Утверждено приказом ООО «ЕРКЦ»
от 26.05.2025 № 41

Положение о защите персональных данных, обрабатываемых в информационной системе «Реестр жилого фонда»

1. Используемые понятия

Безопасность информации – состояние защищенности информации, обрабатываемой средствами вычислительной техники от внутренних или внешних угроз, при котором обеспечены ее конфиденциальность, доступность и целостность.

Доступность информации – состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информация ограниченного доступа – информация, доступ к которой ограничен федеральными законами, за исключением сведений, составляющих государственную тайну.

Конфиденциальность информации – состояние информации (ресурсов информационной системы), при котором доступ к ней осуществляют только субъекты, имеющие на него право.

Оператор информационной системы (оператор) – государственный орган, муниципальный орган, юридическое или физическое лицо, организующий и (или) осуществляющий деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Средства криптографической защиты информации – средства защиты информации, реализующее алгоритмы криптографического преобразования информации.

ФСБ России – Федеральная служба безопасности Российской Федерации.

ФСТЭК России – Федеральная служба по техническому и экспортному контролю.

Целостность информации – состояние защищенности информации, характеризуемое способностью обеспечивать сохранность и неизменность защищаемой информации при попытках несанкционированного или случайного воздействия на нее в процессе обработки или хранения.

2. Общие положения

Настоящее положение о защите персональных данных, обрабатываемой в информационной системе «Реестр жилого фонда» ООО «ЕРКЦ» (далее – Положение), разработано на основании:

1) Федерального закона Российской Федерации от 27.06.2006 №152-ФЗ «О персональных данных»;

2) Федерального закона Российской Федерации от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;

3) Постановления Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

4) Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом ФСТЭК России от 18.02.2013 №21.

Положение определяет порядок организации и проведения работ по защите персональных данных, обрабатываемых в информационной системе «Реестр жилого фонда» (далее – ИС) ООО «ЕРКЦ» (далее – Общество).

Обладателем информации, содержащейся в ИС, является Общество.

Оператором ИС является Общество (далее – Оператор).

Положение предназначено для работников Оператора, работников сторонних организаций, допускаемых в установленном порядке к выполнению работ на основных технических средствах и системах ИС по модернизации оборудования и программного обеспечения ИС.

Ответственность за выполнение требований Положения возлагается на Оператора.

Положение вступает в силу с момента его утверждения руководителем Общества и действует бессрочно до замены его новым положением.

3. Тип обрабатываемой информации в ИС

В ИС осуществляется обработка персональных данных и общедоступной информации (общеизвестные сведения и иная информация, доступ к которой не ограничен (ст. 7 Федерального закона №149-ФЗ).

4. Цели создания системы защиты информации

Целью создания системы защиты информации (далее – СЗИ) в ИС является предотвращение ущерба, возникновение которого возможно в результате утери, хищения, утраты, искажения, подделки информации в любом ее проявлении; реализация адекватных угрозам безопасности информации мер защиты в соответствии с действующими законами и нормативными документами по безопасности информации РФ.

Для информации, обрабатываемой в ИС, требуется обеспечить ее конфиденциальность, целостность и доступность.

5. Основные направления работ по обеспечению безопасности информации

Основными направлениями работ по обеспечению безопасности информации в ИС являются:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к ней;

2) разработка и практическая реализация организационных и технических мероприятий по защите информации;

3) своевременное обнаружение фактов несанкционированного доступа к информации;

4) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

5) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

6) обеспечение возможности незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

7) осуществление постоянного контроля за обеспечением класса защищенности ИС.

6. Основные способы и меры по обеспечению безопасности информации

Основными способами и мерами по обеспечению безопасности информации в ИС являются:

1) привлечение лицензиатов ФСТЭК России для выполнения работ по технической защите информации;

2) противодействие утечке по техническим каналам, несанкционированному доступу, программно-техническому воздействию с целью нарушения конфиденциальности, целостности и доступности информации в процессе ее обработки, передачи и хранения;

3) применение автоматизированных систем в защищенном исполнении для обработки, хранения и передачи информации;

4) использование средств защиты информации, сертифицированных ФСТЭК России и ФСБ России, и контроль их эффективности;

5) аттестация ИС по требованиям безопасности информации.

7. Порядок обработки информации в ИС

Определение необходимого класса защищенности ИС и уровня защищенности персональных данных осуществляется комиссией, сформированной из числа работников Общества. В комиссию должны входить не менее трех человек.

По завершении процедуры классификации составляется Акт категорирования и классификации ИС.

На этапе проведения процедур категорирования и классификации ИС комиссией определяется состав информации, подлежащей защите, формируется перечень защищаемых информационных ресурсов в ИС.

Для ИС приказом руководителя Общества назначается лицо или подразделение, ответственное за организацию защиты информации в ИС (далее – Администратор ИБ, АИБ).

Администратор ИБ в своей деятельности руководствуется Инструкцией администратора информационной безопасности.

К техническому обслуживанию средств и систем ИС допускаются только лица, внесенные в списки лиц, допущенных к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены.

Любые изменения в конфигурации ИС, влияющие на класс защищенности, должны быть учтены АИБ в Журнале регистрации изменений в конфигурации информационной системы.

На основные технические средства и системы ИС может устанавливаться только программное обеспечение, внесенное в перечень программного обеспечения, разрешенного к установке в ИС, который разрабатывает АИБ.

Администратор ИБ составляет Технический паспорт ИС по форме, установленной в Порядке организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну (утвержден приказом ФСТЭК России от 29.04.2021 №77). Затем паспорт ИС утверждается руководителем Общества.

В ИС все съемные машинные носители и машинные носители информации подлежат учету.

В случае если в ИС имеется разграничение прав доступа пользователей к информации, АИБ разрабатывает разрешительную систему доступа к информационным ресурсам ИС с указанием субъектов и объектов доступа.

Для определения вероятных нарушителей и актуальных угроз безопасности для ИС разрабатывается модель угроз безопасности ИС. При необходимости к разработке модели угроз безопасности ИС могут привлекаться организации-лицензиаты ФСТЭК России и ФСБ России.

Ежегодно ответственный за планирование и контроль мероприятий по защите информации в информационной системе разрабатывает план мероприятий по обеспечению защиты информации в ИС на текущий год, который согласуется с руководителем Общества.

Ответственный за планирование и контроль мероприятий по защите информации в информационной системе производит учет всех мероприятий, направленных на обеспечение безопасности информации, обрабатываемой в ИС, в Журнале учета мероприятий по защите информации в ИС.

При обработке информации в ИС запрещается:

1) вносить несогласованные изменения в ИС, которые могут снизить класс защищенности информации;

2) проводить обработку информации без выполнения всех мероприятий по защите информации;

3) допускать к обработке информации лиц, не оформленных в установленном порядке;

4) производить копирование информации на неучтенные носители информации, в том числе для временного хранения информации;

5) обрабатывать информацию на технических средствах в составе ИС при обнаружении каких-либо неисправностей, а также при отключенных средствах защиты информации;

6) обрабатывать защищаемую информацию на технических средствах при окончании сроков действия сертификатов средств защиты информации, за исключением окончания срока действия сертификатов соответствия при условии соблюдения требований по безопасности информации и при наличии действующей технической поддержки на средства защиты информации;

7) передавать информацию за пределы контролируемой зоны без использования средств криптографической защиты.

8. Ответственность за нарушение норм, регулирующих обработку и защиту информации в ИС

Лицо (подразделение), разрешающее доступ работников к информации, несет персональную ответственность за данное разрешение.

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту информации в ИС, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами РФ, а также

привлекаются к гражданско-правовой, административной ответственности в порядке, установленном федеральными законами.

9. Заключительные положения

Администратор ИБ и пользователи ИС обязаны не реже одного раза в год ознакамливаться с Положением.

Администратор ИБ обязан пересматривать и приводить в соответствие положения настоящего документа в случае изменения законодательства Российской Федерации в области защиты информации.

10. Нормативно-правовые акты и методические документы по защите информации

1) Конституция Российской Федерации.

2) Федеральный закон Российской Федерации от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации».

3) Федеральный закон Российской Федерации от 27.07.2006 №152-ФЗ «О персональных данных».

4) Перечень сведений конфиденциального характера, утвержденный Указом Президента РФ от 06.03.1997 №188.

5) Перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами (утвержден постановлением Правительства РФ от 21.03.2012 №211).

6) Требования к защите персональных данных при их обработке в информационных системах персональных данных (утверждены постановлением Правительства РФ от 01.11.2012 №1119).

7) Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (утверждены приказом ФСТЭК России от 18.02.2013 №21).

8) Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (утверждена приказом ФАПСИ России от 13.06.2001 №152).

9) Методический документ «Меры по защите информации в государственных информационных системах», утвержденный ФСТЭК России 11.02.2014.