

УТВЕРЖДЕН
приказом ПАО «Газпром»
от «24» НОЯБРЯ 2021 г. № 503

РЕГЛАМЕНТ
эксплуатации удостоверяющих центров,
зарегистрированных в Сети удостоверяющих центров
Группы Газпром

1. Общие положения

1.1. Настоящий Регламент устанавливает единые требования к эксплуатации удостоверяющих центров, зарегистрированных в Сети удостоверяющих центров Группы Газпром.

1.2. Эксплуатация удостоверяющих центров, зарегистрированных в Сети удостоверяющих центров Группы Газпром осуществляется в соответствии с требованиями Федерального закона от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи», иных законодательных и нормативных правовых актов Российской Федерации, регулирующих отношения в области эксплуатации удостоверяющих центров, локальных нормативных актов ПАО «Газпром», а также настоящего Регламента.

1.3. Требования настоящего Регламента распространяются на удостоверяющие центры, зарегистрированные в Сети удостоверяющих центров Группы Газпром.

2. Термины, определения и сокращения

В настоящем Регламенте применяются следующие сокращения и термины с соответствующими им определениями:

АРМ – автоматизированное рабочее место;

АПМДЗ – аппаратно-программный модуль доверенной загрузки;

Владелец СКП – физическое лицо, которому удостоверяющим центром выдан сертификат ключа проверки неквалифицированной электронной подписи;

ЕВСПД – Единая ведомственная сеть передачи данных ПАО «Газпром»;

Интернет-ресурс СУЦ – информационный ресурс, обеспечивающий доступ к информации о деятельности Сети удостоверяющих центров Группы Газпром, а также доступ Владелец СКП к сервису поиска сертификатов ключей проверки неквалифицированных электронных подписей, расположенный в сети Интернет по адресу <http://caweb.gazprom.ru>;

Комиссия – Комиссия по проведению экспертизы и контролю деятельности удостоверяющих центров, формируемая распорядительным документом ПАО «Газпром»;

ключевой носитель – носитель информации, предназначенный для хранения на нем ключа электронной подписи, исключающий несанкционированный к нему доступ;

ОКЗ – орган криптографической защиты, создаваемый в организации в соответствии с требованиями законодательства Российской Федерации и локальных нормативных актов ПАО «Газпром»;

Ответственный за организацию работы СУЦ – работник ПАО «Газпром», назначаемый распорядительным документом ПАО «Газпром» ответственным за организацию работы Сети удостоверяющих центров Группы Газпром;

ПО – программное обеспечение;

ПАК – программно-аппаратный комплекс;

ПТС – программно-технические средства;

ПУР УЦ – пункт удаленной регистрации удостоверяющего центра, зарегистрированного в Сети удостоверяющих центров Группы Газпром;

регламент УЦ – документ, утверждаемый в установленном порядке в организации, в которой эксплуатируется удостоверяющий центр, определяющий порядок реализации функций удостоверяющего центра, осуществления его прав и исполнения обязанностей в соответствии с требованиями законодательства Российской Федерации и локальных нормативных актов ПАО «Газпром»;

Репозиторий СУЦ – централизованное информационное хранилище сертификатов ключей проверки неквалифицированных электронных подписей УЦ СУЦ и списков аннулированных сертификатов УЦ СУЦ, расположенное в сети Интернет по адресу <http://ca.gazprom.ru>;

СУЦ – Сеть удостоверяющих центров Группы Газпром;

СКЗИ – средства криптографической защиты информации;

СКП – сертификат ключа проверки неквалифицированной электронной подписи;

службы УЦ – сервисы, осуществляющие по запросам пользователей представление информации о статусе сертификатов ключей проверки неквалифицированных электронных подписей посредством реализации протокола OCSP и предоставление меток времени посредством реализации протокола TSP;

СУБД – система управления базами данных;

УЦ – удостоверяющий центр, зарегистрированный в СУЦ;

ЭП – неквалифицированная электронная подпись;

ЭО – организация, оказывающая услуги по техническому обслуживанию и/или эксплуатации УЦ.

3. Организационная структура удостоверяющих центров

3.1. Для обеспечения функционирования УЦ в организации назначаются ответственные лица:

Ответственный за организацию работы УЦ;

Уполномоченное лицо УЦ;
 Администратор УЦ;
 Администратор безопасности УЦ;
 Оператор УЦ;
 Системный администратор УЦ.

3.2. Рекомендуемый перечень функциональных обязанностей ответственных лиц, указанных в пункте 3.1 настоящего Регламента, приведен в приложении № 1.

3.3. Исполнение функциональных обязанностей Ответственного за организацию работы УЦ, Уполномоченного лица УЦ, Администратора УЦ, Администратора безопасности УЦ возлагается на работников организаций, в которых осуществляется эксплуатация УЦ.

3.4. Не допускается возложение функциональных обязанностей Администратора безопасности УЦ и Системного администратора УЦ на одного и того же работника.

3.5. Исполнение функциональных обязанностей Оператора УЦ и Системного администратора УЦ работниками организации, в которой эксплуатируется УЦ, возможно только при наличии лицензий на осуществление деятельности, предусмотренной пунктами 1 и 5 части 1 статьи 12 Федерального закона от 04 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности». Допускается исполнение функциональных обязанностей Оператора УЦ и Системного администратора УЦ по договору оказания услуг технического обслуживания и/или эксплуатации УЦ ЭО, имеющей указанные лицензии.

3.6. Назначение работников для выполнения обязанностей по функционированию УЦ, а также ввод УЦ в постоянную эксплуатацию производится распорядительными документами организации.

3.7. Численность работников, выполняющих обязанности по функционированию/эксплуатации УЦ, может быть увеличена пропорционально количеству и сложности решаемых УЦ задач.

4. Мероприятия по обеспечению деятельности удостоверяющих центров

4.1. Организационно-технические мероприятия при обеспечении функционирования УЦ:

представление в Комиссию актуальной информации о назначениях работников, обеспечивающих функционирование УЦ, и создании дополнительных ПУР УЦ;

ведение актуальной карточки УЦ в соответствии с приложением № 2 и информирование Комиссии обо всех ее изменениях;

согласование изменений, вносимых в Регламент УЦ;

информирование Комиссии о выявленных нарушениях и сбоях в работе УЦ, фактах некорректной работы СКЗИ и другого ПО, используемого для создания ЭП (средства электронной подписи) и шифрования информации;

организация работ по плановой смене СКП Уполномоченного лица УЦ;

обеспечение сохранности программно-аппаратных средств УЦ, носителей резервных копий данных УЦ, ключевого носителя Уполномоченного лица УЦ;

представление необходимых документов в Комиссию для проведения экспертизы при регистрации и перерегистрации УЦ;

соблюдение порядка и правил использования программно-аппаратного комплекса УЦ, определенных эксплуатационной и технической документацией;

обеспечение применения при функционировании УЦ средств УЦ, соответствующих требованиям ФСБ России к средствам удостоверяющих центров класса не ниже КС2;

обеспечение применения в составе УЦ сертифицированных по требованиям безопасности средств межсетевого экранирования, обеспечивающих сетевую защиту программно-аппаратного комплекса УЦ;

обеспечение создания списка аннулированных СКП УЦ и контроль за его публикацией в Репозитории СУЦ;

обеспечение доступности СКП УЦ и списка аннулированных СКП УЦ;

обеспечение ежедневного формирования дампа (файла) СКП, созданных УЦ, по установленной форме и контроль за его корректной загрузкой на Интернет-ресурсе СУЦ;

обеспечение рассылки по электронной почте Владельцам СКП уведомлений о приближении срока окончания действия их СКП (еженедельно, начиная за месяц до окончания срока), а также рассылка сообщений об истечении срока действия их СКП (по окончании срока действия СКП);

обеспечение и контроль синхронизации ПТС УЦ с серверами точного времени вычислительной сети организации;

обеспечение антивирусной защиты УЦ в соответствии с порядком, установленным в организации, и рекомендациями организаций – разработчиков антивирусного ПО, а также ведение контроля за функционированием антивирусного ПО УЦ и наличием актуальных версий антивирусных баз;

обеспечение регулярного резервного копирования системного и прикладного ПО УЦ в соответствии с порядком, установленным в организации;

проведение контроля целостности ПТС УЦ в соответствии с порядком, установленным в Регламенте УЦ;

своевременное проведение работ по установке обновлений и исправлений системного и прикладного ПО.

4.2. Интеграция УЦ с вычислительной сетью организации, а также настройка средств межсетевого экранирования УЦ проводятся в соответствии с приложениями № 3, 4.

4.3. Перечень технических требований к основным настройкам ПТС УЦ, построенных на базе ПАК «КриптоПро УЦ», представлен в приложении № 5.

4.4. Экспертиза и контроль деятельности УЦ, в том числе ПУР УЦ, осуществляется Комиссией в соответствии с Порядком проведения экспертизы и контроля деятельности удостоверяющих центров, утвержденным ПАО «Газпром».

5. Обеспечение сертификатами ключей проверки неквалифицированных электронных подписей

5.1. УЦ создают СКП для работников организаций, в которых эксплуатируются данные УЦ.

5.2. Удостоверяющий центр ООО «Газпром информ» и УЦ, предоставляющие услуги по созданию СКП для применения в Группе Газпром, создают СКП для работников организаций, в которых нет УЦ, на возмездной основе.

6. Работа с СКЗИ и ключевыми документами

6.1. Порядок работы с СКЗИ и ключевыми документами определяется локальными нормативными актами ПАО «Газпром» либо внутренними документами организации.

6.2. При создании ключа ЭП Уполномоченного лица УЦ должна создаваться его копия на отдельном отчуждаемом ключевом носителе. Ключ ЭП Уполномоченного лица УЦ и копия ключа ЭП Уполномоченного лица УЦ подлежат хранению в порядке, исключающем их компрометацию.

7. Приостановление, возобновление и прекращение деятельности удостоверяющего центра

7.1. Приостановление деятельности УЦ осуществляется по причинам: компрометации ключа ЭП УЦ; получения отрицательных результатов экспертизы или контроля деятельности УЦ;

наличия иных существенных нарушений в деятельности УЦ.

7.2. Возобновление деятельности УЦ осуществляется после устранения причин приостановления деятельности УЦ.

7.3. Прекращение деятельности УЦ осуществляется после мотивированного обращения организации, в которой эксплуатируется УЦ, о нецелесообразности дальнейшего функционирования УЦ.

7.4. Мероприятия по приостановлению, возобновлению и прекращению деятельности УЦ проводятся по решению Ответственного за организацию работы СУЦ на основании заключения Комиссии о возможности проведения указанных мероприятий.

7.5. Информация о приостановлении, возобновлении или прекращении деятельности УЦ публикуется на Интернет-ресурсе СУЦ.

7.6. УЦ, в отношении которого принято решение о прекращении деятельности, приостанавливает создание СКП, производит выгрузку электронного реестра выданных СКП и списков аннулированных сертификатов, представляет электронную копию реестра сертификатов и списков, а также заявление на аннулирование всех действующих СКП УЦ в Корпоративный удостоверяющий центр ПАО «Газпром» с принятием необходимых мер по обеспечению целостности находящихся в реестре сведений.

7.7. После публикации на Интернет-ресурсе СУЦ информации о прекращении деятельности УЦ производится аннулирование всех действующих СКП УЦ и внеплановое обновление списка аннулированных сертификатов Корпоративного удостоверяющего центра ПАО «Газпром». С момента аннулирования СКП УЦ все СКП, созданные данным УЦ, прекращают свое действие.

7.8. Организация, в отношении УЦ которой принято решение о прекращении деятельности, обеспечивает хранение и уничтожение документов УЦ в порядке, установленном в такой организации.

Приложение № 1
к Регламенту эксплуатации
удостоверяющих центров,
зарегистрированных в Сети
удостоверяющих центров
Группы Газпром

**Рекомендуемый перечень функциональных обязанностей
ответственных лиц удостоверяющего центра, зарегистрированного
в Сети удостоверяющих центров Группы Газпром**

**1. Функциональные обязанности Ответственного за организацию работы
удостоверяющего центра**

- 1.1. Общая координация деятельности УЦ.
- 1.2. Взаимодействие с руководителями организации, в которой эксплуатируется УЦ, и ЭО по вопросам технического обслуживания и/или эксплуатации УЦ.
- 1.3. Организация работ по разработке и совершенствованию внутренних документов организации в области функционирования УЦ и использования средств ЭП.
- 1.4. Организация работ по заключению между организацией и ЭО договоров на оказание услуг по техническом обслуживанию и/или эксплуатации УЦ.
- 1.5. Организация работ по своевременному включению в бюджет организации необходимых для обеспечения функционирования/эксплуатации УЦ финансовых средств (на техническое обслуживание УЦ, закупку необходимого оборудования, ПО и СКЗИ, сопровождение ПО УЦ и т.д.).

**2. Функциональные обязанности Уполномоченного лица удостоверяющего
центра**

- 2.1. Обеспечение безопасного хранения и использования ключевого носителя с ключом ЭП Уполномоченного лица УЦ (в том числе ключевого носителя с копией ключа ЭП Уполномоченного лица УЦ).
- 2.2. Участие в разработке и совершенствовании внутренних документов организации, связанных с функционированием УЦ и использованием средств ЭП.
- 2.3. Разработка планов по обеспечению работников структурных подразделений организации СКП в соответствии с потребностями подразделений.
- 2.4. Организация работы по проведению разбора конфликтных ситуаций.
- 2.5. Организация работы по взаимодействию с Комиссией по вопросам проведения экспертизы УЦ, разбора конфликтных ситуаций, а также по вопросам проведения контроля деятельности УЦ.

2.6. Визирование поступающих в УЦ заявлений, а также выдаваемых СКП на бумажном носителе.

3. Функциональные обязанности Администратора удостоверяющего центра

3.1. Участие в организации и проведении организационно-технических мероприятий по применению в информационных системах ЭП.

3.2. Разработка внутренних документов по функционированию УЦ.

3.3. Обработка поступающих в УЦ заявлений на создание, аннулирование, приостановление, возобновление действия СКП.

3.4. Организация работ в соответствии с поступающими в УЦ заявлениями с учетом технических возможностей УЦ.

3.5. Оказание методической помощи Владельцам СКП по вопросам использования СКЗИ, оформления необходимых документов и получения СКП.

3.6. Организация и контроль за проведением занятий по использованию СКЗИ с работниками организации, являющимися Владельцами СКП.

3.7. Участие в подготовке договоров, связанных с функционированием и эксплуатацией УЦ.

3.8. Участие в подготовке предложений по включению в бюджет организации необходимых для обеспечения функционирования и эксплуатации УЦ финансовых средств (на техническое обслуживание УЦ, закупку необходимого оборудования, ПО и СКЗИ, сопровождение ПО УЦ и т.д.).

4. Функциональные обязанности Администратора безопасности удостоверяющего центра

4.1. Контроль за эксплуатацией ПТС УЦ в соответствии с требованиями по безопасности.

4.2. Контроль за своевременностью и полнотой проведения мероприятий по защите информационных ресурсов УЦ (мониторинг журналов межсетевого экранирования, антивирусной защиты, процедур проведения обновлений ПО, резервного копирования и др.).

4.3. Контроль за соблюдением Владельцами СКП требований и положений Регламента УЦ, локальных нормативных актов ПАО «Газпром» и внутренних документов организации по вопросам применения СКЗИ.

4.4. Контроль за выполнением требований, установленных Регламентом эксплуатации удостоверяющих центров, зарегистрированных в Сети удостоверяющих центров Группы Газпром, и эксплуатационной документацией на применяемые средства удостоверяющего центра и СКЗИ.

4.5. Участие в разборе конфликтных ситуаций по вопросам применения ЭП.

5. Функциональные обязанности Оператора удостоверяющего центра

- 5.1. Информационное обеспечение Владельцев СКП.
- 5.2. Создание ключей ЭП и ключей проверки ЭП.
- 5.3. Ведение реестра Владельцев СКП.
- 5.4. Ведение реестра СКП.
- 5.5. Создание, выдача, аннулирование, приостановление и возобновление действия СКП.
- 5.6. Проведение процедуры подтверждения подлинности ЭП в документах, представленных в электронной форме, по обращениям Владельцев СКП.
- 5.7. Проведение процедуры подтверждения подлинности ЭП Уполномоченного лица УЦ в созданных СКП.
- 5.8. Участие в разборе конфликтных ситуаций по вопросам применения ЭП.
- 5.9. Оказание методической помощи по вопросам создания СКП, оформления необходимых документов и использования средств ЭП.
- 5.10. Обеспечение документирования информации УЦ в соответствии с установленными требованиями.
- 5.11. Применение ПТС УЦ в соответствии с эксплуатационной и технической документацией.
- 5.12. Осуществление контроля за сохранностью ПТС УЦ.

6. Функциональные обязанности Системного администратора удостоверяющего центра

- 6.1. Обеспечение надежной, бесперебойной эксплуатации ПТС УЦ в соответствии с требованиями технической и эксплуатационной документации.
- 6.2. Выполнение мероприятий по защите информационных ресурсов УЦ (антивирусная защита, обновления ПО, резервное копирование, межсетевое экранирование и др.).
- 6.3. Настройка и конфигурирование ПТС УЦ.
- 6.4. Создание и настройка учетных записей ПТС УЦ.
- 6.5. Выполнение периодического тестового восстановления УЦ.
- 6.6. Настройка конфигурации параметров аудита.
- 6.7. Проведение анализа причин сбоев в работе ПТС УЦ и подготовка предложений по повышению надежности и стабильности их функционирования.
- 6.8. Подготовка проектов внутренних документов по функционированию УЦ.
- 6.9. Проведение настройки АРМ Владельцев СКП для возможности работы с СКЗИ и ПО, обеспечивающими выполнение функций по созданию неквалифицированной электронной подписи и шифрованию.
- 6.10. Проведение работ по внедрению новых информационных технологий в работу УЦ.

Приложение № 2
к Регламенту эксплуатации
удостоверяющих центров,
зарегистрированных в Сети
удостоверяющих центров
Группы Газпром

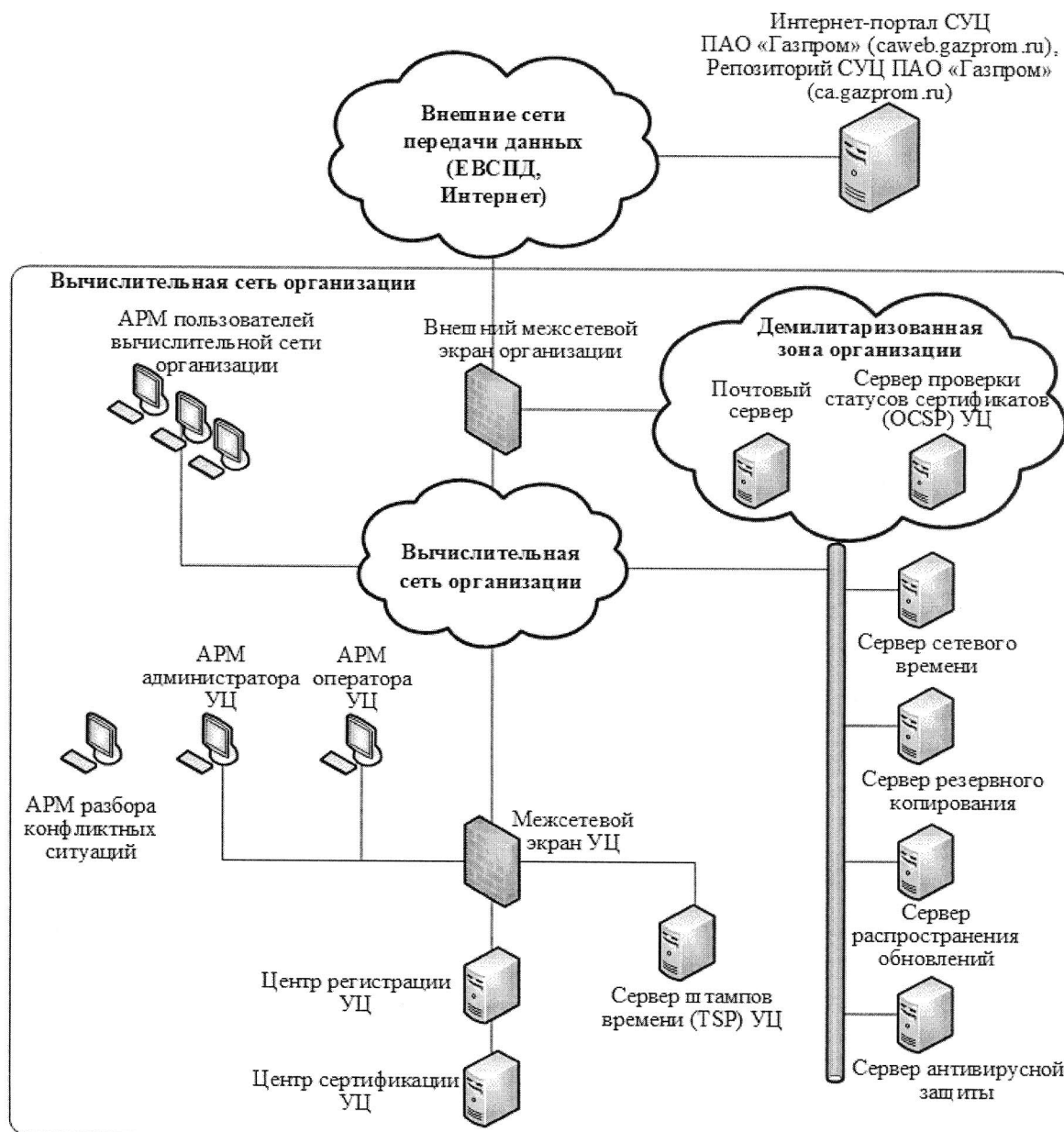
**Карточка удостоверяющего центра, содержащая сведения
о документах, регламентирующих его деятельность**

НАИМЕНОВАНИЕ УЦ	РЕКВИЗИТЫ (наименование документа, номер, дата утверждения)
Паспорт доверенного УЦ	
Лицензии на осуществление деятельности, предусмотренной пунктами 1 и 5 части 1 статьи 12 Федерального закона от 04 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности»	
Аттестат соответствия требованиям по безопасности информации автоматизированной системы УЦ	
Технический паспорт УЦ	
Адреса ПУР УЦ (при наличии)	
Регламент УЦ	
Распорядительный документ организации о вводе в постоянную эксплуатацию УЦ	
Распорядительный документ организации о назначении ответственных лиц УЦ	
Договор на оказание услуг по техническому обслуживанию УЦ между организацией, в которой эксплуатируется УЦ, и организацией, оказывающей указанные услуги (при наличии)	

НАИМЕНОВАНИЕ УЦ	РЕКВИЗИТЫ (наименование документа, номер, дата утверждения)
Должностные инструкции и/или внутренний документ организации, определяющий функциональные обязанности ответственных лиц УЦ	
Внутренний документ организации, регламентирующий порядок антивирусной защиты УЦ	
Внутренний документ организации, регламентирующий порядок обновления программных средств УЦ	
Внутренний документ организации, регламентирующий порядок резервного копирования УЦ	
Внутренний документ организации, регламентирующий порядок доступа в помещения УЦ	
Внутренний документ организации, определяющий организацию работы с СКЗИ (при наличии)	
Распорядительный документ организации о создании ОКЗ (при наличии)	
Внутренний документ организации, содержащий сведения о классификации информационной системы персональных данных УЦ	
Внутренний документ организации, содержащий сведения о настройках межсетевого экрана УЦ	
Контактные данные ответственных лиц УЦ (Ф.И.О., должность, телефон, e-mail)	

Приложение № 3
к Регламенту эксплуатации
удостоверяющих центров,
зарегистрированных в Сети
удостоверяющих центров
Группы Газпром

Типовая схема включения УЦ в состав вычислительной сети организации



Приложение № 4
к Регламенту эксплуатации
удостоверяющих центров,
зарегистрированных в Сети
удостоверяющих центров
Группы Газпром

Типовые информационные потоки для функционирования удостоверяющих центров¹

№ п/п	Источник	Получатель	Сетевые протоколы	Примечание
1	Центр регистрации УЦ	Сервер антивирусной защиты организации	Сетевые протоколы, необходимые для получения обновлений антивирусного ПО	Обновление баз антивирусного ПО (Центр сертификации УЦ получает обновления баз антивирусного ПО через общий сетевой ресурс на Центре регистрации УЦ).
2	Центр регистрации УЦ	Сервер распространения обновлений	tcp/80 (http), tcp/443 (https)	Получение обновлений системного и прикладного ПО (обновление Центра сертификации УЦ осуществляется вручную)
3	Центр регистрации УЦ	Сервер сетевого времени организации	udp/123 (ntp)	Синхронизация времени (синхронизация времени на Центре сертификации УЦ осуществляется через Центр регистрации УЦ)

¹Могут быть скорректированы с учетом особенностей функционирования УЦ.

№ п/п	Источник	Получатель	Сетевые протоколы	Примечание
4	Сервер проверки статусов сертификатов (OCSP) УЦ	Сервер антивирусной защиты организации	Сетевые протоколы, необходимые для получения обновлений антивирусного ПО	Обновление баз антивирусного ПО
5	Сервер проверки статусов сертификатов (OCSP) УЦ	Сервер распространения обновлений	tcp/80 (http), tcp/443 (https)	Получение обновлений системного и прикладного ПО
6	Сервер проверки статусов сертификатов (OCSP) УЦ	Сервер сетевого времени организации	udp/123 (ntp)	Синхронизация времени
7	Сервер штампов времени (TSP) УЦ	Сервер антивирусной защиты организации	Сетевые протоколы, необходимые для получения обновлений антивирусного ПО	Обновление баз антивирусного ПО
8	Сервер штампов времени (TSP) УЦ	Сервер распространения обновлений	tcp/80 (http), tcp/443 (https)	Получение обновлений системного и прикладного ПО
9	Сервер штампов времени (TSP) УЦ	Сервер сетевого времени организации	udp/123 (ntp)	Синхронизация времени

№ п/п	Источник	Получатель	Сетевые протоколы	Примечание
10	Центр регистрации УЦ	Почтовый сервер организации	tcp/25 (smtp)	Отправка служебных сообщений Владельцам СКП УЦ организации
11	АРМ оператора УЦ, АРМ администратора УЦ	Центр регистрации УЦ	tcp/443 (https)	Синхронизация баз данных по протоколу TLS при работе УЦ
12	АРМ оператора УЦ, АРМ системного администратора УЦ	Центр регистрации УЦ	tcp/80 (http)	Доступ к точке распространения списка аннулированных сертификатов ключей проверки неквалифицированных электронных подписей и корневых сертификатов
13	АРМ системного администратора УЦ	Центр регистрации УЦ	tcp/3389 (rdp)	Администрирование Центра регистрации УЦ (администрирование Центра сертификации УЦ осуществляется через Центр регистрации УЦ)
14	АРМ оператора УЦ, АРМ системного администратора УЦ	Сервер антивирусной защиты	Сетевые протоколы, необходимые для получения обновлений антивирусного ПО	Обновление антивирусного ПО
15	АРМ оператора УЦ, АРМ системного администратора УЦ	Сервер распространения обновлений	tcp/80 (http), tcp/443 (https)	Получение обновлений системного и прикладного ПО

№ п/п	Источник	Получатель	Сетевые протоколы	Примечание
16	АРМ оператора УЦ, АРМ системного администратора УЦ	Сервер сетевого времени организации	udp/123 (sntp)	Синхронизация времени
17	Сервер проверки статусов сертификатов (OCSP) УЦ	Центр регистрации УЦ	Сетевые протоколы, необходимые для работы службы OCSP	Работа службы OCSP
18	Сервер штампов времени (TSP) УЦ	Сервер сетевого времени организации	udp/123 (sntp)	Синхронизация времени
19	Центр регистрации УЦ	Сервер резервного копирования организации	Сетевые протоколы, необходимые для работы ПО резервного копирования	Резервное копирование Центра регистрации УЦ (резервное копирование Центра сертификации УЦ осуществляется через общий сетевой ресурс на Центре регистрации УЦ)
20	Вычислительная сеть организации	Центр регистрации УЦ	tcp/80 (http)	Доступ к точке распространения списка аннулированных сертификатов ключей проверки неквалифицированных электронных подписей и корневых сертификатов
21	Вычислительная сеть организации	Сервер проверки статусов сертификатов (OCSP) УЦ	tcp/80 (http)	Проверка сертификатов по OCSP

№ п/п	Источник	Получатель	Сетевые протоколы	Примечание
22	Вычислительная сеть организации	Сервер штампов времени (TSP) УЦ	tcp/80 (http)	Работа со штампами времени
23	Вычислительная сеть организации	Репозиторий СУЦ (ca.gazprom.ru)	tcp/80 (http)	Доступ к точке распространения списка аннулированных сертификатов ключей проверки неквалифицированных электронных подписей и корневых сертификатов
24	Вычислительная сеть организации	Интернет-ресурс СУЦ (caweb.gazprom.ru)	tcp/80 (http), tcp/443 (https)	Доступ к информации на Интернет-ресурсе СУЦ, доступ к сервису поиска СКП
25	Внешние сети передачи данных (ЕВСПД, Интернет)	Сервер проверки статусов сертификатов (OCSP) УЦ	tcp/80 (http)	Проверка сертификатов по OCSP
26	Репозиторий СУЦ (ca.gazprom.ru)	Сервер проверки статусов сертификатов (OCSP) УЦ	tcp/80 (http)	Получение актуальных дампов созданных сертификатов и списка аннулированных сертификатов ключей проверки неквалифицированных электронных подписей

Приложение № 5
к Регламенту эксплуатации
удостоверяющих центров,
зарегистрированных в Сети
удостоверяющих центров
Группы Газпром

**Технические требования
к основным настройкам удостоверяющего центра**

1. Общие положения

1.1. В состав УЦ могут входить следующие компоненты:

Центр сертификации УЦ;

Центр регистрации УЦ;

Служба штампов времени (TSP) УЦ;

Служба проверки статусов сертификатов (OCSP) УЦ;

АРМ оператора УЦ (в том числе в составе ПУР УЦ);

АРМ администратора УЦ (в том числе в составе ПУР УЦ);

АРМ разбора конфликтных ситуаций.

1.2. Компоненты УЦ должны быть защищены с помощью средств межсетевого экранирования.

1.3. Допускается не подключать АРМ разбора конфликтных ситуаций к вычислительной сети организации.

1.4. На всех компонентах УЦ должны быть установлены сертифицированные аппаратно-программные модули доверенной загрузки.

2. Требования к ключу ЭП

2.1. Для хранения ключа ЭП должен использоваться учтенный отчуждаемый сертифицированный ФСТЭК ключевой носитель, исключающий несанкционированное считывание ключевой информации.

2.2. Запрещается использовать жесткий диск (реестр операционной системы) серверов и АРМ УЦ в качестве носителя ключей ЭП.

2.3. При создании ключа ЭП Уполномоченного лица УЦ должна создаваться его копия на отдельном отчуждаемом ключевом носителе. Ключ ЭП Уполномоченного лица УЦ и копия ключа ЭП Уполномоченного лица УЦ подлежат хранению в порядке, исключающем их компрометацию.

2.4. Запрещается использовать ключ ЭП Уполномоченного лица УЦ для целей, отличных от подписи СКП и списка аннулированных сертификатов ключей проверки ЭП.

2.5. Для загрузки ключа ЭП Уполномоченного лица УЦ на Центре сертификации УЦ должна применяться выделенная учетная запись Уполномоченного лица УЦ.

3. Требования к аппаратно-программному модулю доверенной загрузки

3.1. В настройках АПМДЗ в качестве объектов контроля должны быть включены системные файлы, программные средства УЦ и СКЗИ. Допускается осуществление фильтрации файлов по расширениям (например, *.exe, *.com, *.dll, *.sys, *.vxd, *.drv).

3.2. АПМДЗ должен быть сконфигурирован таким образом, чтобы заблокировать процедуру загрузки операционной системы со съемных носителей.

3.3. Длина пароля АПМДЗ должна быть не менее 8 (восьми) символов. В пароле должны присутствовать символы верхнего и нижнего регистра из категорий: английского алфавита (a–z), цифр (0–9), символов, не принадлежащих к алфавитно-цифровому набору (использование русского алфавита не рекомендуется).

3.4. В АПМДЗ должна быть настроена регистрация следующих событий:
изменение настроек;
пересчет контрольных сумм;
создание/удаление пользователей;
удачные и неудачные попытки входа пользователя в систему.

4. Требования к программному обеспечению ПАК УЦ

4.1. Для системных дисков серверов и АРМ, на которых установлены компоненты УЦ, должна быть определена файловая система NTFS.

4.2. Серверы и АРМ, на которых установлены компоненты УЦ, не должны иметь общих сетевых каталогов, которые не используются при функционировании УЦ.

4.3. На серверах и АРМ, на которых установлены компоненты УЦ, должны быть запущены только те службы, функционирование которых необходимо для работы УЦ, установлено только то ПО, которое необходимо для функционирования УЦ и проведения регламентных работ (перечень служб и ПО определяется УЦ и указывается в Техническом паспорте УЦ).

4.4. На серверах и АРМ, на которых установлены компоненты УЦ, должно быть обеспечено использование только тех сетевых протоколов, которые необходимы для функционирования УЦ.

4.5. На серверах, на которых размещены компоненты УЦ, не допускается установки ролей контроллера домена.

4.6. В операционной системе группа «Администраторы» должна содержать только те учетные записи, которые необходимы для функционирования УЦ. Учетная запись Администратор должна быть переименована. Учетная запись Guest должна быть отключена. Свойство Auto Logon должно быть запрещено.

4.7. Конфигурация сервера Центра регистрации УЦ должна обеспечивать функционирование двух сетевых интерфейсов: один (внутренний интерфейс) для взаимодействия с сервером Центра сертификации УЦ, другой (внешний интерфейс) для обеспечения сетевого взаимодействия других компонентов УЦ и пользователей с Центром регистрации УЦ.

4.8. Центр регистрации УЦ и Центр сертификации УЦ должны использовать экземпляры локальных баз данных.

4.9. Парольная политика должна предусматривать блокировку учетных записей на период не менее 10 минут (или до перезагрузки) после 3 неудачных попыток ввода пароля.

4.10. На файловые каталоги веб-узла сервера Центра регистрации УЦ должны быть установлены следующие разрешения:

для администраторов: полный доступ;

для схемы СОЗДАТЕЛЬ-ВЛАДЕЛЕЦ: полный доступ;

для группы «SYSTEM»: полный доступ;

для группы «ВСЕ»: чтение и выполнение, список содержимого папки, чтение.

4.11. Для виртуального каталога, предназначенного для публикации списков аннулированных сертификатов, должен быть запрещен запуск сценариев и исполняемых файлов.

5. Требования к обновлению программного обеспечения

В отношении программного обеспечения серверов и АРМ, на которых размещены компоненты УЦ, должны проводиться своевременные работы по установке рекомендованных разработчиками обновлений и исправлений программного обеспечения.

6. Требования к антивирусной защите

6.1. На всех серверах и АРМ, на которых размещены компоненты УЦ, должно быть установлено антивирусное ПО актуальной версии. Антивирусное ПО должно иметь действующую поддержку от производителя. Отключение антивирусного ПО не допускается. Должны применяться меры по недопущению возможности модификации режима работы антивирусного ПО.

6.2. Настройка антивирусного ПО должна производиться в соответствии с рекомендациями компании производителя антивирусного ПО и порядком, определенном внутренними документами организации.

6.3. Должна обеспечиваться регулярная (не реже одного раза в день) установка обновлений антивирусных сигнатур. Рекомендуемый способ установки антивирусных сигнатур – автоматический.

6.4. Устанавливаемое или изменяемое на ПТС УЦ прикладное ПО предварительно проверяется на отсутствие вирусов. После установки или изменения прикладного ПО выполняется полная антивирусная проверка.

6.5. Все внешние носители информации перед подключением к компонентам УЦ должны быть принудительно проверены на отсутствие вредоносного ПО.

6.6. Параметры настройки и процедуры обновления антивирусных сигнатур должны контролироваться Администратором безопасности УЦ.

7. Требования к резервному копированию

7.1. Файлы и данные, необходимые для полного восстановления работоспособности УЦ, подлежат ежедневному резервному копированию.

7.2. Минимальный перечень данных УЦ, подлежащих резервному копированию, должен включать в себя:

- сертификат ключа проверки ЭП Уполномоченного лица УЦ;
- базу данных Центра сертификации УЦ;
- базы данных Центра регистрации УЦ;
- журналы аудита компонентов УЦ;
- все издаваемые списки аннулированных сертификатов.

7.3. Должно быть осуществлено территориально распределенное хранение резервных копий в количестве, определенном регламентом резервного копирования УЦ (не менее двух копий).

8. Требования к подсистеме регистрации и учета

8.1. Настройка аудита Центра сертификации УЦ.

В журнале событий модуля политики службы сертификации должны регистрироваться следующие события:

- поступление запроса на сертификат;
- создание сертификата;
- аннулирование сертификата;
- опубликование списка аннулированных сертификатов.

8.2. Настройка аудита Центра регистрации УЦ.

В журнале событий ПО Центра регистрации УЦ должны регистрироваться события, имеющие отношения к работе ПАК УЦ.

8.3. Для журналов аудита операционных систем ПТС УЦ должны быть выполнены настройки, обеспечивающие сохранение информации при их переполнении.

8.4. Настройка аудита веб-узла сервера Центра регистрации УЦ должна обеспечивать ежедневное ведение журналов событий в соответствии с эксплуатационной документацией.

В журналах должны отражаться следующие элементы:

- Client IP Address (сетевой адрес клиента);
- User Name (имя пользователя, получившего доступ к серверу);
- Method (метод/действие, которое пытался выполнить клиент, например, POST);
- URI Stem (ресурс URI, т.е. ресурс, к которому было выполнено обращение);
- URI Query (запрос URI, т.е. запрос, который пытался выполнить клиент);
- Protocol Status (состояние протокола в терминах HTTP);
- Win32 Status (состояние Win32 в терминах Windows 2000);
- Bytes Sent (отправлено байт сервером);
- Bytes Received (получено байт сервером);
- Time Token (время, которое заняло действие);
- User Agent (агент пользователя, т.е. обозреватель пользователя).

8.5. Для журналов MS IIS должны быть установлены следующие списки контроля доступа:

- Administrators (полный контроль);
- System (полный контроль);
- Everyone (читать/писать/копировать).

8.6. Настройка аудита СУБД должна обеспечивать аудит всех попыток входа в СУБД.

9. Требования к публикации СКП и списка аннулированных сертификатов ключей проверки неквалифицированных электронных подписей

9.1. УЦ обеспечивает публикацию актуальных СКП Уполномоченного лица УЦ и списков аннулированных сертификатов УЦ по адресам точек, указанным в создаваемых сертификатах. Одна из точек публикации должна размещаться в Репозитории СУЦ (sa.gazprom.ru).

9.2. При формировании списков аннулированных сертификатов ключей проверки неквалифицированных электронных подписей должны использоваться следующие параметры:

- интервал выпуска – 24 часа;
- интервал перекрытия – 2 часа;
- точность часов – 10 мин.

Допускается сокращение интервала выпуска при внеплановом формировании списков аннулированных сертификатов ключей проверки неквалифицированных электронных подписей.

9.3. При проведении в УЦ регламентных работ, приводящих к его временной недоступности, на период проведения работ необходимо производить создание списка аннулированных сертификатов ключей проверки неквалифицированных электронных подписей со сроком действия, превышающим срок или равным сроку проведения регламентных работ.

9.4. УЦ должен обеспечивать формирование дампа (файла) СКП, созданных УЦ, и его доступность для скачивания со стороны Интернет-ресурса СУЦ (caweb.gazprom.ru).

9.5. В дампы СКП должны попадать только актуальные СКП, предназначенные для применения в Сети удостоверяющих центров Группы Газпром. Интервал создания дампа СКП должен составлять не более 24 часов.

9.6. При формировании дампа СКП рекомендуется включать только следующие сведения:

- ID запроса (Request.RequestID);
- Выданный ID запроса (RequestID);
- Дата начала (NotBefore);
- Дата окончания (NotAfter);
- Статус сертификата (Request.DispositionName);
- Серийный номер (SerialNumber);
- Идентификатор имени издателя (IssuerNameID);
- Выданное имя субъекта (DistinguishedName);
- Двоичный сертификат (RawCertificate).