

Приложение №2

к приказу краевого
государственного казенного
учреждения "Центр социальной
поддержки населения по
г. Хабаровску"

от 11.11.2022 № 110

Положение

о защите информации, обрабатываемой в информационных системах
краевого государственного казенного учреждения "Центр социальной
поддержки населения по г. Хабаровску"

1. Общие положения

Настоящее Положение о защите информации, обрабатываемой
информационных системах краевого государственного казенного
учреждения "Центр социальной поддержки населения по г. Хабаровску"
(далее – Положение) разработано на основании:

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

2) Требований о защите информации, не составляющей
государственную тайну, содержащейся в государственных информационных
системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17;

Настоящее Положение определяет порядок организации и проведения
работ по защите информации (далее – Информация, ЗИ), обрабатываемой в
информационных системах (далее – ИС) в краевом государственном
казенном учреждении "Центр социальной поддержки населения по
г. Хабаровску" (далее – Учреждение).

Обладателем информации, содержащейся в ИС, и ее оператором
является Учреждение.

Настоящее Положение предназначено для оператора ИС, 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 настоящего Положения
возлагается на оператора ИС.

2. 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, организующие и(или) осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

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

ФСБ России – Федеральная служба безопасности.

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.

3. Тип обрабатываемой Информации в ИС

В ИС осуществляется обработка информации ограниченного доступа в соответствии с пунктами 1, 3 сведений конфиденциального характера, утвержденных Указом Президента РФ от 06.03.1997 №188.

4. Цели создания системы защиты Информации

Целью создания системы защиты Информации в ИС (далее – СЗИ) 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) передачу 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 сертифицированных ФСТЭК России и ФСБ России средств защиты информации и контроль их эффективности;
- 5) аттестация ИС по требованиям безопасности информации.

7. Порядок обработки Информации в ИС

Определение необходимого класса защищенности ИС осуществляется комиссией, сформированной из числа работников Министерства. В комиссию должно входить не менее трех человек.

По завершении процедуры классификации составляется Акт классификации ИС.

На этапе проведения процедур классификации ИС, комиссией определяется состав Информации, подлежащей защите, формируется Перечень защищаемых информационных ресурсов в ИС.

Для ИС приказом Учреждения 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 ИС.

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.

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 Матрицу 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 привлекать организации лицензиаты ФСТЭК России и ФСБ России, в соответствии с Федеральным законом от 05.04.2013 №44-ФЗ "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд".

Ежегодно, АИБ разрабатывает План мероприятий по обеспечению защиты Информации в ИС на следующий год, который согласуется с директором Учреждения.

Администратор ИБ производит учет всех мероприятий, направленных на обеспечение безопасности Информации, обрабатываемой в ИС, в Журнале учета мероприятий по защите Информации в ИС.

Не допускается обработка Информации в ИС:

- 1) при отсутствии установленных и настроенных сертифицированных ФСТЭК России и (или) ФСБ России средств защиты информации;
- 2) при отсутствии утвержденных организационных документов о порядке эксплуатации 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 на технических средствах в составе ИС Информацию при обнаружении каких-либо неисправностей, а также при отключенных средствах защиты информации;
- 6) обрабатывать на технических средствах защищаемую информацию 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, несут 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 ознакомляться с настоящим Положением.

Администратор ИБ совместно с лицом (подразделением), ответственным за защиту информации в ИС, обязаны 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 от 27 июля 2006г. №149-ФЗ "Об информации, информационных технологиях и о защите информации".
 - 3) Указ Президента Российской Федерации от 6 марта 1997г. №188 "Об утверждении перечня сведений конфиденциального характера".
 - 4) Приказ ФСТЭК России от 11 февраля 2013г. "Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах";
 - 5) Методический документ "Меры по защите информации в государственных информационных системах", утвержденный ФСТЭК России 11.02.2014.
-