ЎЗБЕКИСТОН РЕСПУБЛИКАСИ

«ОЧИҚ КАЛИТЛАР ИНФРАТУЗИЛМАСИГА ҚЎЙИЛАДИГАН ТАЛАБЛАР» МАХСУС ТЕХНИК РЕГЛАМЕНТ

2013 йил

СПЕЦИАЛЬНЫЙ ТЕХНИЧЕСКИЙ РЕГЛАМЕНТ «ТРЕБОВАНИЯ К ИНФРАСТРУКТУРЕ ОТКРЫТЫХ КЛЮЧЕЙ»

2013 год

Расмий нашр

ТОШКЕНТ

Предисловие

1 РАЗРАБОТАН и ВНЕСЕН Экспертным советом в области технического регулирования Государственного комитета связи, информатизации и телекоммуникационных технологий Республики Узбекистан

2 УТВЕРЖДЕН и ВВЕДЕН В ДЕЙСТВИЕ постановлением Узбекского агентства стандартизации, метрологии и сертификации (агентство «Узстандарт») от 4 марта 2013 года № МТР-4

3 ВВЕДЕН ВПЕРВЫЕ

Специальный технический регламент
«Требования к инфраструктуре открытых ключей»

ГЛАВА I. ОБЩИЕ ПОЛОЖЕНИЯ

§ 1. Область применения

1. Настоящий специальный технический регламент «Требования к инфраструктуре открытых ключей» (далее – технический регламент) устанавливает обязательные требования к национальной инфраструктуре открытых ключей, обеспечению конфиденциальности и целостности информации, безопасности помещений, персоналу, сертификатам ключей электронной цифровой подписи, бланкам свидетельств о регистрации, доверенной третьей стороне.

2. Объектами регулирования настоящего технического регламента являются орган регистрации, центры регистрации ключей электронной цифровой подписи. Пользователями являются органы государственной власти и управления, хозяйствующие субъекты, физические лица.

3. Настоящий технический регламент распространяется на орган регистрации и центры регистрации ключей электронной цифровой подписи, функционирующие в Республике Узбекистан.

§ 2. Термины, определения и сокращения

4. В настоящем техническом регламенте применены следующие понятия:

аппаратное средство - специальное устройство или приспособление, предназначенное для обеспечения защиты информации и входящее в комплект технических средств обработки информации;

аутентификация - проверка и подтверждение подлинности определенных реквизитов или идентификаторов, предъявляемых субъектом;

доверенная третья сторона - организация, наделенная правом осуществлять деятельность по предоставлению услуг по проверке электронной цифровой подписи в электронных документах в фиксированный момент времени в отношении отправителя или получателя электронного документа и являющаяся доверенным субъектом, связанным с этими услугами.

закрытый ключ электронной цифровой подписи - последовательность символов, полученная с использованием средств электронной цифровой подписи, известная только подписывающему лицу и предназначенная для создания электронной цифровой подписи в электронном документе;

идентификация - присвоение субъектам и объектам доступа идентификатора и/или сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов;

информационное взаимодействие - процесс взаимодействия двух и более субъектов, целью и основным содержанием которого является изменение имеющейся информации хотя бы у одного из них;

инфраструктура открытых ключей - техническая и организационная инфраструктура, которая обеспечивает поддержку использования технологий криптопреобразований с открытым ключом;

ключ (ключевая информация) - последовательность символов, управляющая операциями шифрования и расшифрования;

компрометация – непреднамеренное раскрытие или обнаружение криптографического ключа или кода.

конфиденциальная информация - документированная информация, не содержащая информацию, отнесенную к государственным секретам, доступ к которой ограничивается в соответствии с законодательством;

несанкционированный доступ к информации - доступ субъекта к информации в нарушение установленных в системе правил разграничения доступа;

орган регистрации центров регистрации ключей электронной цифровой подписи - уполномоченный орган в области применения электронной цифровой подписи, осуществляющий государственную регистрацию Центров регистрации ключей электронной цифровой подписи;

проверка подлинности сертификата - действия, производимые над проверяемым сертификатом ключа электронной цифровой подписи для того, чтобы убедиться в возможности его использования, включая проверку целостности сертификата, области действия сертификата, срока действия сертификата, отсутствия сертификата в актуальном списке отозванных сертификатов;

профиль защиты - независимая от реализации совокупность требований безопасности для некоторой категории объектов, отвечающая специфическим запросам потребителя;

реестр сертификатов - хранилище, содержащее сертификаты и списки отозванных сертификатов в электронном виде и служащее для распространения этих объектов среди пользователей;

режимные помещения – помещения, для которых установлены дополнительные меры безопасности;

сертификат ключа электронной цифровой подписи - электронный документ, подтверждающий соответствие открытого ключа электронной цифровой подписи закрытому ключу электронной цифровой подписи и выданный центром регистрации владельцу закрытого ключа электронной цифровой подписи;

средства криптографической защиты информации - аппаратные, программные или аппаратно-программные средства, осуществляющие криптографические преобразования информации для обеспечения ее безопасности, в том числе:

а) средства шифрования - аппаратные, программные и аппаратно-программные средства, реализующие криптографические алгоритмы преобразования информации и предназначенные для защиты информации от несанкционированного доступа при ее обработке, хранении и передаче по каналам связи;

б) средства имитозащиты - аппаратные, программные и аппаратно-программные средства, реализующие криптографические алгоритмы преобразования информации и предназначенные для защиты от навязывания ложной информации;

в) средства электронной цифровой подписи - совокупность технических и программных средств, обеспечивающих создание электронной цифровой подписи в электронном документе, подтверждение подлинности электронной цифровой подписи, создание открытых и закрытых ключей электронной цифровой подписи;

г) средства кодирования - средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций;

д) средства изготовления ключевых документов и сами ключевые документы (независимо от вида носителя ключевой информации);

уполномоченное лицо центра регистрации - сотрудник центра регистрации, действующий от его имени на основании устава, договора, доверенности на право совершения соответствующих действий;

центр регистрации ключей электронной цифровой подписи - юридическое лицо, прошедшее государственную регистрацию в уполномоченном органе и осуществляющее деятельность по выдаче сертификатов ключей электронной цифровой подписи;

электронный документ - информация, зафиксированная в электронной форме, подтвержденная электронной цифровой подписью и имеющая другие реквизиты электронного документа, позволяющие его идентифицировать.

5. В настоящем техническом регламенте применяются следующие сокращения:

VLAN – виртуальная локальная сеть;

НСД – несанкционированный доступ;

СКЗИ – средство криптографической защиты информации;

СОС – список отозванных сертификатов;

ЭД – электронный документ;

ЭЦП – электронная цифровая подпись.

ГЛАВА II. ОБЩИЕ ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ

§ 1. Административные требования

6. Администрация органа регистрации (центра регистрации) ЭЦП обязана обеспечивать:

1) предотвращение НСД, утечки, хищения, утраты, искажения, блокировки, подделки информации;

2) сохранность информации в реестре сертификатов ключей ЭЦП;

3) надежность работы и предотвращение несанкционированных действий, направленных на нарушение нормального функционирования аппаратно-программных средств, обеспечивающих выполнение ими своих функций, а также средств криптографической защиты информации;

4) защиту сведений, содержащих конфиденциальную информацию органа регистрации (центра регистрации) ЭЦП.

Информационная безопасность обеспечивается путем реализации органом регистрации (центром регистрации) ЭЦП комплекса организационных и инженерно-технических мероприятий, изложенных в главах II-VI настоящего технического регламента.

Приказом руководителя из сотрудников органа регистрации (центра регистрации) ЭЦП назначается ответственное за безопасность лицо.

Защите подлежат сведения, содержащие конфиденциальную информацию, хранимую, обрабатываемую и передаваемую органом регистрации (центром регистрации) ЭЦП в электронном виде и/или на ином носителе.

§ 2. Требования к функциональному разграничению

7. Для выполнения функций органом регистрации (центром регистрации) ЭЦП используется функциональное разграничение членов группы администраторов:

1) администраторы сертификации, в основные обязанности которых входит: выдача и отзыв сертификатов ЭЦП, ведение реестра сертификатов, СОС;

2) администраторы регистрации, в основные обязанности которых входит: взаимодействие с пользователями, прием документов от пользователей, генерация и выдача ключей ЭЦП, проверка ЭЦП.

§ 3. Требования к программному обеспечению

8. Орган регистрации (центры регистрации) ЭЦП должны использовать программные СКЗИ, прошедшие сертификацию в органе по сертификации СКЗИ.

Программное обеспечение органа регистрации (центра регистрации) ЭЦП не должно содержать средств отладки программ, позволяющих модифицировать или искажать алгоритм работы программно-технических средств органа регистрации (центра регистрации) ЭЦП.

§ 4. Требования к аппаратным компонентам

9. При использовании органом регистрации (центрами регистрации) ЭЦП аппаратных СКЗИ, данные СКЗИ должны быть сертифицированы в органе по сертификации СКЗИ.

Аппаратные средства, на которых реализуются СКЗИ, не должны позволять модифицировать или искажать алгоритм работы технических средств органа регистрации (центра регистрации) ЭЦП.

§ 5. Требования по защите от НСД

10. Технические средства органа регистрации (центра регистрации) ЭЦП должны быть защищены от воздействий со стороны внешних сетей передачи данных сертифицированными программными и аппаратно-программными средствами.

Исходя из уровня защиты от НСД, при разработке органа регистрации (центра регистрации) ЭЦП должен быть построен профиль защиты органа регистрации (центра регистрации) ЭЦП, включающий:

1) архитектуру построения органа регистрации (центра регистрации) ЭЦП и принципы взаимодействия объектов органа регистрации (центра регистрации) ЭЦП;

2) описание уточненных возможностей нарушителя;

3) описание механизмов и средств защиты от НСД;

4) описание механизмов аудита и формата данных аудита;

5) перечень защищаемых объектов органа регистрации (центра регистрации) ЭЦП;

6) перечень сотрудников органа регистрации (центра регистрации) ЭЦП;

7) политику безопасности органа регистрации (центра регистрации) ЭЦП (в том числе, правила разграничения доступа, правила пользования операторов и администраторов органа регистрации (центра регистрации) ЭЦП, описание действий в нештатных ситуациях, правила фильтрации межсетевых экранов).

Все положения профиля защиты органа регистрации (центра регистрации) ЭЦП должны быть отражены в документе «Политика безопасности органа регистрации (центра регистрации) ключей ЭЦП».

Для защиты средств вычислительной техники, входящих в состав органа регистрации (центра регистрации) ЭЦП, должны использоваться устройства типа «электронный замок».

§ 6. Требования к целостности технических средств

11. В органе регистрации (центре регистрации) ЭЦП должен производиться контроль несанкционированного случайного или преднамеренного искажения или разрушения информации, программных и аппаратных компонентов.

Контроль целостности должен выполняться не реже одного раза в сутки.

В органе регистрации (центре регистрации) должны быть предусмотрены средства восстановления целостности технических средств органа регистрации (центра регистрации) ЭЦП.

§ 7. Требования к аутентификации

12. Для аутентификации членов группы администраторов при их обращении к средствам вычислительной техники, входящим в состав органа регистрации (центра регистрации) ЭЦП, должен применяться символьный периодически изменяющийся па-

роль (8 символов и более) при использовании буквенно-цифровых знаков латинского алфавита независимо от регистра. Период изменения пароля - тридцать дней.

Администрация органа регистрации (центра регистрации) ЭЦП должна:

1) обеспечить реализацию механизма аутентификации удаленных пользователей при их обращении к техническим средствам органа регистрации (центра регистрации) ЭЦП;

2) точно определить список всех действий пользователя, выполнение которых разрешено до его идентификации и аутентификации. Выполнение остальных действий должно разрешаться только после успешной идентификации и аутентификации пользователя;

3) обеспечить реализацию механизма аутентификации локальных пользователей, имеющих доступ к техническим средствам, входящим в состав органа регистрации (центра регистрации) ЭЦП, но не входящим в состав группы администраторов;

4) обеспечить реализацию механизма ограничения числа безуспешных попыток аутентификации членов группы администраторов и локальных пользователей при их обращении к средствам вычислительной техники, входящей в состав органа регистрации (центра регистрации) ЭЦП.

§ 8. Требования к защите данных, поступающих и экспортируемых из органа регистрации (центра регистрации) ЭЦП

13. Орган регистрации (центр регистрации) ЭЦП должен обеспечивать передачу данных, защищенных от НСД, криптографическим способом.

Для взаимодействия элементов органа регистрации (центра регистрации) ЭЦП в составе сети должна выделяться VLAN, доступная только определенному органу регистрации (центру регистрации) ЭЦП и его элементам.

Взаимодействие между органом регистрации (центром регистрации) ЭЦП должно выполняться с использованием защищенных и сертифицированных протоколов.

Для обеспечения бесперебойности работы органа регистрации (центра регистрации) ЭЦП выделяемые каналы связи должны резервироваться.

В органе регистрации (центре регистрации) ЭЦП должен быть реализован механизм защиты от имитации сообщения. Под «имитацией сообщения» понимается навязывание нарушителем ложных данных, которые воспринимаются органом регистрации (центром регистрации) ЭЦП как действительная информация, защищенная от НСД.

§ 9. Требования к хранению информации на бумажных, магнитных и оптических носителях

14. Все резервные материалы, документация и устройства хранения информации органа регистрации (центра регистрации) ЭЦП должны храниться в защищенных помещениях и пожаробезопасных местах.

Все съемные носители информации должны поштучно регистрироваться и учитываться (приложение 1), они должны храниться в местах, защищенных от возможности случайного или намеренного изменения информации.

Конфиденциальная информация органа регистрации (центра регистрации) ЭЦП на бумажных, магнитных и оптических носителях должна храниться в сейфах или в железных шкафах или ящиках, которые опечатываются печатью ответственных лиц.

§ 10. Требования к регистрации событий

15. В органе регистрации (центре регистрации) ЭЦП должен быть реализован механизм, производящий регистрацию в электронном журнале органа регистрации (центра регистрации) ЭЦП событий, связанных с выполнением органом регистрации (центром регистрации) ЭЦП своих целевых функций.

Список регистрируемых событий включает выпуск и отзыв сертификата, запрос на сертификацию и сообщение о компрометации, приостановке и возобновлении действия сертифицированных ключей.

Структура записи должна включать обязательные поля:

дату и время события;

тип события;

идентификатор пользователя, выполнившего операцию, соответствующую регистрируемому событию;

результат операции: положительный или отрицательный.

Членами группы администраторов должны быть приняты меры для обнаружения и предотвращения несанкционированных записей в журнале аудита.

§ 11. Требования к резервному копированию и восстановлению

16. В органе регистрации (центре регистрации) ЭЦП должны быть реализованы одноразовое резервное копирование и механизм восстановления на случай повреждения технических средств или информации.

Должны быть приняты меры обнаружения несанкционированных изменений сохраненных данных.

ГЛАВА III. ТРЕБОВАНИЯ БЕЗОПАСНОСТИ К ПОМЕЩЕНИЯМ ОРГАНА РЕГИСТРАЦИИ (ЦЕНТРА РЕГИСТРАЦИИ) ЭЦП

§ 1. Требования к размещению технических средств

17. Доступ к техническим средствам должен иметь только уполномоченный персонал.

Серверы и оборудование телекоммуникаций должны быть размещены в выделенном специальном помещении.

Серверы и оборудование телекоммуникаций должны быть установлены в специальных стойках.

Технические средства, используемые персоналом органа регистрации (центра регистрации) ЭЦП, должны быть размещены в рабочих помещениях по схеме организации рабочих мест персонала.

Сервера должны постоянно находиться в режиме ручного или электронного обнаружения НСД.

§ 2. Физический доступ

18. Физический доступ к техническим средствам органа регистрации (центра регистрации) ЭЦП должен удовлетворять следующим требованиям:

1) серверное помещение должно быть оборудовано системой контроля доступа, включая систему видеонаблюдения в видимом и инфракрасном спектре;

2) все двери, окна и другие пути доступа в помещения органа регистрации (центра регистрации) ЭЦП должны быть оборудованы защитными приспособлениями и сигнализацией, предотвращающими несанкционированные проникновения в помещения, а также просмотр, прослушивание и съем электромагнитного излучения;

3) помещения органа регистрации (центра регистрации) ЭЦП должны быть оснащены охранной сигнализацией, связанной с охранным помещением, пультом централизованного наблюдения за сигнализацией или с дежурным по сигнализации;

4) система сигнализации должна быть защищена дублирующей системой и средствами электропитания, гарантирующими функционирование в случае отключения внешнего электропитания;

5) доступом без сопровождения к техническим средствам органа регистрации (центра регистрации) ЭЦП должен обладать только персонал, определенный в списке доступа;

6) персонал, не находящийся в списке доступа, должен сопровождаться и контролироваться уполномоченным лицом органа регистрации (центра регистрации);

7) должен вестись журнал доступа к техническим средствам органа регистрации (центра регистрации) ЭЦП;

8) идентификационные средства доступа в серверное помещение должны выдаваться сотрудникам по приказу руководителя;

9) ключи механических замков рабочих помещений должны выдаваться сотрудникам по распоряжению руководителя на основании схемы организации рабочих мест персонала;

10) контроль целостности технических средств органа регистрации (центра регистрации) ЭЦП должен осуществляться при каждом обращении к органу регистрации (центру регистрации) ЭЦП, но не реже одного раза в неделю;

11) оборудование в активированном состоянии должно быть защищено от НСД;

12) после ввода пароля, защищающего секретный ключ, пользователи не должны оставлять свои рабочие места без присмотра.

ГЛАВА IV. ТРЕБОВАНИЯ К ПЕРСОНАЛУ

§ 1. Объекты оценки персонала

19. Объектами оценки являются: уполномоченное лицо и персонал, осуществляющие свою деятельность в органе регистрации (центре регистрации).

Уполномоченное лицо органа регистрации (центра регистрации) в соответствии со структурой органа регистрации (центра регистрации) относится к административной службе.

Административная служба предназначена для решения задач по управлению деятельностью органа регистрации (центра регистрации), координации деятельности остальных служб органа регистрации (центра регистрации) и взаимодействию с пользователями в части разрешения вопросов, связанных с предоставлением услуг.

Персонал органа регистрации (центра регистрации) в соответствии со структурой относится к одному из следующих организационных подразделений (служб):

1) служба регистрации;

2) служба безопасности;

3) техническая служба.

Служба регистрации предназначена для решения задач по предоставлению пользователю услуг органа регистрации (центра регистрации): выдача сертификатов ключей ЭЦП, приостановление, возобновление действия сертификатов и их аннулирование, ведение реестра сертификатов ключей ЭЦП.

Служба безопасности предназначена для решения задач по организации и выполнению мероприятий по защите ресурсов органа регистрации (центра регистрации), а также по изготовлению и предоставлению ключей ЭЦП по обращению пользователей.

Техническая служба предназначена для решения задач по организации и выполнению мероприятий по эксплуатации программных и технических средств обеспечения деятельности органа регистрации (центра регистрации) и по техническому сопровождению распространяемых им средств ЭЦП и шифрования.

Службы возглавляют начальники служб, назначаемые приказом руководителя органа регистрации (центра регистрации).

§ 2. Общие требования к уполномоченному лицу органа регистрации (центра регистрации)

20. К уполномоченному лицу органа регистрации (центра регистрации), как минимум, должны предъявляться следующие общие требования:

1) наличие допуска к конфиденциальной информации и полное доверие (иметь рекомендации, характеристики);

2) знание политики безопасности и соблюдение её требования в своей деятельности;

3) отсутствие в послужном списке отстранений от должности за служебное несоответствие или несоблюдение правил работы;

4) необходимое обучение и инструктаж по выполнению обязанностей.

Уполномоченное лицо органа регистрации (центра регистрации) должно решать следующие возложенные на него задачи:

1) организовывать и обеспечивать работу органа регистрации (центра регистрации) для выполнения им своих функций в соответствии с требованиями Закона Рес-

публики Узбекистан «Об электронной цифровой подписи», «Положения о порядке деятельности центров регистрации ключей электронных цифровых подписей», утвержденного постановлением Кабинета Министров Республики Узбекистан от 26.09.05 г. №215, и Устава органа регистрации (центра регистрации);

2) контролировать выполнение службами органа регистрации (центра регистрации) своих задач и обязанностей;

3) заключать договора с пользователями на оказание услуг органа регистрации (центра регистрации);

4) принимать меры по защите своего закрытого ключа ЭЦП и использовать его в целях, определенных законодательством;

5) подписывать сертификаты ключей ЭЦП, выдаваемых органом регистрации (центром регистрации), и нести ответственность за их уникальность и полноту представленной в них информации в соответствии с требованиями законодательства в области использования ЭЦП;

6) подписывать список отозванных сертификатов ключей ЭЦП и нести ответственность за достоверность фактов отзыва сертификатов.

§ 3. Общие требования к персоналу органа регистрации (центра регистрации)

21. Профессиональная пригодность персонала органа регистрации (центра регистрации) определяется наличием у них знаний, умений и способностей по прикладному и системному программированию, опыта обслуживания и поддержки инфраструктуры открытых ключей, компьютерных сетей и Интернет. Персонал службы регистрации также должен обладать знаниями по криптологии.

Персонал должен:

1) выполнять требования защиты конфиденциальной информации и информационной безопасности органа регистрации (центра регистрации);

2) эксплуатировать программные и технические средства в соответствии с эксплуатационно-технической документацией.

§ 4. Требования к персоналу органа регистрации (центра регистрации) в области защиты конфиденциальной информации при особых условиях или чрезвычайных ситуациях

22. Для обеспечения защиты конфиденциальной информации при особых условиях или чрезвычайных ситуациях персоналом должны проводиться меры по резервированию серверов центра регистрации ключей ЭЦП с установкой на них полнофункциональной программы, резервированию базы данных центра регистрации.

При восстановлении данных персоналом должно обеспечиваться:

- копирование данных центра регистрации на внешние носители;
- восстановление базы данных на основе резервной копии данных.

Восстановлению должны подлежать сертификаты открытых ключей ЭЦП.

ГЛАВА V. ТРЕБОВАНИЯ К КОНФИДЕНЦИАЛЬНОСТИ

§ 1. Конфиденциальная информация

23. Конфиденциальной информацией органа регистрации (центра регистрации) является:

1) персональные данные владельцев ЭЦП, хранящиеся в органе регистрации (центре регистрации) и не подлежащие непосредственной рассылке в качестве части сертификата ключа ЭЦП или списков выданных, приостановленных, возобновленных и аннулированных сертификатов. Данная информация не подлежит публикации;

2) закрытый ключ уполномоченного лица органа регистрации (центра регистрации);

3) парольная информация органа регистрации (центра регистрации);

4) информация, хранящаяся в журналах аудита;

5) отчетные материалы по выполненным проверкам деятельности органа регистрации (центра регистрации) (за исключением заключения по результатам проверок);

6) сведения, связанные с коммерческой деятельностью (коммерческая тайна).

Конфиденциальная информация является информацией ограниченного распространения. Документы, содержащие конфиденциальную информацию, должны иметь гриф «Для служебного пользования».

Защита конфиденциальной информации является одной из основных задач в области обеспечения информационной безопасности органа регистрации (центра регист-

рации) и осуществляется режимными и организационно-техническими мероприятиями в комплексе с Системой защиты конфиденциальной информации (глава V, §2).

Орган регистрации (центр регистрации) не должен раскрывать конфиденциальную информацию третьим лицам за исключением случаев, требующих ее раскрытия в соответствии с действующим законодательством или при наличии решения суда.

Конфиденциальная информация органа регистрации (центра регистрации) может храниться в электронной форме и/или на бумажных носителях.

Информация, не являющаяся конфиденциальной информацией, является открытой информацией и может публиковаться органом регистрации (центром регистрации). Место, способ и время публикации также определяется органом регистрации (центром регистрации).

Не считается конфиденциальной информация, включаемая:

1) в сертификаты ключей ЭЦП;

2) в списки выданных, приостановленных, возобновленных и аннулированных сертификатов ключей ЭЦП, издаваемых органом регистрации (центром регистрации);

3) в публикуемое заключение по результатам проверок деятельности центра регистрации.

Закрытые ключи владельцев ЭЦП, соответствующие сертификату ключа ЭЦП, являются конфиденциальной информацией этих пользователей.

Владельцы ЭЦП обязаны обеспечить контроль за использованием закрытых ключей ЭЦП, защищать свои закрытые ключи ЭЦП и принимать все возможные меры для предотвращения их компрометации.

Орган регистрации (центр регистрации) не депонирует и не архивирует закрытые ключи ЭЦП, а также не создает их дубликаты.

Защита архивируемой конфиденциальной информации должна осуществляться методами физического обеспечения безопасности или комбинацией методов физической и криптографической защиты.

Все резервные файлы архивируемой конфиденциальной информации должны храниться в защищенном и, при возможности, в географически удаленном месте.

Персонал органа регистрации (центра регистрации), имеющий по роду своей деятельности прямое отношение к обработке, передаче, приему и хранению конфиденциальной информации, допускается к работе с СКЗИ только после подписания обязательства о неразглашении конфиденциальной информации (далее – Обязательство). Ответственность за разглашение конфиденциальной информации должна быть определена в тексте Обязательства.

В случае нарушения требований вышеуказанного Обязательства руководство органа регистрации (центра регистрации) может приостановить допуск соответствующего сотрудника к СКЗИ и конфиденциальной информации.

Обязанности между сотрудниками органа регистрации (центра регистрации) должны быть распределены с учетом персональной ответственности за сохранность СКЗИ, ключевых носителей и документов, а также за порученные участки работы.

При определении обязанностей сотрудников органа регистрации (центра регистрации) должно быть учтено, что безопасность хранения, обработки и передачи конфиденциальной информации с использованием СКЗИ обеспечивается:

- соблюдением режима конфиденциальности при обращении со сведениями, которые им доверены или стали известны по работе, в том числе со сведениями о функционировании и порядке обеспечения безопасности применяемых СКЗИ и ключевых носителей;

- точным выполнением требований по обеспечению безопасности конфиденциальной информации;

- надежным хранением СКЗИ, эксплуатационной и технической документации к ним, ключевых носителей и носителей конфиденциальной информации;

- своевременным выявлением попыток посторонних лиц получить сведения о защищаемой конфиденциальной информации, об используемых СКЗИ или ключевых носителях;

- немедленным принятием мер по предупреждению разглашения защищаемых сведений конфиденциального характера, а также возможной утечки таких сведений при выявлении фактов утраты или недостачи СКЗИ, ключевых носителей, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т.п.

Орган регистрации и центры регистрации ключей ЭЦП должны иметь лицензию на использование СКЗИ, если на данном объекте используются СКЗИ для защиты информации ограниченного доступа или лицензию на иные виды деятельности, если лицензирование данного вида деятельности обязательно.

§ 2. Система защиты конфиденциальной информации

24. Система защиты конфиденциальной информации информационной системы органа регистрации (центра регистрации) должна включать в себя следующие подсистемы:

1) криптографической защиты информации, включающей в себя программные и/или программно-аппаратные СКЗИ;

2) защиты информации от НСД, включающей в себя программные и/или программно-аппаратные средства аутентификации и идентификации, разграничения доступа, межсетевые экраны;

3) активного аудита информационной безопасности органа регистрации (центра регистрации);

4) обнаружения вторжений;

5) резервного копирования и архивирования данных;

6) обеспечения целостности информации, программных и аппаратных средств, в том числе криптографическими методами;

7) обеспечения безотказной работы, включающей в себя антивирусные средства;

8) защиты оборудования от утечки информации по техническим и побочным каналам;

9) обеспечения защиты информации от НСД режимными и организационно-техническими мероприятиями.

§ 3. Ответственность органа (центра) регистрации и владельца ЭЦП при использовании конфиденциальной информации

25. Орган регистрации (центр регистрации) несет ответственность за разглашение конфиденциальной информации.

Распределение ответственности в области защиты конфиденциальной информации между органом регистрации, центром регистрации, владельцами и пользователями ЭЦП закрепляется через заключаемые договора.

При выдаче сертификата ключа ЭЦП владельцу ЭЦП органом регистрации (центром регистрации) должна быть дана полная информация о правилах пользования и хранения ключей ЭЦП, а также об обязанностях и ответственности владельца ЭЦП.

При компрометации закрытого ключа владельца ЭЦП по вине органа регистрации (центра регистрации) последний несет ответственность за понесенный владельцем ЭЦП материальный ущерб, а также бесплатно изготавливает и выдает ему новый сертификат ключа ЭЦП.

Центр регистрации не несет ответственность за последствия компрометации владельцем ЭЦП своего закрытого ключа ЭЦП.

§ 4. Основные режимные и организационно-технические мероприятия

26. К основным режимным мероприятиям в области защиты конфиденциальной информации органа регистрации (центра регистрации) относятся следующие мероприятия:

1) исключение возможности бесконтрольного проникновения в помещения, в которых размещаются технические средства органа регистрации (центра регистрации) со встроенными СКЗИ (далее – режимные помещения), посторонних лиц;

2) исключение возможности визуального просмотра документов с конфиденциальной информацией, в том числе и с экранов мониторов, на которых она отражается, через окна (путем соответствующего размещения технических средств в режимном помещении);

3) обеспечение сохранности находящихся в режимных помещениях документов с конфиденциальной информацией и технических средств;

4) оборудование входных дверей режимных помещений замками, обеспечивающими надежное закрытие помещений в нерабочее время;

5) оборудование окон и дверей охранной сигнализацией, а режимных помещений средствами видеонаблюдения, связанными с пультом централизованной охраны;

6) ограничение допуска в режимные помещения. Допуск в эти помещения могут иметь только руководитель органа регистрации (центра регистрации), сотрудники подразделения безопасности и персонал, имеющий прямое отношение к обработке, передаче, приему и хранению конфиденциальной информации;

7) оборудование средствами контроля вскрытия системных блоков компьютеров с СКЗИ;

8) осуществление ремонта и/или последующего использования системных блоков только после гарантированного удаления с них программного обеспечения СКЗИ и конфиденциальной информации;

9) обновление оборудования органа регистрации (центра регистрации) должно производиться доверенным и подготовленным персоналом;

10) обеспечение соответствия вышеуказанных режимных помещений требованиям техники безопасности, санитарным нормам и требованиям пожарной безопасности.

К основным организационно-техническим мероприятиям в области защиты конфиденциальной информации органа регистрации (центра регистрации) относятся:

1) определение должностных лиц, ответственных за обеспечение информационной безопасности и эксплуатацию СКЗИ;

2) поэкземплярный учет используемых СКЗИ, эксплуатационной и технической документации к ним, а также ключевых носителей;

3) определение степени конфиденциальности обрабатываемой и хранимой информации;

4) разработка модели нарушителя;

5) использование сертифицированных средств защиты информации;

6) эксплуатация объекта информатизации в соответствии с условиями и требованиями, установленными аттестатом соответствия, нормативно-правовыми актами и иными документами в области информационной безопасности;

7) разработка нормативных документов, регламентирующих вопросы защиты конфиденциальной информации и эксплуатации СКЗИ, а также инструкций по соблюдению правил обеспечения защиты конфиденциальной информации как для персонала органа регистрации (центра регистрации), так и для владельцев и пользователей ЭЦП;

8) допуск к работе с СКЗИ персонала органа регистрации (центра регистрации), имеющего навыки работы на персональном компьютере и ознакомленного с правилами эксплуатации СКЗИ;

9) предоставление прав доступа к обработке конфиденциальной информации только персоналу, имеющему допуск к работе с указанной информацией;

10) контроль и обеспечение соблюдения требований использования СКЗИ, установленных в их эксплуатационной и технической документации;

11) расследование и составление заключений по фактам нарушения требований использования СКЗИ; разработка и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

12) организация выдачи ключей механических замков рабочих помещений органа регистрации (центра регистрации) его сотрудникам по распоряжению руководства на основании схемы организации рабочих мест персонала;

13) регистрация прихода/ухода персонала органа регистрации (центра регистрации) в соответствующем журнале или с помощью автоматизированной системы.

ГЛАВА VI. ТРЕБОВАНИЯ К КЛЮЧЕВОЙ ИНФОРМАЦИИ

27. К ключевой информации, формируемой и/или хранимой в органе регистрации (центре регистрации), относятся следующие пары закрытых и открытых ключей ЭЦП:

1) ключ уполномоченного лица органа регистрации (центра регистрации), используемый для подписи сертификатов и списков выданных, приостановленных, возобновленных и аннулированных сертификатов;

2) ключи шифрования сервера органа регистрации (центра регистрации).

Секретный ключ, используемый для подписи сертификатов и средств отозванных сертификатов, не должен использоваться ни для каких иных целей.

Секретный ключ ЭЦП и ключ шифрования должны храниться на специальном съемном носителе, не допускающем извлечение и копирование секретного ключа ЭЦП без специального программного обеспечения на другой носитель информации.

В органе регистрации (центре регистрации) ЭЦП должен быть реализован механизм хранения в памяти средств вычислительной техники, входящих в состав органа регистрации (центра регистрации) ЭЦП, ключевой информации, включая секретные ключи ЭЦП, с предварительным их шифрованием.

Должен быть обеспечен срок действия секретного ключа центра регистрации ЭЦП не менее одного года.

В целях защиты конфиденциальной ключевой информации руководством и ответственным персоналом органа регистрации (центра регистрации) должно обеспечиваться выполнение следующих мероприятий:

1) поэкземплярный учет в журналах:

а) носителей с секретными ключами шифрования;

б) инсталляционных дискет с программным обеспечением СКЗИ;

2) определение сотрудников, ответственных за учет и хранение закрытых (секретных) ключей ЭЦП;

3) выделение сейфа или иного хранилища, обеспечивающего сохранность ключевой информации, для хранения носителей с закрытыми (секретными) ключами ЭЦП и шифрования;

4) исключение непреднамеренного уничтожения или иного, не предусмотренного правилами пользования СКЗИ, применения ключей и инсталляционных дискет с

программным обеспечением СКЗИ в случае их хранения в одном хранилище с другими документами;

5) изготовление одного дубликата ключевого носителя, предназначенного для использования в случае физического выхода из строя основного (рабочего) носителя;

6) раздельное хранение рабочего и резервного ключевых носителей; создание условий, при которых будет невозможна их одновременная компрометация;

7) создание условий при транспортировке ключевых носителей с закрытой (секретной) ключевой информацией, обеспечивающих их защиту от физических повреждений и внешнего воздействия на записанную ключевую информацию.

Категорически запрещается:

1) вносить несанкционированные изменения в Систему защиты конфиденциальной информации, описанную в главе V §2;

2) осуществлять несанкционированное копирование ключевой информации;

3) хранить ключевые носители вне специально установленных для этого мест;

4) выдавать ключевые носители лицам, не допущенным к работе с ними;

5) во время перерывов в работе оставлять ключевые носители без присмотра в устройствах считывания персонального компьютера, на рабочем месте, шкафах и ящиках, для этого не предназначенных;

6) производить уничтожение ключей на ключевых носителях после окончания срока их действия или хранения, а также после их выведения из действия способами, отличными от определенных в эксплуатационной документации на СКЗИ;

7) проносить и использовать в помещениях, где размещены СКЗИ, сотовые телефоны, радиотелефоны и другую излучающую радиоэлектронную аппаратуру.

ГЛАВА VII. ИЗГОТОВЛЕНИЕ БЛАНКОВ СВИДЕТЕЛЬСТВ О РЕГИСТРАЦИИ

§ 1. Изготовление бланков

28. Изготовление бланков свидетельств о государственной регистрации центров регистрации ключей ЭЦП (далее - свидетельств о регистрации) осуществляется полиграфическими предприятиями, прошедшими регистрацию в Узбекском агентстве по печати и информации Республики Узбекистан, имеющими разрешение органов внутренних дел и включенными в перечень предприятий, имеющих право на печатание бланков строгой отчетности согласно законодательству Республики Узбекистан.

Бланк свидетельства о регистрации утверждается органом регистрации.

Для изготовления бланков свидетельств направляется письменная заявка в полиграфическое предприятие с приложением утвержденного образца бланка свидетельства и с указанием следующей информации:

1) полная характеристика дизайна;
2) элементы защищенности бланка;
3) характеристика бумаги (вид, марка и плотность бумаги).

§ 2. Получение, учет, хранение и списание бланков свидетельств о регистрации

29. Органом регистрации назначается лицо, материально ответственное за прием, учет, хранение и выдачу бланков свидетельств о регистрации (далее – ответственное лицо).

На время отсутствия ответственного лица (отпуск, командировка, болезнь и т.д.) указанные бланки должны передаваться по акту лицу, временно исполняющему его обязанности.

Ответственным лицом ведется книга учета бланков свидетельств о регистрации.

Книга учета бланков свидетельств о регистрации заполняется четко, разборчиво и без сокращений. Подчистки в книге не допускаются. Допущенные ошибки исправляются с соответствующими оговорками. Книга должна быть прошнурована, скреплена печатью, ее листы пронумерованы. Общее число листов в книге заверяется подписями ответственного лица и его руководителя.

Доставка бланков свидетельств о регистрации из полиграфического предприятия органу регистрации производится в страховых мешках или посылках, с отметкой на сопроводительных адресах или ярлыках к мешкам «С бланками строгой отчетности».

При поступлении бланков свидетельств о регистрации из полиграфического предприятия на материальный склад органа регистрации пакеты с бланками в обязательном порядке просматриваются ответственным лицом на предмет нарушения упаковки, проверяется соответствие количества полученных упаковок (по наименованию и номерам бланков) количеству, указанному в сопроводительных документах (счетах-фактурах, накладных).

По итогам проверки пакетов с бланками составляется акт приема-передачи (органом регистрации от полиграфического предприятия) и, под расписку в сопроводи-

тельных документах, пакеты с бланками принимаются ответственным лицом органа регистрации на хранение.

В случае отсутствия расхождений с данными сопроводительных документов бланки свидетельств о регистрации приходуются ответственным лицом в соответствующей книге учета бланков свидетельств о регистрации.

Бланки свидетельств о регистрации должны приходоваться ответственным лицом в день поступления.

При получении и оприходовании бланков свидетельств о регистрации составляется акт проверки бланков свидетельств о регистрации в трех экземплярах в случаях:

1) поступления бланков без сопроводительных документов;

2) установления несоответствия наименования и количества поступивших бланков с данными, указанными в сопроводительных документах;

3) обнаружения недостачи или дефектных бланков;

4) выявления отсутствия или повреждения защитной сетки или печатного текста;

5) наличия дублированных номеров либо бланков, имеющих иные номера;

6) наличия бланков со скошенным шрифтом, неправильно обрезанных и неправильного формата;

7) отсутствия серий и номеров на бланках или иного несоответствия их наклейке полиграфического предприятия на пакетах с бланками.

Первый экземпляр акта с дефектными бланками и с сопроводительным письмом направляется в полиграфическое предприятие, второй и третий экземпляры – остаются в деле.

Бланки свидетельств о регистрации должны храниться в сейфах либо шкафах и в специально оборудованных помещениях.

Испорченные при заполнении, изношенные или поврежденные бланки, а также бланки, сданные в связи с перерегистрацией либо аннулированием, не реже одного раза в год списываются и уничтожаются постоянно действующей комиссией, созданной на основании приказа руководителя органа регистрации, по акту, составленному в двух экземплярах. Уничтожение производится путем измельчения на бумагорезательной машине.

Испорченные и/или аннулированные бланки свидетельств обязательно хранятся до уничтожения ответственным лицом с составлением на них реестра в соответствии с приложением 2.

О каждом случае утраты бланков свидетельств о регистрации ответственное лицо немедленно сообщает руководству.

По каждому случаю утраты бланков незамедлительно проводится служебное расследование с целью установления лиц, виновных в утрате бланков, производится немедленная ревизия и снятие остатков имеющихся бланков, а также принимаются все необходимые меры к обеспечению их сохранности.

По итогам служебного расследования составляется акт с указанием обстоятельств утраты, порчи, количества недостающих бланков с перечислением их номеров.

Акт представляется руководству органа регистрации для принятия соответствующего решения.

В необходимых случаях в отношении лиц, виновных в утрате бланков свидетельств о регистрации, материалы передаются в следственные органы.

Не реже одного раза в полгода орган регистрации со специально созданной постоянно действующей комиссией производит инвентаризацию бланков свидетельств о регистрации за истекший период.

На основании инвентаризации составляется соответствующий акт с последующим представлением на утверждение руководителю органа регистрации.

§ 3. Оформление и выдача бланков свидетельств о регистрации

30. Выдача бланков свидетельств о регистрации производится ответственным лицом на основании решения органа регистрации о государственной регистрации центра регистрации.

Заполнение бланков свидетельств о регистрации осуществляется после внесения соответствующих записей в реестр бланков свидетельств о регистрации.

При заполнении бланков запись на бланке свидетельств о регистрации должна быть черного цвета и производиться с применением технических средств.

Помарки и подчистки на бланках, а также сокращение слов не допускаются.

Заполненные бланки свидетельств о регистрации подписываются руководителем органа регистрации и заверяются гербовой печатью.

Выдача свидетельства о регистрации руководителю регистрируемого центра регистрации или его доверенному лицу производится с предъявлением им доверительного письма и документа, подтверждающего его личность.

При выдаче бланков свидетельств о регистрации ответственное лицо вносит соответствующую запись в книгу учета бланков свидетельств о регистрации.

Руководитель или доверенное лицо от организации-заявителя расписывается в получении бланков свидетельств о регистрации в книге учета бланков свидетельств о регистрации, а также в журнале выдачи свидетельств о регистрации в соответствии с приложением 3.

Порядковый номер записи о выдаче бланка свидетельства о регистрации в книге учета бланков свидетельств о регистрации проставляется на соответствующем заявлении на государственную регистрацию центра регистрации. Заявление, вместе с копией решения о государственной регистрации подшивается в специальное дело.

Дефектные, изношенные, а также сданные в связи с перерегистрацией либо аннулированием бланки свидетельств о регистрации сдаются ответственному лицу, о чем составляется соответствующий акт.

ГЛАВА VIII. ТРЕБОВАНИЯ К СЕРТИФИКАТУ

§ 1. Сертификат ключа ЭЦП

31. Сертификат ключа ЭЦП представляет собой документ, подтверждающий соответствие открытого ключа ЭЦП закрытому ключу ЭЦП и выданный центром регистрации владельцу закрытого ключа ЭЦП.

Сертификат ключа ЭЦП может быть изготовлен в форме ЭД и в форме документа на бумажном носителе. Форма журнала выдачи сертификатов ключей ЭЦП уполномоченным лицам центра регистрации приведена в приложении 4.

Сертификат ключа ЭЦП должен содержать:

1) фамилию, инициалы физического лица – владельца закрытого ключа ЭЦП;

2) наименование юридического лица, если владелец закрытого ключа ЭЦП является его представителем;

3) номер и срок его действия;

4) открытый ключ ЭЦП;

5) наименование средств ЭЦП, с помощью которых можно использовать открытый ключ ЭЦП;

6) наименование и местонахождение центра регистрации, выдавшего данный сертификат;

7) сведения о целях использования ЭЦП;

8) электронный адрес реестра сертификатов ключей ЭЦП.

В момент подписания ЭД сертификат ЭЦП должен быть действительным и ЭЦП должна иметь юридическую силу.

По инициативе владельца закрытого ключа ЭЦП в сертификат ключа ЭЦП могут быть включены и иные данные.

ЭД, созданные в период действительности сертификата ключа ЭЦП при наличии других реквизитов, позволяющих идентифицировать документированную информацию, являются подлинниками. Подлинность этих документов сохраняется в дальнейшем независимо от состояния ЭЦП.

32. Расширение идентификатора ключа субъекта в сертификате ключа ЭЦП идентифицирует сертифицируемый открытый ключ. Оно дает возможность различать различные ключи, используемые одним субъектом.

Идентификатор ключа должен быть уникальным по отношению ко всем идентификаторам ключа для субъекта, вместе с которыми он используется.

33. Расширение использования ключа в сертификате ключа ЭЦП указывает цели, для которых используется сертифицированный открытый ключ.

34. Расширение дополнительного использования ключа в сертификате ключа ЭЦП указывает на цели, для которых может быть использован сертификат открытого ключа, в дополнение к основным целям, указанным в поле расширения использования ключа.

Цели использования ключа ЭЦП могут быть определены любой организацией при необходимости.

35. Расширение периода использования закрытого ключа в сертификате ключа ЭЦП указывает на период использования закрытого ключа, соответствующего сертифицированному открытому ключу.

§ 2. Порядок ведения реестра сертификатов ключей ЭЦП и СОС

36. Реестр сертификатов ключей ведется в электронном виде, доступ к реестру для пользователей ЭЦП должен быть свободный.

Сертификаты открытых ключей представлены в реестре в форме электронных копий изготовленных сертификатов.

Центр регистрации обязан обеспечивать своевременное обновление реестра сертификатов ключей ЭЦП. Изменения в реестре должны производиться с момента выдачи, приостановления и возобновления действия сертификата ключа ЭЦП и его аннулирования.

В реестре должны содержаться выданные, действующие, приостановленные и аннулированные сертификаты ключей ЭЦП.

В реестре сертификатов ключей центра регистрации указываются следующие данные о владельце ЭЦП:

1) фамилия, инициалы владельца ЭЦП;

2) основания и даты продления, приостановления и возобновления действия, аннулирования сертификата ключа ЭЦП.

37. Данные о приостановленных и аннулированных сертификатах ключей ЭЦП предоставляются в виде СОС в электронной форме.

СОС создается с использованием единой базы сертификатов центров регистрации и публикуется на веб-сайтах центров регистрации.

§ 3. Порядок приостановления действия и аннулирования сертификата ключа ЭЦП

38. Приостановление действия сертификата ключа ЭЦП осуществляется на основании заявления владельца ЭЦП.

Срок приостановления действия сертификата ключа ЭЦП не должен превышать срок действия данного сертификата ключа ЭЦП.

При приостановлении действия сертификата ключа ЭЦП центр регистрации вносит соответствующую запись в реестр сертификатов ключей ЭЦП и в течение трех дней письменно уведомляет об этом владельца ЭЦП.

Возобновление действия данного сертификата ключа ЭЦП осуществляется на основании заявления владельца ЭЦП в течение срока, на который было приостановлено действие сертификата ключа ЭЦП.

Сертификат ключа ЭЦП аннулируется на основании заявления владельца ЭЦП. Заявление на аннулирование сертификата ключа ЭЦП подается заявителем в электронной или бумажной форме.

Сертификат ключа ЭЦП также аннулируется центром регистрации независимо от согласия владельца ЭЦП в случаях:

1) истечения срока действия данного сертификата;

2) прекращения действия документа, на основании которого был выдан сертификат ключа ЭЦП;

3) выявления фактов невыполнения владельцем ЭЦП обязательств, предусмотренных частью второй статьи 10 Закона Республики Узбекистан «Об электронной цифровой подписи»;

4) истечения срока приостановления действия сертификата ключа ЭЦП и отсутствия заявления владельца ЭЦП на его возобновление.

После аннулирования ключа ЭЦП центром регистрации вносится запись в реестр сертификатов ключей ЭЦП и направляется его владельцу официальное уведомление - список аннулированных сертификатов.

§ 4. Порядок хранения сертификатов ключей ЭЦП и других документов центров регистрации

39. Дальнейшему хранению в ведомственном архиве и/или архиве подлежит следующая документированная информация:

1) реестр сертификатов клиентов центра регистрации;

2) реестр сертификатов уполномоченных лиц центра регистрации;

3) реестр выпускаемых СОС;

4) журналы аудита программно-аппаратных средств обеспечения деятельности центра регистрации;

5) реестр клиентов, зарегистрированных в центре регистрации в качестве пользователей услуг;

6) договора, заключенные между клиентом и центром регистрации;

7) доверенность заявителя на изготовление электронных ключей (ключевой пары) для выпущенного сертификата;

8) заявления на изготовление сертификата;

9) заявления об аннулировании (отзыве) сертификата;

10) заявления о приостановлении действия сертификата;

11) заявления о возобновлении действия сертификата;

12) служебные документы центра регистрации.

40. Срок хранения документов в ведомственном архиве и/или в архиве устанавливается законодательством.

41. Хранение сертификата открытого ключа пользователей центра регистрации в реестре сертификатов открытых ключей центра регистрации осуществляется в течение установленного срока действия сертификата открытого ключа.

Порядок хранения сертификата ключа ЭЦП в форме ЭД в центре регистрации определяются договором между центром регистрации и владельцем ЭЦП.

По истечении срока хранения сертификата ключа ЭЦП в форме ЭД он исключается из реестра сертификатов ключей ЭЦП центра регистрации и переводится в режим архивного хранения.

Аннулированный сертификат ключа ЭЦП в форме ЭД хранится в центре регистрации не менее трех лет.

ГЛАВА IX. ТРЕБОВАНИЯ К ФУНКЦИЯМ ОРГАНА И ЦЕНТРА РЕГИСТРАЦИИ

§ 1. Орган регистрации

42. Орган регистрации:

1) разрабатывает нормы и правила по использованию ЭЦП;

2) осуществляет государственную регистрацию центров регистрации ключей ЭЦП;

3) ведет единый государственный реестр сертификатов ключей ЭЦП уполномоченных лиц центров регистрации;

4) выдает сертификаты ключей ЭЦП уполномоченным лицам центров регистрации.

§ 2. Центр регистрации

43. Центр регистрации:

1) создает закрытые и открытые ключи ЭЦП;

2) обеспечивает защиту закрытого ключа владельца ЭЦП;

3) ведет реестр сертификатов ключей ЭЦП;

4) выдает сертификаты ключей ЭЦП юридическим и физическим лицам;

5) приостанавливает и возобновляет действие сертификатов ключей ЭЦП, а также аннулирует их.

44. Центр регистрации имеет право аннулировать сертификат ключа ЭЦП в случае установленного факта компрометации соответствующего закрытого ключа, с уведомлением владельца аннулированного сертификата ключа ЭЦП и указанием обоснованных причин.

45. Центр регистрации обязан:

1) осуществлять эксплуатацию информационной системы центра регистрации в установленном порядке;

2) уведомлять орган регистрации обо всех изменениях в информационных технологиях, составе и размещении средств и систем информатики, условиях их эксплуатации, которые могут повлиять на эффективность мер и средств защиты информации;

3) представлять в орган регистрации документы для осуществления контроля и мониторинга за эксплуатацией центра регистрации, прошедшего государственную регистрацию.

4) не разглашать или предоставлять персональные данные заявителей, ставшие ему известными в связи с осуществлением возложенных на него задач, за исключением случаев, предусмотренных законодательством;

5) использовать закрытый ключ ЭЦП уполномоченного лица центра регистрации только для подписи выданных им сертификатов открытых ключей и списков аннулированных сертификатов;

6) принимать меры по защите закрытого ключа уполномоченного лица центра регистрации;

7) не разглашать регистрационную информацию владельцев ЭЦП, за исключением информации, используемой для идентификации владельцев сертификатов ключей ЭЦП и заносимой в изготавливаемые сертификаты;

8) изготавливать зарегистрированному владельцу ЭЦП по его заявлению закрытый и открытый ключ с использованием средств ЭЦП, сертифицированных в соответствии с действующим законодательством Республики Узбекистан;

9) записывать ключ на съемный носитель данных в соответствии с требованиями по эксплуатации программного и/или аппаратного средства, выполняющего процедуру генерации ключей;

10) выполнять процедуру генерации ключей и запись ключей на съемный носитель данных только с использованием программного и/или аппаратного средства, сертифицированного в соответствии с законодательством Республики Узбекистан;

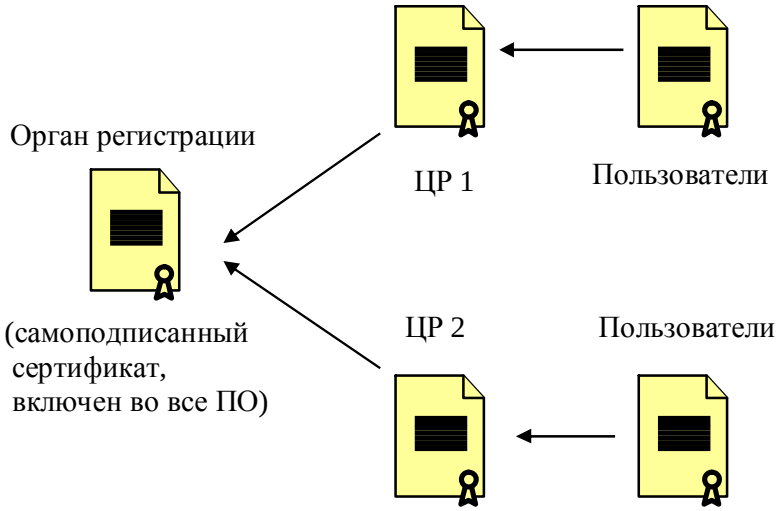
11) обеспечивать уникальность регистрационных (серийных) номеров изготавливаемых сертификатов ключей ЭЦП владельцев ЭЦП;

12) обеспечивать уникальность значений открытых ключей в изготовленных сертификатах открытых ключей пользователей ЭЦП;

13) включать полный Интернет адрес -URL реестра сертификатов ключей ЭЦП в издаваемые сертификаты ключей ЭЦП пользователей центра регистрации.

§ 3. Требования взаимодействия центра регистрации с органом регистрации

46. Пользователи обращаются с запросом на выдачу сертификатов в центры регистрации, а центры регистрации - в орган регистрации, имеющий самоподписанный сертификат, согласно следующей схеме, приведенной на рисунке 1.



ПО – программное обеспечение;
ЦР – центр регистрации.

Рисунок 1 - Схема взаимодействия центров регистрации с органом регистрации

§ 4. Требования к единому государственному реестру сертификатов

47. Единый государственный реестр сертификатов ключей ЭЦП центров регитсрации и пользователей ведется органом регистрации.

После выдачи сертификата ключа ЭЦП центр регистрации в течение одного часа уведомляет орган регистрации и включает данный сертификат в единый государственный реестр сертификатов ключей ЭЦП.

При приостановлении, возобновлении действия сертификата орган регистрации вносит изменения в единый государственный реестр сертификатов ключей ЭЦП.

Взаимодействие центра регистрации с единым реестром сертификатов приведено на рисунке 2.

Рисунок 2 - Взаимодействие центра регистрации с единым реестром сертификатов

Официальным уведомлением о факте приостановления действия сертификата ключа ЭЦП является опубликование СОС, содержащего сведения о приостановленном сертификате по адресу органа регистрации.

Официальным уведомлением о факте возобновления действия сертификата ключа ЭЦП является опубликование органом регистрации СОС, не содержащего сведения о приостановленном сертификате.

Официальным уведомлением о факте аннулирования сертификата ключа ЭЦП является опубликование СОС, содержащего сведения об аннулированном (отозванном) сертификате по адресу органа регистрации.

При аннулировании действия сертификата и при внесении изменений в сертификат орган регистрации вносит изменения в единый государственный реестр сертификатов ключей ЭЦП.

§ 5. Требования к функциям доверенной третьей стороны

48. К функциям доверенной третьей стороны должны относиться:

1) подтверждение подлинности при организации обмена защищенными ЭД;

2) проставление штампа времени на заверенном ЭД;

3) создание квитанций по факту проверки ЭЦП при длительном архивном хранении ЭД;

4) проверка ЭЦП пользователей в качестве третьей доверенной стороны;

5) проверка действительности цифрового сертификата;

6) подтверждение истинности открыто публикуемой государственными органами информации, а также контроль всех модификаций данной информации с целью предотвращения возможности подделки;

7) нотариальное удостоверение договоров;

8) ведение реестра нотариальных актов;

9) обеспечение гарантии соответствия текста документа воле заявителей, аутентичности адреса отправки ЭД;

10) изготовление электронных копий бумажных документов и заверение их своей ЭЦП;

11) выдача электронных подтверждений подлинности документов.

Доверенная третья сторона должна:

1) предоставлять информацию о неправомерных действиях пользователей;

2) нести ответственность за достоверность заверяемой ей информации;

3) иметь собственную подпись или знак, который прикрепляется к документу.

После подписания ЭД доверенной третьей стороной любые изменения в любом из элементов ЭД должны считаться недействительными.

§ 6. Требования к целостности и неотказуемости

49. Орган регистрации и центр регистрации должны обеспечивать целостность информации и неотказуемость.

50. Целостность информации заключается в её существовании в неискаженном виде по отношению к некоторому первоначальному состоянию.

51. Неотказуемость заключается в невозможности отказаться от совершенных действий при использовании сертификата ключа ЭЦП и обеспечивает два вида услуг: неотказуемость с подтверждением подлинности владельца сертификата ключа ЭЦП и неотказуемость с подтверждением доставки информации.

ГЛАВА X. ПОДТВЕРЖДЕНИЕ ПОДЛИННОСТИ ЭЦП

§ 1. Подтверждение подлинности ЭЦП

52. Подтверждение подлинности ЭЦП в ЭД - положительный результат проверки принадлежности ЭЦП в ЭД ее владельцу с помощью сертифицированного средства ЭЦП и сертификата ключа ЭЦП и отсутствия искажений в подписанном данной ЭЦП ЭД.

§ 2. Процедура подтверждения ЭЦП в ЭД с использованием сертификата

53. Подтверждение ЭЦП в ЭД осуществляется центрами регистрации по обращению клиентов, на основании представленного в письменной форме заявления о подтверждении ЭЦП в ЭД.

В представленном заявлении должна быть указана информация о дате и времени формирования ЭЦП в ЭД. Обязательным приложением к заявлению о подтверждении ЭЦП в ЭД является внешний носитель электронной информации, на котором записаны:

1) исходный (неподписанный) файл ЭД, к которому применялась ЭЦП;

2) файл ЭД, подписанный ЭЦП, авторство которого оспаривается;

3) файл сертификата уполномоченного лица центра регистрации, являющегося издателем сертификата, соответствующего закрытому (секретному) ключу, с помощью которого была сформирована ЭЦП в ЭД.

По результатам проверки клиент получает на руки протокол (акт) проверки ЭЦП, в котором содержатся:

1) результат проверки ЭЦП сертифицированным средством;

2) детальный отчет по выполненной проверке (экспертизе).

Детальный отчет по выполненной проверке (экспертизе) содержит следующие обязательные компоненты:

1) время и место проведения проверки (экспертизы);

2) основания для проведения проверки (экспертизы);

3) сведения об эксперте или комиссии экспертов (фамилия, инициалы, занимаемая должность);

4) вопросы, поставленные перед экспертом или комиссией экспертов;

5) объекты исследований и материалы по заявлению, представленные эксперту для проведения проверки (экспертизы);

6) содержание и результаты исследований с указанием примененных методов;

7) оценку результатов исследований, выводы по поставленным вопросам и их обоснование.

Детальный отчет составляется в простой письменной форме и заверяется собственноручной подписью эксперта или членами комиссии экспертов.

В случае отказа в рассмотрении заявления клиента работник центра регистрации вносит в его заявление свою резолюцию, раскрывающую причину отказа в рассмотрении поступившей заявки, снимает копию заявления. В оригинале заявления и в его копии клиент ставит свою подпись, подтверждающую факт ознакомления с содержащейся в нем резолюцией работника центра регистрации.

Подтверждение ЭЦП уполномоченного лица центра регистрации осуществляется центрами регистрации по обращению клиентов, на основании представленного в письменной форме заявления о подтверждении ЭЦП уполномоченного лица центра регистрации в сертификате.

Обязательным приложением к заявлению о подтверждении ЭЦП уполномоченного лица центра регистрации является внешний носитель электронной информации, на котором записаны:

1) файл сертификата зарегистрированного владельца сертификата, подвергающийся процедуре проверки;

2) файл сертификата уполномоченного лица центра регистрации, являющегося издателем сертификата зарегистрированного владельца сертификата, в достоверности которого заявитель сомневается и намерен подвергнуть процедуре проверки;

3) файл СОС, издателем которого является центр регистрации, использовавшийся клиентом-заявителем для проверки ЭЦП уполномоченного лица центра регистрации.

Срок рассмотрения заявления о подтверждении ЭЦП уполномоченного лица центра регистрации в сертификате составляет пять рабочих дней с момента его представления в центр регистрации.

§ 3. Использование штампа времени

54. Для доказательства момента подписания ЭД в информационной системе может предусматриваться использование дополнительного реквизита подписанного ЭД – штампа времени.

Штамп времени на ЭД удостоверяет время создания ЭЦП для последующего разрешения конфликтов, связанных с использованием ЭД.

Сервис предоставления штампа времени на создание ЭЦП обеспечивается используемой информационной системой.

ГЛАВА XI. ПРЕДСТАВЛЕНИЕ ИНФОРМАЦИИ О КОМПРОМЕТАЦИИ СЕКРЕТНОГО (ЗАКРЫТОГО) КЛЮЧА

55. В случае выявления фактов компрометации закрытого (секретного) ключа стороны действующего договора обязаны немедленно предпринять действия, позволяющие избежать (устранить) факты несанкционированного использования закрытого (секретного) ключа.

Центр регистрации рассматривает в качестве факта компрометации закрытого (секретного) ключа клиента следующие события:

1) передача владельцем сертификата своего персонального ключевого носителя, содержащего закрытый (секретный) ключ, в пользование другому физическому лицу;

2) утрата ключевого носителя владельцем сертификата, содержащего его персональный закрытый (секретный) ключ, по причине утери либо кражи ключевого носителя;

3) утрата владельцем сертификата своего персонального закрытого (секретного) ключа в результате механического повреждения ключевого носителя;

4) выявление владельцем персонального закрытого (секретного) ключа фактов и событий несанкционированного его использования посторонними лицами;

5) изменение статуса владельца сертификата (подразумевается, что в результате произошедших изменений ранее предоставленные сведения, на основании которых был выпущен сертификат, утратили свою юридическую силу).

При выявлении факта компрометации закрытого (секретного) ключа его владелец обязан:

1) немедленно проинформировать работника центра регистрации о факте компрометации;

2) представить письменное заявление об аннулировании (отзыве) действующего сертификата с внесением сведений, раскрывающих причины компрометации сертификата;

3) немедленно приостановить обмен ЭД со всеми участниками информационного взаимодействия с применением ЭЦП и функций шифрования.

Клиент, объявивший о компрометации собственных криптографических ключей, обязан в течение одного рабочего дня документально оформить уведомление о произошедшем событии и направить его в центр регистрации.

ГЛАВА XII. ПОРЯДОК ПРОВЕДЕНИЯ ГОСУДАРСТВЕННОГО КОНТРОЛЯ

56. Государственный комитет связи, информатизации и телекоммуникационных технологий Республики Узбекистан является уполномоченным органом государственного контроля и надзора за обеспечением выполнения и соблюдения требований настоящего регламента и осуществляет государственный контроль (надзор) в порядке, установленном законодательством в области электронной цифровой подписи. Государственный контроль (надзор) за соответствием инфраструктуры открытых ключей обязательным требованиям настоящего технического регламента, проводится как на плановой основе, так и на внеплановой основе, при наличии претензий (жалоб) пользователей инфраструктуры открытых ключей.

57. В случае выявления нарушения требований настоящего технического регламента, уполномоченный орган вправе приостановить действие свидетельства о государственной регистрации центра регистрации, в целях недопущения причинения вреда и нанесению ущерба гражданам, и выдавать предписания об устранении нарушений, и устанавливать обоснованный с учетом характера нарушений срок для исполнения предписаний.

58. При проведении контроля должностное лицо уполномоченного органа осуществляет следующие действия:

1) рассматривает представленные центром регистрации документы, связанные с выполнением работ;

2) проверяет:

a) соблюдение требований технического регламента, нормативных документов применительно к выполненным работам;

b) устранение нарушений (недостатков) применительно к выполненным работам, выявленных ранее при проведении контроля со стороны уполномоченного органа;

3) оформляет результаты проведенной проверки выполненных работ;

Акт, оформляемый по результатам проверки, и выданное на его основании предписание составляются в двух экземплярах. К акту о проведенной проверке прилагаются составленные либо полученные в процессе проведения проверки документы. Первые экземпляры акта и предписания, а также копии указанных документов направляются (вручаются) уполномоченному лицу центра регистрации. Вторые экземпляры акта и предписания, а также составленные либо полученные в процессе проведения проверки документы остаются в деле уполномоченного органа.

После устранения выявленных уполномоченным органом нарушений, центр регистрации направляет в уполномоченный орган извещение об устранении выявленных нарушений.

Проверки могут быть сопряжены с проведением уполномоченным органом экспертиз, обследований помещений центра регистрации на предмет обеспечения безопасности.

Требования к проведению экспертиз, обследований определяются в соответствии с регламентом работы органа регистрации центров регистрации ключей электронной цифровой подписи.

Экспертизы, обследования назначаются должностным лицом уполномоченного органа в зависимости от предмета и результата проверки, при этом определяется их объем, состав и характер.

Перед началом проведения экспертизы, обследования, но не позднее, чем за три рабочих дня до даты проведения, центр регистрации уведомляется должностным лицом уполномоченного органа о проведении такой экспертизы, обследования. В уведомлении указываются сведения о дате проведения экспертизы, обследования, их объеме, составе и характере, иные сведения, необходимые для их проведения.

Результаты проведенных экспертиз, обследований оформляются документом – «Заключение по итогам оценки соответствия» (приложение 5), в котором должно содержаться подробное описание проведенного исследования и сделанные в результате его проведения выводы в зависимости от объема, состава и характера проведенной экспертизы, обследования. К указанному документу прилагаются копии документов, составленные в процессе проведения экспертизы, обследования.

Один экземпляр документа, отражающего результаты проведенных экспертиз, обследований остается в деле уполномоченного органа, второй экземпляр передается в центр регистрации.

59. При неустранении центром регистрации в установленные уполномоченным органом сроки нарушений, приведших к приостановлению действия свидетельства о государственной регистрации, уполномоченный орган вправе аннулировать свидетельство о государственной регистрации центра регистрации.

Приложение 1
к Специальному техническому
регламенту «Требования к инфраструктуре
открытых ключей»

Форма журнала

учета и регистрации всех съемных носителей органа (центра) регистрации

Метка съемного носителя (учетный номер)	Фамилия исполнителя	(Получил, вернул, передал)	Дата записи информации	Подпись исполнителя	Примечание

Приложение 2
к Специальному техническому
регламенту «Требования к инфраструктуре
открытых ключей»

Форма журнала
учета бланков свидетельств о государственной регистрации
и сертификатов ключей, подлежащих уничтожению

Дата	Номер бланка	Причина (испорченный, изношенный, перерегистрация, аннулирование)	Основание и документы перерегистрации и аннулирования	Акт сдачи бланка центром регистрации в орган регистрации (номер и дата)	Акт уничтожения бланка (номер и дата)

Приложение 3
к Специальному техническому
регламенту «Требования к инфраструктуре
открытых ключей»

Форма журнала

выдачи свидетельств о государственной регистрации центра регистрации

Наименование организации-заявителя	Наименование центра регистрации	Почтовый адрес, тел/факс, e-mail центра регистрации	Номер свидетельства	Срок действия (с__ по__)	Фамилия, инициалы, должность доверенного лица	Данные документа доверенного лица	Дата получения	Подпись доверенного лица о получении

Приложение 4
к Специальному техническому
регламенту «Требования к инфраструктуре
открытых ключей»

Форма журнала

выдачи сертификатов ключей ЭЦП уполномоченным лицам

центра регистрации

Наименование центра регистрации	Почтовый адрес, тел/факс, e-mail центра регистрации	Номер сертификата	Срок действия (с__ по__)	Фамилия, инициалы, должность уполномоченного лица	Паспортные данные уполномоченного лица	Дата получения	Подпись уполномоченного лица о получении

Приложение 5
к Специальному техническому
регламенту «Требования к инфраструктуре
открытых ключей»

Форма заключения по итогам оценки соответствия центра регистрации требованиям технического регламента

УТВЕРЖДАЮ

_____

(должность руководителя органа регистрации)

_____ _____

подпись фамилия, инициалы

_____

дата

Заключение
по итогам оценки соответствия центра регистрации требованиям технического регламента

_____

(полное и сокращенное наименование юридического лица с указанием его организаци-

_____

онноправовой формы, полное и сокращенное наименование центра регистрации, адрес)

В период с "__" _____ 20__ года по "__" _____ 20__ года орган регистрации на основании _____ провел оценку соответствия

_____

(наименование центра регистрации)

_____

(полное наименование юридического лица с указанием организационно-правовой формы)

требованиям к национальной инфраструктуре открытых ключей, обеспечению конфиденциальности и целостности информации, безопасности помещений, персоналу, сертификатам ключей электронной цифровой подписи, бланкам свидетельств о регистрации, предъ-

являемым к организациям, исполняющим функции центра регистрации в соответствии с положениями специального технического регламента «Требования к инфраструктуре открытых ключей».

На основании оценки соответствия _____ принято следующее решение:

_____

_____

_____

_____

_____

Настоящее заключение действительно до "__" _____ 20__ года.

Уполномоченное лицо
органа регистрации _____ _____
(подпись) (фамилия, инициалы)