Приложение № 1
к приказу Федерального казенного
учреждения «Объединенная дирекция по
реализации федеральных инвестиционных
программ» Министерства строительства и
жилищно-коммунального хозяйства
Российской Федерации
от «04» июня 2019 г. № 56

РЕГЛАМЕНТ ДОСТУПА
к ресурсам информационной системы выданных и оплаченных государственных жилищных сертификатов в рамках государственной программы Российской Федерации «Обеспечение доступным и комфортным жильем и коммунальными услугами граждан Российской Федерации» с использованием каналов связи сетей общего пользования

I. Общие положения

1.1. Настоящий регламент определяет порядок организации доступа пользователей к ресурсам информационной системы учета выданных и оплаченных государственных жилищных сертификатов в рамках государственной программы Российской Федерации «Обеспечение доступным и комфортным жильем и коммунальными услугами граждан Российской Федерации» (далее – ИС ГЖС) с использованием каналов связи информационно-телекоммуникационных сетей общего пользования (далее - ИТКС Интернет).

1.2. Оператором ИС ГЖС выступает Федеральное казенное учреждение «Объединенная дирекция по реализации федеральных инвестиционных программ» Министерства строительства и жилищно-коммунального хозяйства Российской Федерации (далее – Оператор, Учреждение).

1.3. Пользователями ИС ГЖС являются уполномоченные сотрудники Оператора. Ограниченный доступ к ресурсам ИС ГЖС также предоставляется пользователям ИС ГЖС – уполномоченным сотрудникам федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, органов местного самоуправления закрытых административно-территориальных образований, органов местного самоуправления муниципальных образований, в границы которых включены территории, ранее входившие в закрытые административно-территориальные образования, и администрации города Байконура, осуществляющих выдачу государственных жилищных сертификатов (далее – ГЖС) в рамках государственной программы Российской Федерации «Обеспечение доступным и комфортным жильем и коммунальными услугами граждан Российской Федерации» (далее – органы, осуществляющие выдачу ГЖС).

1.4. ИС ГЖС функционирует на двух физических серверах под управлением сертифицированной операционной системы Astra Linux Special Edition релиз «Смоленск».

1.5. Пользователям ИС ГЖС предоставляется доступ к ресурсам ИС ГЖС с использованием каналов связи ИТКС Интернет. Для организации доступа использован сертифицированный Веб-сервер Apache2 из состава операционной системы Astra Linux Special Edition релиз «Смоленск».

1.6. В соответствии с возможностями актуального нарушителя, определенными в частной модели угроз безопасности информации ИС ГЖС, и, руководствуясь требованиями Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации (далее – СЗКИ), необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, утвержденных приказом Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. № 378, средства криптографической защиты информации в случае использования для защиты каналов связи ИС ГЖС, должны соответствовать требованиям Федеральной службы безопасности Российской Федерации к защищенности СКЗИ по классу не ниже КС1.

1.7. Для организации защищенных каналов связи ИС ГЖС применяются следующие сертифицированные средства защиты информации:

№ п/п	Наименование и тип средств защиты информации	Сведения о сертификате	Место установки
1.	АПКШ «Континент» 3.7 IPC-10-FW	ФСБ России № СФ/124-3018 Действителен до 16.декабря.2021 г. ФСБ России № СФ/525-3138 Действителен до 19 мая 2020 г.	В локальной сети на границе ИС ГЖС
2.	ПАК «Соболь» 3.0	ФСБ России № СФ/527-2623 Действителен до 01 июня 2020 г.	В составе АПКШ «Континент» 3.7
3.	АПКШ «Континент» 3.7-СОА. Детектор атак. IPC100	ФСБ России № СФ/СЗИ-0088 Действителен до 30 июня 2019 г.	В локальной сети
4.	СКЗИ «Континент-АП» 3.7	ФСБ России СФ/124-3019 Действителен до 16 декабря 2019 г.	Автоматизированные рабочие места пользователей и администраторов

II. Организация защищенных каналов связи

2.1 Защищенный доступ к ресурсам ИС ГЖС (защита каналов связи) организован посредством сервера доступа АПКШ «Континент».

2.2. Для защищенного доступа к ресурсам ИС ГЖС с использованием каналов связи сетей общего пользования (ИТКС Интернет) органу, осуществляющему выдачу ГЖС, необходимо:

а) установить и настроить на автоматизированном рабочем месте (далее – АРМ) пользователя ИС ГЖС программу-клиент СКЗИ «Континент-АП» 3.7 КС1 или выше;

б) направить в адрес Оператора:

проект соглашения об информационном взаимодействии по форме согласно приложению № 2 к настоящему приказу;

декларацию о соответствии требованиям безопасности информации по форме согласно приложению № 3 к настоящему приказу;

заявку на предоставление доступа к ресурсам ИС ГЖС (организацию защищенного канала связи) по форме согласно приложению № 1 к настоящему Регламенту.

2.3. В случае положительного решения о предоставлении доступа к ресурсам ИС ГЖС администратор СКЗИ Оператора с использованием средств центра управления сетью (ЦУС) АПКШ «Континент» генерирует ключевую информацию (сертификат) в электронном виде и направляет администратору СКЗИ органа, осуществляющего выдачу ГЖС (далее – локальный администратор СКЗИ), или пользователю ИС ГЖС способом, исключающим ее компрометацию, указанным в заявке о предоставлении доступа к ресурсам ИС ГЖС.

При выборе способа направления ключевой информации (сертификата) на CD-R или DVD-R диске либо на флэш-карте одновременно с заявкой о предоставлении доступа Оператору направляется соответствующий носитель электронной информации для записи на нем ключевой информации (сертификата).

Допускается направление заархивированной ключевой информации (сертификата), защищенной паролем, по электронной почте, указанной в заявке на предоставление доступа к ресурсам ИС ГЖС. В данном случае пароль к архиву направляется способом, отличным от передачи ключевой информации (сертификата).

В случае, если в заявке о предоставлении доступа к ресурсам ИС ГЖС не указан способ направления ключевой информации (сертификата) указанный способ определяет Оператор.

2.4. Пароль, необходимый для настройки СКЗИ, сообщается локальному администратору СКЗИ или пользователю ИС ГЖС способом, отличным от передачи ключевой информации (сертификата).

Пароль, необходимый для настройки СКЗИ, меняется не реже одного раза в год. При назначении нового пароля уполномоченный сотрудник

Оператора сообщает его локальному администратору СКЗИ или пользователю ИС ГЖС способом, исключающим ее компрометацию, указанным в заявке о предоставлении доступа к ресурсам ИС ГЖС.

2.5. В случае утери пароля орган, осуществляющий выдачу ГЖС, направляет в адрес Оператора заявку на восстановление парольной фразы по форме согласно приложению № 2 к настоящему Регламенту.

Администратор СКЗИ Оператора производит генерацию новой парольной фразы и сообщает его пользователю ИС ГЖС способом, исключающим ее компрометацию, указанным в заявке на восстановление парольной фразы.

2.6. В случае компрометации ключевой информации (сертификата) к СКЗИ осуществляется внеплановая смена ключевой информации (сертификата) к СКЗИ.

К событиям, связанным с компрометацией ключевой информации (сертификата), относятся (включая, но не ограничиваясь) следующие ситуации:

потеря ключевых носителей;

потеря ключевых носителей с их последующим обнаружением;

увольнение сотрудников, имевших доступ к ключевой информации;

нарушение правил хранения и уничтожения ключей;

возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;

нарушение печати на сейфе с ключевыми носителями;

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

2.7. В случае компрометации ключей к СКЗИ, орган, осуществляющий выдачу ГЖС, направляет в адрес Оператора заявку на перевыпуск ключевой информации (сертификата) по форме согласно приложению № 3 к настоящему Регламенту.

Администратор СКЗИ Оператора производит генерацию новой ключевой информации (сертификата) и направляет пользователю ИС ГЖС способом, исключающим ее компрометацию, указанным в заявке на перевыпуск криптографических ключей.

III. Уполномоченные сотрудники оператора

3.1. В компетенцию уполномоченных сотрудников Оператора (администраторов ИС ГЖС и СКЗИ) входит решение следующих вопросов, возникающих при использовании защищенной сети передачи данных:

а) в рамках администрирования защищенной сети передачи данных:

создает и удаляет абонентские пункты сети;

обеспечивает работоспособность сети в зоне его ответственности;

ведёт учёт и обеспечивает хранение полученных заявок;

б) в рамках технического сопровождения:

оказывает консультации уполномоченным представителям органов, осуществляющих выдачу ГЖС, при возникновении неисправностей, таких как блокировка рабочей станции вследствие нарушения режима безопасности, потеря связи между узлами сети;

оказывает консультации уполномоченных представителей органов, осуществляющих выдачу ГЖС, по организационным и техническим вопросам эксплуатации ИС ГЖС и СКЗИ;

3.2. Актуализация информации СКЗИ.

В целях настоящего Регламента под актуализацией информации СКЗИ понимается:

добавление или удаление доступа к другому узлу СКЗИ (изменение СКЗИ-связей узла);

изменение имени пользователя или имени абонентского пункта СКЗИ.

Изменение имени пользователя или имени абонентского пункта СКЗИ допускается только в рамках одной органа, осуществляющего выдачу ГЖС.

Для осуществления вышеуказанных действий орган, осуществляющий выдачу ГЖС, направляет заявку в адрес Оператора. В заявке указывается:

наименование органа, осуществляющего выдачу ГЖС, фамилия, имя и отчество администратора (пользователя) СКЗИ, телефон и электронная почта для обратной связи;

идентификаторы сетевых узлов либо идентификаторы пользователей СКЗИ, подлежащих изменению.

IV. Обязанности органа, осуществляющего выдачу ГЖС,

4.1. Орган, осуществляющий выдачу ГЖС, подключаемый к ИС ГЖС, назначает уполномоченных лиц (локальных администраторов СКЗИ), ответственных за организацию связи и обеспечение безопасности при взаимодействии с ИС ГЖС, определяет перечень сотрудников, которым необходим доступ к ресурсам ИС ГЖС (пользователей СКЗИ).

4.2. Локальный администратор СКЗИ, в своей работе руководствуется требованиями законодательства РФ и внутренними локальными нормативными актами, регламентирующими работу в ИС ГЖС, требованиями федеральных законов в области защиты информации, руководящими и нормативными документами уполномоченных органов (ФСТЭК России, ФСБ России, Роскомнадзор), документацией ИС ГЖС и настоящим Регламентом.

4.3. Локальный администратор СКЗИ обязан:

осуществлять установку, настройку и поддержку в надлежащем работоспособном состоянии аппаратных и программных СКЗИ, включая определение категорий пользователей и назначение им прав, настройку политики контроля событий безопасности на серверах и рабочих станциях организации, взаимодействующих с ИС;

осуществлять настройку и управление средствами межсетевого экранирования и коммуникационного оборудования, находящиеся в зоне ответственности организации-участника;

вести поэкземплярный учёт используемых в своей организации СКЗИ, эксплуатационной и технической документации, ключевых документов;

контролировать соблюдение пользователями СКЗИ правил эксплуатации СКЗИ, ограничивает доступ к СКЗИ посторонних лиц;

контролировать неизменность состояния средств защиты, их параметров и режимов защиты, физическую сохранность СКЗИ и ключевых документов, соблюдение режима безопасности, а также установленных правил работы с СКЗИ;

своевременно анализировать журнал учёта событий, регистрируемых средствами защиты, с целью выявления возможных нарушений;

не допускать установку, использование, хранение и тиражирование на технических средствах, на которых установлены СКЗИ программных средств, не связанных с выполнением функциональных задач,

оказывать помощь пользователям в части применения СКЗИ и консультирует по вопросам введённого режима защиты;

в случае отказа работоспособности технических средств с установленными СКЗИ, в том числе средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

4.4. В случае невозможности самостоятельного устранения сбоев в работе, локальный администратор СКЗИ взаимодействует с уполномоченными специалистами Оператора и (или) Организаций-Лицензиатов.

4.5. Пользователь СКЗИ несёт персональную ответственность за свои действия. В своей работе Пользователь СКЗИ руководствуется требованиями законодательства РФ и внутренними локальными нормативными актами, регламентирующими работу с СКЗИ.

4.6. Пользователь СКЗИ обязан:

выполнять требования настоящего регламента, действующих нормативных документов и внутренних инструкций и распоряжений, регламентирующих порядок работы с СКЗИ;

знать и соблюдать установленные требования по учёту, хранению и пересылке носителей информации, обеспечению безопасности информации, а также руководящих и организационно-распорядительных документов;

немедленно докладывать администратору СКЗИ обо всех выявленных нарушениях в работе СКЗИ.

4.7. При возникновении неполадок, связанных с работой СКЗИ, пользователь СКЗИ обязан:

немедленно поставить в известность локального администратора СКЗИ;

следовать дальнейшим инструкциям локального администратора СКЗИ.

4.8. При возникновении неполадок, связанных с работой СКЗИ, локальный администратор СКЗИ обязан разобраться в характере неполадки и принять меры, направленные на устранение. Локальный администратор СКЗИ должен знать варианты устранения типовых неполадок, используя для этого документацию СКЗИ и соответствующие инструкции.

В случае невозможности устранить неисправность своими силами, орган, осуществляющий выдачу ГЖС, обращается за технической поддержкой к специалистам Оператора и (или) Организаций-Лицензиатов.