Приложение № 1

к приказу ФКУ «Объединенная дирекция» Минстроя России

от « 20 » сентября 2024 г. № ПРВ-15

**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 ФКУ «Объединенная дирекция» Минстроя России (далее – Оператор).

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, исполнительных органов 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 в рамках государственной программы Российской Федерации «Обеспечение доступным и комфортным жильем и коммунальными услугами граждан Российской Федерации» либо работающих с информационными ресурсами Единого реестра граждан, перед которыми имеются федеральные жилищные обязательства (которые имеют право на государственную поддержку в улучшении жилищных условий) (далее ‑ организации, осуществляющие работу в ИС ГЖС).

1.4. ИС ГЖС развернута и функционирует на ресурсах информационной инфраструктуры Оператора.

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 –СКЗИ), 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, СКЗИ 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.

**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 организации, осуществляющей работу в ИС ГЖС, необходимо:

а) приобрести право на использование (лицензию) программного обеспечения;

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 по форме согласно приложению № 1 к настоящему Регламенту;

копию права на использование (лицензию) программного обеспечения.

2.3. В случае положительного решения о предоставлении доступа к ресурсам ИС ГЖС администратор СКЗИ с использованием средств центра управления сетью АПКШ «Континент» генерирует ключевую информацию в электронном виде и направляет Оператору, далее Оператор направляет ключевую информацию локальному администратору СКЗИ (далее – локальный администратор СКЗИ) или пользователю ИС ГЖС организации, осуществляющей работу в ИС ГЖС, способом, исключающим компрометацию ключевой информации, указанным в заявке на предоставление доступа к ресурсам ИС ГЖС.

При выборе способа направления ключевой информации 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.

Допускается направление заархивированной ключевой информации, 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.

В случае, если в заявке на предоставление доступа к ресурсам ИС ГЖС не указан способ направления ключевой информации 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.

Пароль, необходимый для настройки СКЗИ, меняется не реже одного раза в год.

2.5. Локальному администратору СКЗИ или пользователю ИС ГЖС необходимо с использованием полученной ключевой информации установить и настроить на автоматизированном рабочем месте пользователя ИС ГЖС программу-клиент СКЗИ «Континент-АП».

2.6. В случае утери пароля организация, осуществляющая работу   
в ИС ГЖС, направляет в адрес Оператора заявку на перевыпуск ключевой информации по форме согласно приложению № 2 к настоящему Регламенту.

Администратор СКЗИ производит перевыпуск ключевой информации и направляет ее Оператору, далее Оператор направляет ключевую информацию пользователю ИС ГЖС способом, исключающим компрометацию ключевой информации, указанным в заявке на перевыпуск ключевой информации.

2.7. В случае компрометации ключевой информации осуществляется внеплановая смена ключевой информации.

К событиям, связанным с компрометацией ключевой информации, 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).

2.8. В случае компрометации ключевой информации, организация, осуществляющая работу в ИС ГЖС, направляет в адрес Оператора заявку на перевыпуск ключевой информации по форме согласно приложению № 2 к настоящему Регламенту.

Администратор СКЗИ производит генерацию новой ключевой информации и направляет ее Оператору, Оператор направляет пользователю ИС ГЖС способом, исключающим ее компрометацию, указанным в заявке на перевыпуск ключевой информации.

**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 организаций, осуществляющих работу в ИС ГЖС, при возникновении неисправностей, таких как блокировка рабочей станции вследствие нарушения режима безопасности, потеря связи между узлами сети;

оказывает консультации уполномоченных представителей организаций, осуществляющих работу в ИС 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 организации, осуществляющей работу в ИС ГЖС.

Для осуществления вышеуказанных действий организация, осуществляющая работу в ИС ГЖС, направляет заявку в адрес Оператора. В заявке указывается:

наименование организации, осуществляющей работу в ИС 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 организации, осуществляющей работу в ИС ГЖС.**

4.1. Организация, осуществляющая работу в ИС ГЖС, подключаемая 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 ГЖС;

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 СКЗИ, локальный администратор СКЗИ обращается   
к уполномоченным специалистам Оператора, разработчика СКЗИ и (или) организации-лицензиата.

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, организация, осуществляющая работу в ИС ГЖС, обращается за технической поддержкой к специалистам Оператора и (или) Организаций-Лицензиатов.

Приложение № 1

к Регламенту доступа

к ресурсам информационной системы с использованием каналов связи сетей общего пользования

ФОРМА

ЗАЯВКА

на предоставление 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»

(организацию защищенного канала связи)

(полное наименование юридического лица)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ИНН: |  | | | |
| в лице | |  | | |
|  | | (должность, фамилия, имя и отчество (при наличии) руководителя или ответственного лица за информационную безопасность, с указанием реквизитов приказа о назначении ответственного лица) | | |
| в связи с | | |  | |
|  | | | (указывается основание для предоставления доступа (плановое подключение, предоставление доступа новому сотруднику и т.д.) | |
| Ключевую информацию прошу направить: | | | |  |
|  | | | | |
| (указывается способ отправки и адрес) | | | | |

|  |  |
| --- | --- |
| Пароль (пароли) прошу сообщить: |  |
|  | (указывается способ, отличный от способа доставки ключевой информации: электронная почта; СМС по телефону) |

|  |  |
| --- | --- |
| Для следующих сотрудников: |  |
|  | (должность, фамилия, имя и отчество в именительном падеже, номер телефона, электронная почта,  версия СКЗИ «Континент АП», операционная система на автоматизированном рабочем месте сотрудника) |
|  | (должность, фамилия, имя и отчество в именительном падеже, номер телефона, электронная почта,  версия СКЗИ «Континент АП», операционная система на автоматизированном рабочем месте сотрудника) |

Инструктаж пользователей средств криптографической защиты информации проведён, ведётся учёт используемых средств криптографической защиты информации, требования по работе с средств криптографической защиты информации, утверждённые приказом ФСБ России от 21 февраля 2008 г.   
№ 149/6/6-622, и приказом ФАПСИ от 13 июня 2001 г. № 152, соблюдаются.

|  |  |  |  |
| --- | --- | --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_ |
| (должность, фамилия, имя и отчество руководителя или ответственного лица за информационную безопасность) | (подпись) | (фамилия и инициалы) | (дата) |

М.П.

Приложение № 2

к Регламенту доступа

к ресурсам информационной системы с использованием каналов связи сетей общего пользования

ФОРМА

ЗАЯВКА

на перевыпуск ключевой информации для предоставления 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»

(организации защищенного канала связи)

(полное наименование юридического лица)

|  |  |  |
| --- | --- | --- |
| в лице |  | |
|  | (должность, фамилия, имя и отчество руководителя или ответственного лица за информационную безопасность, с указанием реквизитов приказа о назначении ответственного лица) | |
| в связи с | |  |

(указывается основание для превыпуска ключевой информации)

прошу перевыпустить ключевую информацию для следующих пользователей средств криптографической защиты информации:

|  |  |  |
| --- | --- | --- |
| Прежнее имя  сертификата безопасности ключевой информации | Должность, фамилия,  имя и отчество,  номер телефона, электронная почта | Используемая версия СКЗИ «Континент АП», операционная система на автоматизированном рабочем месте пользователя СКЗИ |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| |  | | --- | | Ключевую информацию прошу направить: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (указывается способ отправки и адрес) |   Пароль (пароли) прошу сообщить: | |
|  | (указывается способ, отличный от способа доставки ключевой информации: электронная почта; СМС по телефону) |

По факту утраты (уничтожения, компрометации) ключевой информации проведено служебное расследование. Результаты расследования прилагаю\*.

После получения новой ключевой информации, старая ключевая информация будет удалена из средств криптографической защиты информации и снята с учёта, пароли пользователей уничтожены.

|  |  |  |  |
| --- | --- | --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_ |
| (должность, фамилия, имя и отчество руководителя или ответственного лица за информационную безопасность) | (подпись) | (фамилия и инициалы) | (дата) |

М.П.

<\*> - информация указывается в случае компрометации ключевой информации

Приложение № 2

к приказу ФКУ «Объединенная дирекция» Минстроя России

от «20» сентября 2024 г. № ПРВ-15

ФОРМА

СОГЛАШЕНИЕ №\_\_\_\_\_\_\_

"\_\_\_\_\_"\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_г.

**Об информационном взаимодействии**

Федеральное казенное учреждение «Объединенная дирекция   
по реализации федеральных инвестиционных программ» Министерства строительства и жилищно-коммунального хозяйства Российской Федерации   
(далее – ФКУ «Объединенная дирекция» Минстроя России), именуемое   
в дальнейшем «Оператор», в лице начальника Управления обеспечения жильем отдельных категорий граждан ФКУ «Объединенная дирекция» Минстроя России Бабарицкого Анатолия Николаевича с одной стороны, и \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(наименование органа, осуществляющего выдачу государственных жилищных сертификатов, либо работающих с информационными ресурсами Единого реестра)

именуемый в дальнейшем «Организация-участник», в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ с другой стороны, вместе именуемые «Стороны» и каждый в отдельности «Сторона», руководствуясь требованиями законодательства Российской Федерации в области персональных данных и приказом ФКУ «Объединенная дирекция» Минстроя России от «\_\_» сентября 2024 г. № \_\_\_, заключили настоящее Соглашение о нижеследующем:

1. Стороны осуществляют защищенное информационное взаимодействие в рамках функционирования 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, информационная система).

2. При осуществлении информационного взаимодействия Стороны обязуются руководствоваться Правилами выпуска и реализации государственных жилищных сертификатов в рамках реализации комплекса процессных мероприятий «Выполнение государственных обязательств по обеспечению жильем отдельных категорий граждан» государственной программы Российской Федерации «Обеспечение доступным и комфортным жильем и коммунальными услугами граждан Российской Федерации», утверждёнными постановлением Правительства Российской Федерации от 21 марта 2006 г. № 153, и Регламентом предоставления доступа 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» с использованием каналов связи сетей общего пользования (далее – Регламент), утвержденным приказом ФКУ «Объединенная дирекция» Минстроя России от «\_\_» сентября 2024 г. № \_\_\_.

3. Условия получения доступа к ресурсам информационной системы и размещения (публикации) в ней информации устанавливаются Регламентом.

4. Обязанности сторон

4.1. Оператор:

а) обеспечивает доступ к ресурсам информационной системы;

б) обеспечивает размещение (публикацию) в информационной системе информации Организации-участника.

4.2. Организация-участник:

а) выполняет требования информационной безопасности при осуществлении доступа к ресурсам информационной системы с использованием каналов связи сетей общего пользования, установленные Регламентом;

б) отвечает за правомочность и достоверность информации, размещенной (опубликованной) в информационной системе в соответствии с законодательством Российской Федерации.

5. В случае нарушения Организацией-участником пункта 4.2 настоящего Соглашения Оператор вправе приостановить доступ Организации-участника к ресурсам информационной системы до устранения нарушения.

6. Стороны соглашаются считать информацию, полученную при информационном взаимодействии в рамках настоящего Соглашения, конфиденциальной и не подлежащей разглашению.

7. Стороны имеют право прекратить действие настоящего Соглашения в одностороннем порядке путем письменного уведомления об этом другой Стороны.

8. По взаимному согласию Сторон в настоящее Соглашение могут вноситься изменения и дополнения, оформляемые дополнительными соглашениями.

9. Спорные вопросы, возникающие между Сторонами, связанные с толкованием и (или) реализацией настоящего Соглашения, решаются путем проведения консультаций и переговоров.

10. Настоящее Соглашение не налагает на Стороны никаких финансовых обязательств.

11. Настоящее Соглашение вступает в силу с даты его подписания Сторонами и заключается на неопределенный срок.

12. Настоящее Соглашение составлено в двух экземплярах, имеющих одинаковую юридическую силу, один экземпляр для Оператора ИС ГЖС, второй экземпляр для Организации-участника.

13. Место нахождения, адреса сторон:

Оператор:

Место нахождения: Российская Федерация, 109316, г. Москва, Волгоградский проспект, д. 45, стр. 1.

Организация-участник:

Место нахождения:

|  |  |  |
| --- | --- | --- |
| **Оператор ИС ГЖС**  Начальник Управления обеспечения жильем отдельных категорий граждан ФКУ «Объединенная дирекция» Минстроя России  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_А.Н. Бабарицкий |  | **Организация-участник**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (должность, подпись, расшифровка подписи) |

Приложение № 3

к приказу ФКУ «Объединенная дирекция»

Минстроя России

от «20» сентября 2024 г. № ПРВ-15

ФОРМА

**ДЕКЛАРАЦИЯ О СООТВЕТСТВИИ**

требованиям безопасности информации

1. Сведения об организации (*наименование, местонахождение, ИНН*).

2. Настоящей Декларацией подтверждается соответствие информационной системы (автоматизированных рабочих мест пользователей) Организации, подключаемых к информационной системе учета выданных и оплаченных государственных жилищных сертификатов в рамках государственной программы Российской Федерации «Обеспечение доступным и комфортным жильем и коммунальными услугами граждан Российской Федерации» (ИС ГЖС) требованиям законодательства Российской Федерации в области персональных данных, включая применение правовых, организационных и технических мер по обеспечению безопасности персональных данных, определенных статьями 18.1 и 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», в соответствии с:

приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

приказом Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

3. Принятые меры по обеспечению безопасности персональных данных обеспечивает 3-й уровень защищенности и нейтрализацию актуальных угроз безопасности информации.

4. Номер организации в Реестре операторов, осуществляющих обработку персональных данных \_\_\_\_\_\_\_\_\_\_\_\_.

|  |  |  |  |
| --- | --- | --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_ |
| (должность, фамилия, имя и отчество (при наличии) руководителя (заместителя руководителя) | (подпись) | (фамилия и инициалы) | (дата) |