировать его в течение 5 рабочих дней об имеющихся основаниях для такого решения, связанных с отсутствием технической возможности организации данного взаимодействия.

33. В случае принятия положительного решения об организации межсетевого взаимодействия оператор и участник подписывают соглашение о межсетевом взаимодействии. Оператор совместно с администратором и администратором сторонней защищенной виртуальной сети организует формирование необходимой адресной и ключевой информации для каждой из сетей.

34. Данная информация доверенным способом передается в соответствующие центры управления сетями (далее – ЦУС), с которыми необходимо осуществлять межсетевое взаимодействие.

35. Во всех ЦУС производится ввод и обработка полученных из других ЦУС данных, установление связей.

36. Ответная информация доверенным способом передается в соответствующие ЦУС, где она обрабатывается и вводится в действие. На этом этапе завершается процесс создания межсетевого взаимодействия между ЦУС, в дальнейшем обмен данными между ними производится в автоматическом режиме.

37. Сформированная ключевая и справочная информация через ЦУС отправляется на абонентские пункты, участвующие в межсетевом взаимодействии.

38. После завершения процедуры организации межсетевого взаимодействия между ЕГСУПД и сторонней защищенной виртуальной сетью подписывается протокол установления межсетевого взаимодействия.

VIII. Компрометация ключевой информации абонентских пунктов

39. Под компрометацией ключевой информации (ключей) понимается утрата доверия к тому, что используемые ключи обеспечивают безопасность информации.

40. Ключи пользователя считаются скомпрометированными в следующих случаях:

посторонним лицам мог стать доступен файл ключевого дистрибутива;

посторонним лицам мог стать доступен съемный носитель с ключевой информацией;

посторонние лица могли получить неконтролируемый физический доступ к ключевой информации, хранящейся на компьютере, если все ключи хранятся на компьютере;

увольнение пользователя, на которого оформлены пароль и ключ.

41. Оператор совместно с администратором при получении информации о компрометации ключевой информации в течение 1 рабочего дня должен убедиться в достоверности сообщения о компрометации, после этого обязан немедленно аннулировать скомпрометированные ключи и внести соответствующую запись в справочник связей.

42. В случае наступления любого из событий, связанных с компрометацией ключевой информации, пользователь немедленно прекращает связь с другими абонентскими пунктами, посредством выключения компонента ЕГСУПД или персонального компьютера пользователя и незамедлительно сообщает о факте компрометации ключей соответствующего абонентского пункта оператору ЕГСУПД.

43. К событиям, требующим проведения расследования и принятия решения о компрометации ключевой информации, относится возникновение подозрений в несанкционированном доступе к информации, находящейся в ЕГСУПД. Расследование проводится комиссией, состоящей из:

пользователя;

представителя оператора;

представителя администратора.

В течение 5 рабочих дней проводится расследование, в ходе которого выясняется, откуда и каким образом произошло несанкционированное получение информации из абонентского пункта пользователя.

IX. Порядок организации хранения и учета ключевой информации компонентов ЕГСУПД

44. Хранение, эксплуатация и учет компонентов ЕГСУПД, ключевой информации компонентов ЕГСУПД осуществляются администратором и участником в соответствии с требованиями Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» (далее – приказ ФАПСИ от 13 июня 2001 г. № 152).

45. Учет компонентов ЕГСУПД ведется в журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

46. Компоненты ЕГСУПД учитываются совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование.

47. Все полученные экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должны быть выданы под расписку в соответствующем журнале поэкземплярного учета пользователям компонентов ЕГСУПД, несущим персональную ответственность за их сохранность.

48. Если эксплуатационной и технической документацией к компонентам ЕГСУПД предусмотрено применение разовых ключевых носителей или криптоключи вводят и хранят (в течение всего срока их действия) непосредственно в компоненте ЕГСУПД, то такой разовый ключевой носитель или электронная запись соответствующего криптоключа должны регистрироваться в техническом журнале.

49. В состав ключевой информации компонентов ЕГСУПД входят следующие составляющие:

дистрибутив справочно-ключевой информации, который представляет собой сборник, содержащий личные ключи пользователя, ключевой набор сетевого узла и адресные справочники компонента ЕГСУПД;

личные ключи пользователя, представляющие собой ключи защиты пользователя, необходимые для его аутентификации на сетевом узле;

резервный набор персональных ключей пользователя, предназначенный для получения дистанционного обновления ключевой информации при изменении исходной ключевой информации в удостоверяющем и ключевом центре.

50. Дистрибутив справочно-ключевой информации и резервные наборы персональных ключей формируются администратором.

51. Личные ключи пользователя устанавливаются при первичной инициализации в контейнер на абонентском пункте или переносятся на ключевой носитель.

X. Установка и ввод в эксплуатацию компонентов ЕГСУПД

52. Требования к установке компонентов ЕГСУПД:

установка, настройка и управление компонента ЕГСУПД осуществляется администратором. Все действия производятся строго в соответствии с технической и эксплуатационной документацией на компоненты ЕГСУПД;

в случаях наличия у участника запрета на допуск посторонних лиц к компоненту ЕГСУПД его установка может производиться участником самостоятельно;

на каждый компонент ЕГСУПД участником оформляется акт установки и ввода в эксплуатацию СКЗИ по типовой форме;

экземпляры акта хранятся у участника, а копии передаются оператору и администратору.

53. Требования к размещению компонентов ЕГСУПД:

а) общие требования:

размещение, охрана и специальное оборудование помещений, в которых установлены компоненты ЕГСУПД и ведется работа с носителями персональной ключевой информации, должны исключать возможность бесконтрольного проникновения в них посторонних лиц, прослушивания ведущихся там переговоров и просмотра помещений посторонними лицами, а также гарантировать сохранность находящихся в этих помещениях ключевых документов;

порядок охраны и организации режима помещений, в которых установлены компоненты ЕГСУПД, регламентируется разделом 4 приказа ФАПСИ от 13 июня 2001 г. № 152;

при подключении компонентов ЕГСУПД к каналам передачи данных, выходящих за пределы контролируемой зоны, необходимо выполнение действующих в Российской Федерации требований по защите информации от утечки по техническим каналам, в том числе по каналу связи;

б) требования к размещению компонента ЕГСУПД:

компонент ЕГСУПД устанавливается в выделенных помещениях серверных узлов;

доступ в помещение серверных узлов должен быть ограничен и осуществляться в соответствии с нормами приказа Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

в) требования к размещению программного компонента ЕГСУПД абонентского пункта:

программный компонент ЕГСУПД является персональным средством защиты пользователя и размещается на рабочем месте пользователя.

Дополнительных специальных требований к помещениям, где установлен программный компонент ЕГСУПД, настоящим Положением не предъявляется.

54. Настройка операционной системы абонентского пункта, а также выбор типа аутентификации производятся в соответствии с эксплуатационной и технической документацией на компоненты ЕГСУПД.

XI. Вывод компонентов ЕГСУПД из эксплуатации

55. Вывод компонентов ЕГСУПД из эксплуатации оформляется в виде акта по типовой форме, который хранится у администратора.

56. Удаление ключевой информации компонентов ЕГСУПД:

удаление ключевой информации при обновлениях или деинсталляции программного обеспечения производится штатными средствами компонента ЕГСУПД;

удаление ключевой информации на жестких дисках, дискетах или флэш-памяти производится с использованием специальной программы, входящей в состав компонента ЕГСУПД. В журнале учета выдачи ключевых документов делается отметка об уничтожении ключей.

Ключевая информация должна быть уничтожена в сроки, указанные в эксплуатационной и технической документации. Если срок уничтожения эксплуатационной и технической документацией не установлен, то ключевые документы должны быть уничтожены не позднее 10 рабочих дней после вывода их из действия.

При удалении дистрибутивов или невозможности воспользоваться штатными средствами удаление ключевой информации производится администратором под расписку в соответствующих журналах поэкземплярного учета, а уничтожение большого объема ключевых документов может быть оформлено актом.

Уничтожение по акту производит комиссия в составе не менее двух человек из числа лиц, допущенных к использованию компонента ЕГСУПД. В акте указывается, что уничтожается и в каком количестве. В конце акта делается итоговая запись (цифрами и прописью) о количестве наименований и экземпляров уничтожаемых ключевых документов, инсталлирующих криптосредства носителей, эксплуатационной и технической документации. О проведенном уничтожении делаются отметки в соответствующих журналах поэкземплярного учета.

XII. Техническое обслуживание ЕГСУПД

57. Технические мероприятия по обслуживанию компонентов ЕГСУПД организуются администратором.

58. К техническим работам относятся:

реконфигурирование ЕГСУПД;

установка (переустановка) программного обеспечения, в том числе операционных систем, заявка на которую осуществляется по форме согласно приложению к настоящему Положению;

техническое обслуживание компонентов ЕГСУПД;

обновление компонента ЕГСУПД;

другие виды работ, необходимость проведения которых определяется администратором по согласованию с оператором.

59. О проведении плановых работ администратор уведомляет оператора не менее чем за 72 часа до намеченного срока начала работ.

60. Администратор осуществляет периодический контроль работоспособности компонентов ЕГСУПД (компонент ЕГСУПД и абонентские пункты).

61. Контроль может осуществляться как непосредственно на проверяемом компоненте, так и удаленно. Контрольная проверка осуществляется в следующих случаях:

при вводе компонента в эксплуатацию;

при изменении лица, ответственного за эксплуатацию;

при изменении состава аппаратных средств компонента;

периодически, по графику, разрабатываемому оператором.

62. Результаты проверки оформляются в виде протокола проверки в соответствии с технической и эксплуатационной документацией на компоненты ЕГСУПД.

63. Удаленная проверка компонентов ЕГСУПД осуществляется выборочно или полностью для всех компонентов ЕГСУПД после процедуры удаленного обновления программного обеспечения или периодически в промежутках между контрольными проверками.

64. При обнаружении фактов сбоев в работе программного обеспечения или нарушении правил эксплуатации ЕГСУПД пользователь обязан уведомить об этом оператора.

65. В случае возникновения производственной необходимости проведения аварийных и планово-профилактических работ доступ к ЕГСУПД или ее отдельным сегментам может быть закрыт.

66. Для защиты компонентов ЕГСУПД от сбоев электропитания, компоненты ЕГСУПД необходимо оборудовать источниками бесперебойного питания, мощность которых в случае отключения электропитания обеспечит возможность корректного завершения выполняемых задач.

67. В случае возникновения нештатных ситуаций участники с привлечением администратора обязаны восстановить работоспособность используемых ими компонентов ЕГСУПД в течение 1 рабочего дня.

ПРИЛОЖЕНИЕ
к Положению о Единой
государственной системе управления
и передачи данных Республики
Дагестан

Ф О Р М А
заявки на подключение к Единой государственной системе управления и передачи данных Республики Дагестан
(оформляется на бланке органа/организации)

В связи с производственной необходимостью *(наименование органа/организации)* просит подключить к Единой государственной системе управления и передачи данных Республики Дагестан следующих сотрудников для *(указать для выполнения каких задач осуществляется подключение (перечень из пункта 3 Положения о Единой государственной системе управления и передачи данных Республики Дагестан)*.

ФИО	Должность	Контактная информация

Ф О Р М А
заявки на установку (настройку) компонентов ЕГСУПД, используемых участником Единой государственной системы управления и передачи данных Республики Дагестан
(оформляется на бланке органа/организации)

В связи с *(указать причину) (наименование органа/организации)* просит осуществить установку (настройку) компонентов ЕГСУПД для следующих сотрудников.

Ф.И.О.	Должность	Контактная информация

Ф О Р М А
заявки на организацию межсетевого взаимодействия
(оформляется на бланке органа/организации)

В связи с *(приводится подробное обоснование) (наименование органа/организации)* просит организовать межсетевое взаимодействие между Единой государственной системой управления и передачи данных Республики Дагестан и *(наименование сети)*.

Абонентский пункт в сети Правительства Республики Дагестан	Абонентский пункт и номер сети для организации связей