ГУБЕРНАТОР ЯМАЛО-НЕНЕЦКОГО АВТОНОМНОГО ОКРУГА

ПОСТАНОВЛЕНИЕ

29 января 2016 г. № 13-ПГ

г. Салехард

Об электронной подписи в региональной межведомственной системе электронного документооборота Ямало-Ненецкого автономного округа

В целях обеспечения условий для реализации юридически значимого электронного документооборота при внешнем и внутреннем документационном взаимодействии органов государственной власти Ямало-Ненецкого автономного округа, иных государственный органов Ямало-Ненецкого автономного округа, органов местного самоуправления в Ямало-Ненецком автономном округе, государственных и муниципальных учреждений Ямало-Ненецкого автономного округа **п о с т а н о в л я ю:**

1. Утвердить прилагаемый Порядок формирования среды использования электронной подписи в региональной межведомственной системе электронного документооборота Ямало-Ненецкого автономного округа (далее – Порядок).

2. Рекомендовать органам государственной власти, иным государственным органам Ямало-Ненецкого автономного округа, органам местного самоуправления в Ямало-Ненецком автономном округе, самостоятельно осуществляющим управление (администрирование) аппаратно-программных компонентов региональной межведомственной системы электронного документооборота Ямало-Ненецкого автономного округа своих системных организаций (далее – РМСЭД, Участники РМСЭД, Сегмент РМСЭД):

2.1. разработать и принять положения об управлении (администрировании) Сегментов РМСЭД с определением уполномоченных должностных лиц/структурных подразделений/исполнительных органов государственной власти Ямало-Ненецкого автономного округа, их прав и обязанностей;

2.2. реализовать в информационных системах Участников РМСЭД среду использования электронной подписи в соответствии с применяемым её видом согласно Порядку;

2.3. разработать (при необходимости) и принять правовые акты Участника РМСЭД по процедурам, установленным Порядком;

2.4. провести ревизию порядка осуществляемого внутреннего и внешнего документационного взаимодействия, процедур делопроизводства в целях повышения их эффективности, снижения организационных, временных, материально-технических затрат на их осуществление, в том числе и за счёт последовательного перехода на использование электронных документов, при обеспечении сохранности документального фонда;

2.5. направить информацию о реализации:

подпунктов 2.1 – 2.3 настоящего пункта – в департамент информационных технологий и связи Ямало-Ненецкого автономного округа;

подпункта 2.4 настоящего пункта – в аппарат Губернатора Ямало-Ненецкого автономного округа.

3. Контроль за исполнением настоящего постановления возложить на заместителя Губернатора Ямало-Ненецкого автономного округа, руководителя аппарата Губернатора Ямало-Ненецкого автономного округа Фиголь Н.В.

Губернатор
Ямало-Ненецкого автономного округа Д.Н. Кобылкин

Аппарат Губернатора Ямало-Ненецкого автономного округа
Управление по обеспечению деятельности Правительства и Губернатора

УТВЕРЖДЁН

постановлением Губернатора
Ямало-Ненецкого автономного округа
от 29 января 2016 года № 13-ПГ

ПОРЯДОК

формирования среды использования электронной подписи в региональной межведомственной системе электронного документооборота Ямало-Ненецкого автономного округа

I. Используемые термины и обозначения

РМСЭД – региональная межведомственная система электронного документооборота Ямало-Ненецкого автономного округа (далее – автономный округ);

Участник РМСЭД – орган государственной власти автономного округа, иной государственный орган автономного округа, орган местного самоуправления в автономном округе, самостоятельно осуществляющий управление (администрирование) аппаратно-программных компонентов РМСЭД своих системных организаций (далее – сегмент РМСЭД) и включенный в перечень участников региональной межведомственной системы электронного документооборота автономного округа и наименований их системных организаций, утвержденный распоряжением Губернатора автономного округа от 06 июня 2011 года № 123-Р.

Основное подразделение Участника РМСЭД – исполнительный орган государственной власти автономного округа, орган местного самоуправления в автономном округе и подведомственное им государственное и муниципальное учреждение, а также иные организации и учреждения, указанные в базе данных «Структура организации» Участника РМСЭД, являющиеся юридическим лицом и источником комплектования государственных и муниципальных архивов.

Подразделение Участника РМСЭД – структурное подразделение Участника РМСЭД или основного подразделения Участника РМСЭД, не являющиеся юридическим лицом и источником комплектования государственных и муниципальных архивов.

Электронная подпись (далее – 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.

Электронный документ РМСЭД – запись или взаимоувязанная совокупность записей баз данных, отображаемая в визуальных формах РМСЭД в виде набора именованных полей и их содержания (реквизитов).

Аутентификация – процедура проверки принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности.

Авторизация – предоставление определённому лицу или группе лиц прав на выполнение определённых действий; а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий.

Идентификация – процедура, в результате выполнения которой для субъекта идентификации выявляется его идентификатор, однозначно идентифицирующий этого субъекта в информационной системе.

II. Общие положения

2.1. При организации документационного взаимодействия в РМСЭД используются: усиленная квалифицированная электронная подпись, усиленная неквалифицированная электронная подпись и простая электронная подпись (далее – квалифицированная ЭП, неквалифицированная ЭП, простая ЭП).

2.2. Квалифицированная ЭП применяется:

2.2.1. при предоставлении государственных или муниципальных услуг и исполнении государственных или муниципальных функций;

2.2.2. в случаях когда федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами, установлена обязательность использования данного вида ЭП;

2.2.3. если в соответствии с федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или обычаем делового оборота документ должен быть заверен печатью;

2.2.4. при документационном взаимодействии между основными подразделениями различных Участников РМСЭД;

2.2.5. при международном документационном взаимодействии, когда необходимость использования данного вида ЭП определена нормами права иностранного государства и международными стандартами.

2.3. Неквалифицированная ЭП применяется:

2.3.1. в случаях когда федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами, правовыми актами автономного округа и настоящим Порядком не установлена обязательность использования квалифицированной ЭП, предусмотрена возможность использования данного вида ЭП или отсутствует запрет на её использование;

2.3.2. при документационном взаимодействии между основными подразделениями одного Участника РМСЭД в порядке, определяемом правовым актом основного подразделения Участника РМСЭД;

2.4. Простая ЭП применяется:

2.4.1. в случаях когда федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами, правовыми актами автономного округа и настоящим Порядком, не установлена обязательность использования квалифицированной ЭП или неквалифицированной ЭП, предусмотрена возможность использования данного вида ЭП или отсутствует запрет на ее использование;

2.4.2. при документационном взаимодействии между основными подразделениями одного Участника РМСЭД в порядке, определяемом правовым актом Участника РМСЭД;

2.4.3. при документационном взаимодействии между структурными подразделениями и сотрудниками одного подразделения Участника РМСЭД;

2.4.4. в случаях когда электронный документ РМСЭД, полученный основным подразделением Участника РМСЭД, направляется на исполнение или ознакомление в подведомственное ему учреждение.

2.5. Документы, определенные к подписанию простой ЭП, могут быть подписаны неквалифицированной ЭП или квалифицированной ЭП. Документы, определенные к подписанию неквалифицированной ЭП, могут быть подписаны квалифицированной ЭП. Иная замена видов ЭП не допускается.

2.6. Электронные копии электронных документов или документов на бумажном носителе могут быть заверены видом ЭП, определенным настоящим Порядком.

2.7. Электронный документ, подписанный ЭП, признается равнозначным документу на бумажном носителе, подписанному собственноручной подписью, кроме случаев, если федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе. Недопустимо признание ЭП и (или) подписанного ею электронного документа не имеющим юридической силы только на основании того, что такая ЭП создана не собственноручно, а с использованием средств ЭП для автоматического создания и (или) автоматической проверки ЭП в РМСЭД.

2.8. Одной ЭП могут быть подписаны несколько связанных между собой электронных документов (пакет электронных документов). При подписании ЭП пакета электронных документов каждый из электронных документов, входящих в этот пакет, считается подписанным ЭП того вида, которой подписан пакет электронных документов.

2.9. Юридический статус электронного документа РМСЭД (подписан или заверен), его частей, реквизитов (полей) или действий с ними определяется по соотношению полей указания автора документа/действия или владельца ключа ЭП с полями отображения идентификатора владельца ключа ЭП.

В случае соответствия этих полей документ является собственноручно подписанным, а действие – выполненным лично. В противном случае документ является заверенным, а действие – выполненным по доверенности.

III. Правила получения и использования простой ЭП

3.1. Требования к среде использования простой ЭП

3.1.1. Простая ЭП может быть реализована на отдельных автоматизированных рабочих местах, в отдельных информационных системах основных подразделений Участника РМСЭД и подразделений Участника РМСЭД (далее при совместном упоминании – (основное) подразделение Участника

РМСЭД), информационных системах Участника РМСЭД при обеспечении средствами используемой операционной системы или специализированного программного обеспечения (далее – ПО) запрета на самостоятельное изменение системного времени и даты используемого персонального компьютера.

3.1.2. Участник РМСЭД должен обеспечить реализацию парольной политики РМСЭД с учетом следующих требований:

- длина пароля не менее 6 символов (требования к наличию отдельных символов могут не устанавливаться);
- длина очереди предыдущих паролей – не менее 1 (новый пароль не должен повторять предыдущий);
- срок действия пароля – не более 2 лет.

3.2. Порядок создания и выдачи ключей простой ЭП

3.2.1. Правом создания (замены), ликвидации и выдачи ключа простой ЭП обладают (основные) подразделения Участника РМСЭД, наделенные правовым актом Участника РМСЭД полномочиями на управление (администрирование) закрепленного сегмента РМСЭД (далее – оператор ключей). Если оператор ключей является основным подразделением Участника РМСЭД, то своим правовым актом он определяет должностных лиц, уполномоченных на реализацию данных полномочий, в противном случае такие должностные лица определяются правовым актом Участника РМСЭД (далее – администратор ключей).

3.2.2. Правом создания заявки на создание или ликвидацию ключа простой ЭП (далее – заявка) обладают руководители (основных) подразделений Участника РМСЭД или руководители их кадровых служб. Правовым актом Участника РМСЭД или основного подразделения Участника РМСЭД могут быть определены иные уполномоченные должные лица. В последнем случае копия соответствующего правового акта направляется оператору ключей.

3.2.3. Заявка на создание ключа простой ЭП должна содержать следующую информацию о сотруднике, претендующем на владение ключом простой ЭП (далее – претендент):

- полные фамилия, имя, отчество (при наличии) с различением букв «е» и «ё» (при наличии последней) в именительном и дательном падежах;
- полное наименование замещаемой должности с указанием всех уровней служебной иерархии;
- контактные координаты: номера телефонов и аппаратов факсимильной связи с указанием кода междугородной связи, адреса служебной электронной почты (при наличии);
- данные места нахождения: юридический и почтовый адрес (в случае отличия от данных структурного подразделения) и номер кабинета (комнаты);
- фотография в электронном виде формата JPG (необязательно);
- список сотрудников, замещающих в РМСЭД претендента;
- список сотрудников, которых должен замещать в РМСЭД претендент;

- дополнительная информация, связанная с обеспечением полномочий претендента в РМСЭД (место регистрации и т.д.).

3.2.4. Заявка на ликвидацию ключа простой ЭП должна содержать следующую информацию о владельце ключа простой ЭП:

- полные фамилия, имя, отчество (при наличии);
- полное наименование замещаемой должности;
- обоснование предлагаемых к осуществлению действий: вид, номер, дата, наименование правового акта с приложением копии/выписки или представление к ознакомлению с ним;
- дополнительная информация при необходимости, в т.ч. по передаче полномочий в РМСЭД владельца ключа простой ЭП.

3.2.5. Форма, вид, содержание и порядок подачи и исполнения заявки могут быть определены правовым актом Участника РМСЭД или оператора выдачи ключей. При этом должны быть обеспечены фиксация автора, даты подачи и содержания заявки и обеспечен срок хранения не менее двух лет.

В случае отсутствия такого правового акта заявка направляется средствами РМСЭД в виде электронного внутреннего документа, подписанного простой ЭП заявителя, на имя руководителя оператора ключей или администратора ключей.

3.2.6. Заявка исполняется не позднее рабочего дня, следующего за днем направления. В случае необходимости в получении дополнительной информации срок исполнения заявки продлевается на периоды запроса и получения такой информации.

3.2.7. При создании ключа простой ЭП администратор ключей:

- с использованием средств базового ПО, на базе англоязычного написания фамилии, имени и отчества формирует уникальный, с учетом наличия однофамильцев и доменного имени, идентификатор владельца ключа простой ЭП (Lotus-имя). Например: Иванов Иван Иванович – Ivan I[.] Ivanov, Ivan Iv[.] Ivanov, Ivan Ivanovich Ivanov и т.д.;
- в качестве альтернативного Lotus-имени указывает оригинальные фамилию, имя, отчество (при наличии);
- назначает временный технологический пароль;
- создает идентификационный файл и принимает меры по его резервному копированию;
- с использованием средств прикладного ПО обеспечивает внесение в базу данных «Структура организации» Участника РМСЭД сведений о владельце ключа простой ЭП в соответствии с предоставленной информацией и осуществляет настройку прав доступа и действий в соответствии с требуемыми полномочиями.

3.2.8. В результате действий по созданию ключа простой ЭП средствами прикладного ПО РМСЭД формируется идентификационный файл. При создании идентификационного файла осуществляется генерация пары ключей шифрования. Публичный ключ помещается в идентификационный файл и в адресной книге (Domino Directory) Участника РМСЭД и доступен (для считывания) всем пользователям. Личный ключ сохраняется только в идентификационном файле и защищается паролем, вводимым при регистрации.

3.2.9. В (основных) подразделениях Участника РМСЭД должны быть определены должностные лица, как правило, из числа специалистов, осуществляющих обслуживание и эксплуатацию локальных информационных систем и автоматизированных рабочих мест (далее – ответственные за эксплуатацию). Информация об ответственных за эксплуатацию за подписью руководителя (основного) подразделения Участника РМСЭД направляется оператору или администратору ключей.

3.2.10. Идентификационный файл и временный технологический пароль администратор ключа с использованием доверенной среды передачи данных направляет ответственному за эксплуатацию и получает подтверждение о его получении.

3.2.11. Ответственный за эксплуатацию на автоматизированном рабочем месте претендента осуществляет необходимые действия по установке (при необходимости), настройке системного и прикладного ПО, установке идентификационного файла. После установления соответствия личности должностного лица, осуществляющего действия на данном автоматизированном рабочем месте, и претендента ознакамливает его с обязанностями владельца, ключа ЭП и сообщает ему временный технологический пароль.

3.3. Обязанность, ответственность и права администратора ключей и оператора ключей простой ЭП

3.3.1. Администратор ключей и оператор ключей обязаны обеспечивать конфиденциальность ключа.

3.3.2. Оператор ключей ведет реестр владельцев ключей, содержащий следующую информацию:

- фамилия, имя, отчество (при наличии) владельца ключа;
- идентификатор владельца ключа;
- дата создания идентификатора;
- дата замены ключа (при замене);
- дата ликвидации ключа (при ликвидации).

Срок хранения записей реестра – пять лет с даты ликвидации ключа.

3.3.3. В случае если в процессе выдачи ключа администратор ключей направил идентификационные данные с нарушением установленной процедуры передачи или направил их лицу, не являющемуся ответственным за эксплуатацию, то гражданско-правовую ответственность, а в случаях, установленных федеральными законами, иную ответственность за неблагоприятные последствия, наступившие для участников отношений в результате допущенной ошибки, несет оператор выдачи ключа.

В случае если в процессе реализации ключа ответственный за эксплуатацию допустил ошибку при установлении личности претендента, то гражданско-правовую ответственность, а в случаях, установленных федеральными законами, иную ответственность за неблагоприятные последствия, наступившие для участников отношений в результате допущенной ошибки, несет

руководитель (основного) подразделения Участника РМСЭД, определивший данное должное лицо в качестве ответственного за эксплуатацию.

3.3.4. При возникновении инцидентов информационной безопасности приостановление действия или ликвидация ключа простой ЭП осуществляется самостоятельно администратором ключей незамедлительно при получении таких сведений с уведомлением владельца ключа ЭП и ответственного за эксплуатацию.

3.4. Обязанность, ответственность и права владельца ключа простой ЭП

3.4.1. Владелец ключа ЭП обязан:

- хранить в тайне ключ ЭП, принимать все возможные меры, предотвращающие нарушение его конфиденциальности;
- исключить возможность его несанкционированного использования третьими лицами;
- заменить назначенный временный технологический пароль личным паролем, сформированным в соответствии с требованиями утвержденной парольной политики;
- формировать ЭП с использованием ключа простой ЭП, полученного в порядке, установленном настоящим Порядком;
- в случае нарушения конфиденциальности ключа простой ЭП или его утери незамедлительно или в ближайший рабочий день уведомить об этом оператора ключа;
- не использовать ключ простой ЭП при наличии оснований полагать, что конфиденциальность данного ключа нарушена.

3.4.2. Гражданско-правовую ответственность за негативные последствия, наступившие в результате несоблюдения владельцем ключа ЭП обязанностей, установленных пунктом 3.4.1 настоящего Порядка, несет владелец ключа ЭП.

3.4.3. Владелец ключа ЭП, чье право было нарушено, должен обратиться к оператору ключа с заявлением о факте несанкционированного использования его простой ЭП. В этом случае оператор ключа аннулирует пароль простой ЭП незамедлительно с момента получения указанного заявления.

3.5. Применение простой ЭП

3.5.1. Действия пользователя, осуществляемые по созданию, изменению (регистрации, согласованию, подписанию и т.д.), открытию документа протоколируются средствами РМСЭД. Информация о пользователе, совершившем действия с документом, дате, времени и сути совершенных изменений с указанием первоначального и конечного состояния измененных реквизитов (полей) документа сохраняется в специализированной базе данных РМСЭД.

3.5.2. В визуальных формах отображения документов РМСЭД, вне зависимости от их вида, отображаются идентификаторы владельцев ключа простой ЭП, осуществивших первое и последнее ключевые действия (создание, подписание, регистрация и т.д.) с документом.

Технические операции РМСЭД, совершаемые с документом в целях обеспечения его доступности, осуществляются от имени служебной записи Administrator и подписываются от ее имени простой ЭП.

3.5.3. В целях установления промежуточных состояний документа РМСЭД или его отдельных реквизитов (полей) оператору ключей направляется запрос в порядке, определяемом Участником РМСЭД или оператором ключей. Рассмотрению подлежат запросы должностных лиц, интересы которых или интересы (основного) подразделения Участника РМСЭД, которое они возглавляют, затронуты в процессе создания, исполнения, изменения или удаления документа РМСЭД, являющегося предметов запроса.

3.6. Проверка соответствия владельца ключа простой ЭП и идентификатора владельца ключа простой ЭП

3.6.1. Базовое и прикладное ПО РМСЭД обеспечивают многофакторную и многоуровневую процедуру авторизации пользователя, в результате которой ему предоставляются назначенные права на доступ к информации и на действия с ней.

3.6.2. Базовое ПО на основании указанного пользователем идентификационного файла (id-файл) и введенного пользователем пароля, осуществляет процедуру взаимной аутентификации, в результате которой определяется однозначное соответствие записи базы данных «Адресная книга» и идентификатора владельца ключа простой ЭП (Lotus-имя).

Прикладное ПО, по Lotus-имени, на основании содержания базы данных «Структура организации» (далее – СО) данного Участника РМСЭД определяет персону, соответствующую исходному идентификатору. По взаимоувязанной информации в базе данных СО определяется запись «Штатная единица», содержащая все данные о роли и полномочиях владельца ключа простой ЭП в РМСЭД.

3.6.3. Взаимодействие владельца ключа простой ЭП и ПО РМСЭД осуществляется с использованием пары личный/публичный ключ на основании криптографических алгоритмов.

3.6.4. Проверка соответствия владельца ключа простой ЭП и идентификатора владельца ключа простой ЭП осуществляется заинтересованным лицом самостоятельно на основании содержания базы данных СО соответствующего Участника РМСЭД.

IV. Правила получения и использования неквалифицированной ЭП

4.1. Требования к среде использования неквалифицированной ЭП

4.1.1. Неквалифицированная ЭП может быть реализована на отдельных автоматизированных рабочих местах, в отдельных информационных системах основных подразделений Участника РМСЭД и подразделений Участника РМСЭД, информационных системах Участника РМСЭД при обеспечении выполнения требований к среде использования простой ЭП и её наличия на

автоматизированном рабочем месте, предназначенном для установки неквалифицированной ЭП.

4.1.2. Участник РМСЭД должен обеспечить реализацию парольной политики РМСЭД с учетом следующих дополнительных требований к среде простой ЭП:

- длина пароля не менее 6 символов (с установкой требования к наличию как минимум одного из требований: наличие символа в верхнем регистре, наличие цифры);
- длина очереди предыдущих паролей – не менее 2 (новый пароль не должен повторять 2 предыдущих);
- срок действия пароля – не более 1 года.

4.2. Порядок создания и выдачи ключей неквалифицированной ЭП

4.2.1. Порядок создания и выдачи ключей неквалифицированной ЭП соответствует порядку создания и выдачи ключей простой ЭП.

4.2.2. Функции оператора ключей и администратора ключей неквалифицированной ЭП возлагаются на оператора ключей и администратора ключей простой ЭП при отражении данного факта в правовых актах, указанных в пункте 3.2.1 настоящего Порядка.

4.2.3. Обязанности, ответственность и права владельца неквалифицированной ЭП, администратора ключей и оператора ключей неквалифицированной ЭП соответствуют аналогичным положениям простой ЭП.

4.3. Применение неквалифицированной ЭП

4.3.1. Применение неквалифицированной ЭП может быть осуществлено для отдельных операций с отдельными видами документов, для которых предусмотрена реализация данной функции.

Подписание документа РМСЭД неквалифицированной ЭП осуществляется дополнительным элементом управления РКК (например, кнопка «Подписать»). Данный элемент становится доступным для использования только при совпадении идентификатора владельца ключа неквалифицированной ЭП или лица, его замещающего в РМСЭД, и должностного лица, указанного в качестве подписанта документа.

Для завершения процедуры подписания документа РМСЭД неквалифицированной ЭП необходимо подтвердить запрос системы на применение ЭП.

4.3.2. Факт подписания документа РМСЭД подтверждается заверительной надписью, отображаемой в нередактируемых областях РКК и содержащей дату и время подписания, а также слово «Подписано» в случае совпадения идентификатора владельца ключа неквалифицированной ЭП должностного лица, осуществившего подписание, и владельца ключа неквалифицированной ЭП, указанного в качестве подписанта документа, или слово «Заверено» в случае, когда процедуру подписания осуществило должностное лицо, являющиеся

замещающим в РМСЭД автора документа. В последнем случае заверительная надпись дополняется указанием фамилии и инициалов должностного лица, осуществившего заверение документа РМСЭД неквалифицированной ЭП.

4.3.3. Защищаемые реквизиты (поля) подписанного проекта документа РМСЭД могут быть изменены автором проекта или лицом, его замещающим в РМСЭД, только после отзыва ранее наложенной подписи. При подписании такого проекта в дальнейшем неквалифицированная ЭП формируется заново.

После регистрации подписанного проекта документа РМСЭД изменение содержания его подписанных реквизитов невозможно.

4.3.4. Техническая реализация РМСЭД подразумевает возможность совместного использование простой ЭП и неквалифицированной ЭП. При использовании неквалифицированной ЭП автоматически применяется и простая ЭП, но не наоборот.

4.4. Проверка соответствия владельца ключа неквалифицированной ЭП и идентификатора владельца ключа неквалифицированной ЭП

4.4.1. При использовании неквалифицированной ЭП дополнительные действия по определению соответствия владельца ключа неквалифицированной ЭП и идентификатора владельца ключа неквалифицированной ЭП не требуются в силу их идентичности.

V. Правила получения и использования квалифицированной ЭП

5.1. Требования к среде использования квалифицированной ЭП

5.1.1. Реализация документационного взаимодействия в РМСЭД с использованием квалифицированной ЭП возможна для Участников РМСЭД, включенных в систему юридически значимого защищенного электронного документооборота автономного округа (далее – СЮЗЗЭД).

5.1.2. Квалифицированная ЭП может быть реализована в информационной системе участника РМСЭД только при обязательном установлении системного времени СЮЗЗЭД, являющейся приоритетной для применения в информационных системах Участника РМСЭД. Данный факт утверждается правовым актом Участника РМСЭД.

Для применения квалифицированной ЭП Участнику РМСЭД необходимо осуществить установку и настройку специализированного модуля Locker предметного ПО РМСЭД, обеспечивающего взаимодействие РМСЭД и средств создания и проверки квалифицированной ЭП.

5.1.3. Квалифицированная ЭП может быть реализована на отдельных автоматизированных рабочих местах при обеспечении наличия на них простой ЭП.

5.1.4. Участник РМСЭД должен обеспечить реализацию парольной политики РМСЭД с учетом следующих дополнительных требований к среде неквалифицированной ЭП:

- длина пароля не менее 6 символов (с установкой следующего требования: наличие символа в верхнем регистре, наличие цифры);

- длина очереди предыдущих паролей – не менее 3 (новый пароль не должен повторять 3 предыдущих);

- срок действия пароля – не более 6 месяцев.

5.2. Порядок создания и выдачи ключей квалифицированной ЭП

5.2.1. Изготовление, предоставление, замена и ликвидация сертификатов и ключей квалифицированной ЭП осуществляется региональным удостоверяющим центром (далее – РУЦ) в порядке, определяемом Регламентом РУЦ. Участник РМСЭД своей доверенностью уполномочивает администратора ключей или иное должностное лицо оператора ключей на осуществление взаимодействия с РУЦ по данным вопросам (далее – уполномоченный).

5.2.2. Уполномоченный централизовано осуществляет сбор требуемого пакета документов должностных лиц, претендующих на получение сертификатов квалифицированной ЭП, и направляет их в РУЦ в электронном виде. При подаче заявления на выпуск сертификата квалифицированной ЭП необходимо указать область применения «РМСЭД».

5.2.3. РУЦ выпускает сертификаты квалифицированной ЭП, производит действия по сопоставлению сертификатов и Lotus-имен пользователей РМСЭД и, используя защищенные каналы связи VipNet, передает ключи квалифицированной ЭП Участнику РМСЭД в лице уполномоченного.

5.2.4. Уполномоченный организует или осуществляет необходимые организационные мероприятия, установку и настройку требуемого ПО на рабочем месте претендента с целью предоставления возможности применения квалифицированной ЭП.

5.3. Применение квалифицированной ЭП

5.3.1. Порядок применения в РМСЭД квалифицированной ЭП совпадает с порядком применения неквалифицированной ЭП.

5.3.2. Техническая реализация РМСЭД подразумевает возможность совместного использования простой ЭП и квалифицированной ЭП. При использовании квалифицированной ЭП одновременно применяется и простая ЭП, но не наоборот.

Совместное использование неквалифицированной ЭП и квалифицированной ЭП невозможно.

VI. Заключительные положения

6.1. Электронный документ РМСЭД может содержать электронные документы, полученные из иных информационных систем электронного документооборота, подписанные любым видом ЭП в порядке, определенным автором (создателем) документа или оператором информационной системы

электронного документооборота – источника получения такого документа. В данном случае документ РМСЭД является контейнером исходного документа и может быть подписан ЭП в порядке, определенном настоящим Порядком, вне зависимости от вида ЭП, использованного автором вложенного документа.