АДМИНИСТРАЦИЯ ГОРНОЗАВОДСКОГО ГОРОДСКОГО ОКРУГА ПЕРМСКОГО КРАЯ

П О С Т А Н О В Л Е Н И Е

11.03.2021 № 208

Об утверждении Положения о порядке работы со средствами криптографической защиты информации в администрации Горнозаводского городского округа Пермского края

Руководствуясь Федеральными законами от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи», постановлением Правительства Российской Федерации от 09 февраля 2012 г. № 111 «Об электронной подписи, используемой органами исполнительной власти и органами местного самоуправления при организации электронного взаимодействия между собой, о порядке ее использования, а также об установлении требований к обеспечению совместимости средств электронной подписи», 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», приказами Федеральной службы безопасности Российской Федерации от 09 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации», 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», приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в

государственных информационных системах», статьями 23, 29 Устава Горнозаводского городского округа Пермского края

администрация Горнозаводского городского округа Пермского края ПОСТАНОВЛЯЕТ:

1. Утвердить прилагаемое Положение о порядке работы со средствами криптографической защиты информации в администрации Горнозаводского городского округа Пермского края (далее - Положение).

2. Руководителям органов администрации Горнозаводского городского округа Пермского края, должностным лицам администрации Горнозаводского городского округа Пермского края, являющихся владельцами сертификата ключа электронной подписи обеспечить исполнение настоящего Положения.

3. Обнародовать настоящее постановление в зданиях, расположенных по адресам: г. Горнозаводск, ул. Кирова, 65, г. Горнозаводск, ул. Свердлова, 59, р.п. Теплая Гора, ул. Советская, 5, р.п. Промысла, ул. Комсомольская, 1, р.п. Кусье-Александровский, ул. Ленина, 2, р.п. Пашия, ул. Ленина, 4, п. Вильва, ул. Пионерская, 6, р.п. Медведка, ул. Октябрьская, 18, п. Средняя Усьва, ул. Советская, 12, р.п. Бисер, ул. Советская, 23, р.п. Старый Бисер, ул. Ермакова, 1, р.п. Сараны, ул. Кирова, 2, а также на официальном сайте администрации Горнозаводского городского округа Пермского края (www.gornozavodskii.ru).

4. Настоящее постановление вступает в силу с момента обнародования.

5. Контроль за исполнением настоящего постановления возложить на управляющего делами администрации Горнозаводского городского округа Пермского края.

Глава городского округа –
глава администрации Горнозаводского
городского округа Пермского края А.Н. Афанасьев

Подлинный экземпляр документа находится в администрации Горнозаводского городского округа Пермского края в деле № 01-07 за 2021 год

Хорсун

D:\картотека\TXT\63178.doc 11

УТВЕРЖДЕНО
постановлением администрации
Горнозаводского городского округа
Пермского края
от 11.03.2021 № 208

ПОЛОЖЕНИЕ
о порядке работы со средствами криптографической защиты информации в администрации Горнозаводского городского округа Пермского края

I. Термины и определения, используемые в настоящем Положении

1.1. Электронная подпись – 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 (далее – ЭП).

1.2. Сертификат ключа проверки электронной подписи – 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.

1.3. Квалифицированный сертификат ключа проверки электронной подписи (далее – квалифицированный сертификат) – сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным Федеральным законом от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи» (далее – Федеральный закон) и иными принимаемыми в соответствии с ним нормативными правовыми актами, созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее – уполномоченный федеральный орган), и являющийся в связи с этим официальным документом.

1.4. Владелец сертификата ключа проверки электронной подписи - лицо, которому в установленном Федеральным законом порядке выдан сертификат ключа проверки электронной подписи.

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

1.6. Ключ проверки электронной подписи - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее – проверка электронной подписи).

1.7. Удостоверяющий центр – юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов

ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом.

1.8. Аккредитация удостоверяющего центра – признание соответствия удостоверяющего центра требованиям Федерального закона.

1.9. Средства электронной подписи – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций – создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

1.10. Средства удостоверяющего центра – программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра.

1.11. Участники электронного взаимодействия – осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, индивидуальные предприниматели, а также граждане.

1.12. Вручение сертификата ключа проверки электронной подписи – передача доверенным лицом удостоверяющего центра созданного этим удостоверяющим центром сертификата ключа проверки электронной подписи его владельцу.

1.13. Подтверждение владения ключом электронной подписи – получение удостоверяющим центром, уполномоченным федеральным органом доказательств того, что лицо, обратившееся за получением сертификата ключа проверки электронной подписи, владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному таким лицом для получения сертификата.

1.14. Журнал учета ключей электронной подписи средств криптографической защиты информации, эксплуатационной и технической документации к ним, сертификатов – документ, содержащий данные о выданных уполномоченным сотрудникам сертификатов.

1.15. Компрометация ключа – утрата доверия к тому, что используемые ключи ЭП обеспечивают безопасность информации, а также используются только конкретным Уполномоченным сотрудником и по назначению.

1.16. Материальный носитель ключевой информации – материальный объект, используемый для записи и хранения информации, необходимой для подписания электронных документов ЭП.

1.17. Участник – юридическое лицо, принимающее участие в юридически значимом электронном документообороте.

1.18. Средства криптографической защиты информации (далее – СКЗИ) – аппаратно-программный комплекс, выполняющий функцию создания ЭП, а также обеспечивающий защиту информации по утвержденным стандартам и сертифицированный в соответствии с действующим законодательством.

1.19. Пользователь СКЗИ – сотрудник Участника, непосредственно допущенный к работе со средствами криптографической защиты информации.

1.20. Статус электронного документа – атрибут электронного документа, идентифицирующий его состояние по определенному признаку.

1.21. Уполномоченный сотрудник – должностное лицо Участника, наделенное полномочиями по подписанию ЭП электронных документов в соответствии с утвержденным Регламентом.

1.22. Усиленная квалифицированная электронная подпись – вид электронной подписи, который соответствует следующим признакам: получена в результате криптографического преобразования информации с использованием ключа электронной подписи; позволяет определить лицо, подписавшее электронный документ; позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания; информация для проверки указана в сертификате.

1.23. Электронный документ (далее – ЭД) – документ, в котором информация представлена в электронной форме.

II. Организация и обеспечение безопасности хранения и применения СКЗИ

2.1. При работе с СКЗИ должны соблюдаться требования «Инструкции об организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащих сведений, составляющих государственную тайну», утвержденную приказом Федерального агентства правительственной связи и информации (ФАПСИ) при Президенте Российской Федерации от 13 июня 2001 г. № 152, нормативно-правовых актов администрации Горнозаводского городского округа Пермского края и настоящего Положения.

2.2. При использовании СКЗИ участники электронного взаимодействия обязаны:

2.2.1. обеспечивать конфиденциальность ключей электронных подписей, в частности не допускать использование принадлежащих им ключей электронных подписей без их согласия;

2.2.2. уведомлять удостоверяющий центр, выдавший сертификат ключа проверки электронной подписи, и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;

2.2.3.не использовать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена;

2.2.4. использовать для создания и проверки квалифицированных электронных подписей, создания ключей квалифицированных электронных

подписей и ключей их проверки средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом.

2.2.5. соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием СКЗИ;

2.2.6. сообщать в орган криптографической защиты о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;

2.2.7. сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

2.2.8. немедленно уведомлять орган криптографической защиты о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.

2.3. Запрещается:

2.3.1. осуществлять несанкционированное копирование ключевых носителей;

2.3.2. разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер и иные средства отображения информации;

2.3.3. записывать на ключевые носители постороннюю информацию;

2.3.4. вносить какие-либо изменения в программное обеспечение средств квалифицированной электронной подписи;

2.3.5. использовать ключевые носители в режимах, не предусмотренных штатным режимом использования ключевого носителя;

2.4. Непосредственно к работе с СКЗИ пользователи допускаются после ознакомления с Инструкцией 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, утвержденной приказом Федерального агентства Правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 г. № 152.

2.5. Ответственность за конфиденциальность сохранения ключа электронной подписи возлагается на владельца ключа ЭП.

2.6. Сертификат действует с момента его выдачи, если в сертификате не указана иная дата начала его действия, и прекращает свое действие в соответствии с условиями, предусмотренными частью 6 статьи 14 Федерального закона от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

2.7. Прекращение действия сертификата, выданного участнику межведомственного электронного взаимодействия на имя его уполномоченного лица, осуществляется в обязательном порядке при смене такого уполномоченного лица, а также в случае нарушения конфиденциальности ключа электронной подписи (компрометация ключа).

III. Порядок обращения с СКЗИ и ключами ЭП

3.1. Для организации и обеспечения безопасности хранения и применения ЭП следует использовать СКЗИ, предусматривающие запись ключей ЭП на материальные носители (компакт-диски (CD-ROM), eToken, RuToken), либо, при хранении ключа ЭП на несъемных носителях информации, парольную защиту с защитой от копирования.

3.2. Длина пароля должна быть не менее 8 символов, пароль должен включать в себя буквы в нижнем и верхнем регистрах, цифры и специальные символы.

3.3. Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключи ЭП подлежат поэкземплярному учету.

3.4. Журнал учета ключей ЭП, эксплуатационной и технической документации к ним (приложение к настоящему Положению) ведет ответственный за эксплуатацию СКЗИ сотрудник Участника.

3.5. Все полученные ответственным за эксплуатацию СКЗИ сотрудником Участника экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключей ЭП должны быть выданы под роспись в соответствующем журнале учета ключей ЭП, несущим персональную ответственность за их сохранность.

3.6. Передача СКЗИ, эксплуатационной и технической документации к ним, ключей ЭП допускается только между пользователями СКЗИ и (или) ответственными за эксплуатацию СКЗИ сотрудниками Участника под роспись в соответствующих журналах учета ключей ЭП.

3.7. Пользователи СКЗИ хранят носители СКЗИ, эксплуатационную и техническую документацию к ним, ключи ЭП в сейфах, в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

3.8. Неиспользованные или выведенные из действия ключевые документы подлежат уничтожению на месте эксплуатации.

3.9. Уничтожение ключей ЭП может производиться путем физического уничтожения материального носителя, на котором они расположены, или путем стирания (разрушения) ключей ЭП без материального носителя (для обеспечения возможности его многократного использования).

3.10. Бумажные и прочие сгораемые материальные носители, а также эксплуатационная и техническая документация к СКЗИ уничтожается путем сжигания или с помощью любых бумагорезательных машин.

3.11. Ключи ЭП должны быть уничтожены в сроки, указанные в эксплуатационной и технической документации к соответствующим СКЗИ. Если срок уничтожения эксплуатационной и технической документации не установлен, то ключи ЭП должны быть уничтожены не позднее 10 суток после вывода их из действия (окончания срока действия). Факт уничтожения оформляется в журнале учета ключей ЭП.

3.12. Ключи ЭП уничтожаются либо пользователем СКЗИ, либо ответственным за эксплуатацию СКЗИ сотрудником Участника под расписку в журнале учета ключей ЭП, а уничтожение большого объема ключей ЭП может быть оформлено актом.

3.13. В случае передачи (списания, сдачи в ремонт) сторонним лицам технических средств, на которых были установлены ключи ЭП, необходимо гарантированно удалить всю информацию, использование которой третьими лицами может потенциально нанести вред организации, в том числе средства квалифицированной ЭП.

VI. Действия в случае компрометации ключей

4.1. Прекращение действия сертификата, выданного участнику межведомственного электронного взаимодействия на имя его уполномоченного лица, осуществляется в обязательном порядке при смене такого уполномоченного лица, а также в случае нарушения конфиденциальности ключа электронной подписи (компрометация ключа).

4.2. К событиям, связанным с компрометацией ключей, относят следующее:

4.2.1. утрата материальных носителей, содержащих ключи ЭП;

4.2.2. потеря материальных носителей, содержащих ключи ЭП, с их последующим обнаружением;

4.2.3. хищение материальных носителей, содержащих ключи ЭП;

4.2.4. разглашение содержимого материальных носителей, содержащих ключи ЭП;

4.2.5. несанкционированное копирование материальных носителей , содержащих ключи ЭП;

4.2.6. увольнении сотрудников, имевших доступ к материальным носителям, содержащим ключи ЭП;

4.2.7. нарушение правил хранения и уничтожения (после окончания срока действия материальных носителей, содержащих ключи ЭП;

4.2.8. возникновение подозрений на утечку содержимого материальных носителей, содержащих ключи ЭП, или ее искажение в Системе;

4.2.9. случаи, когда нельзя достоверно установить, что произошло с материальными носителями (в том числе случаи, когда материальный носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленников);

4.2.10. любые другие виды разглашения содержимого материальных носителей, в результате которых ключи ЭП могут стать доступными посторонним лицам и (или) процессам.

4.3. Уполномоченный сотрудник Участника самостоятельно определяет факт компрометации ключа и оценивает значение этого события. Мероприятия по розыску и локализации последствий компрометации ключа организует и осуществляет организатор с участием Уполномоченного сотрудника Участника (владельца скомпрометированного ключа).

4.4. В случае установления факта компрометации ключа Уполномоченный сотрудник участника обязан незамедлительно прекратить эксплуатацию. В максимально короткие сроки после сообщения о компрометации ключа организатор обеспечивает прекращение использования соответствующего сертификата уполномоченного сотрудника.

4.5. Возобновление работы уполномоченного сотрудника участника происходит только после замены скомпрометированного ключа.

4.6. Для получения новых ключей Уполномоченный сотрудник участника должен руководствоваться порядком получения новых ключей, установленным удостоверяющим центром.

Приложение
к Положению о порядке работы со средствами
криптографической защиты информации в
администрации Горнозаводского городского округа
Пермского края

Журнал учета ключей электронной подписи

№ п/п	Дата начала использования электронной подписи	Ф.И.О. владельца электронной подписи	Тип электронной подписи	Серийный номер сертификата ключа электронной подписи	Дата окончания использования электронной подписи	Подпись
1	2	3	4	5	6	7