Приложение №1
Утверждено
приказом директора
от 03.03.2025г №22/1

ПОЛОЖЕНИЕ
по организации и проведению работ по обеспечению безопасности персональных данных при их автоматизированной обработке в информационных системах в Государственном бюджетном учреждении Республики Крым «Центр социального обслуживания граждан пожилого возраста и инвалидов Бахчисарайского района»

г. Бахчисарай
2025

1. Общие положения

1.1. Положение об организации и проведении работ по обеспечению безопасности персональных данных при их автоматизированной обработке в информационных системах персональных данных (далее - Положение) разработано в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ "О персональных данных", Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", Приказом ФСТЭК России от 11.02.2013 №17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах", Приказом ФСТЭК России от 18.02.2013 №21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных", методическими рекомендациями ФСТЭК России и ФСБ России в целях обеспечения безопасности персональных данных (далее - ПДн) при их обработке в информационных системах персональных данных (далее - ИСПДн).

1.2. Положение определяет порядок работы персонала в ИСПДн в части обеспечения безопасности ПДн при их обработке, порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, разработку и принятие мер по предотвращению возможных опасных последствий таких нарушений, порядок приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления, порядок обучения персонала практике работы в ИСПДн, порядок контроля соблюдения условий использования средств защиты информации, предусмотренные эксплуатационной и технической документацией, правила обновления общесистемного и прикладного программного обеспечения, правила организации антивирусной защиты и парольной защиты ИСПДн, порядок охраны и допуска посторонних лиц в помещения ограниченного доступа.

2. Область действия документа

2.1. Действие Положения распространяется на информационные системы персональных данных Учреждения, в которых осуществляется обработка персональных данных.

2.2. Все работники Учреждения, допущенные к работе с персональными данными, в обязательном порядке должны быть ознакомлены с настоящим Положением под подпись.

3. Вступление в силу документа

3.1 Настоящее Положение вступает в силу с момента его утверждения руководителем и действует бессрочно до замены его новым Положением.

3.2 Все изменения в Положение вносятся приказом руководителя.

4. Организация и проведение работ по обеспечению безопасности персональных данных при их обработке информационных системах персональных данных

4.1. Планирование работ по обеспечению безопасности персональных данных

4.1.1. В целях исполнения настоящего Положения ответственный за защиту ПДи администратор безопасности составляет и утверждает у руководителя план работ по обеспечению безопасности персональных данных, обрабатываемых в Учреждении.

Проводимые в Учреждении мероприятия по обеспечению безопасности персональных данных учитываются в плане мероприятий по защите персональных данных в Учреждении.

4.2 Выполнение работ по обеспечению безопасности персональных данных

4.2.1. В целях организации и проведения работ по обеспечению безопасности персональных данных в Учреждении приказом руководителя назначаются:

- лицо, ответственное за проведение мероприятий по обеспечению безопасности персональных данных и поддержание необходимого уровня информационной безопасности;
- администратор информационной безопасности, ответственный за установку, настройку и обслуживание средств защиты информации, применяемых в Учреждении для обеспечения безопасности персональных данных, а также за организацию и проведение инструктажа работников по основам информационной безопасности при работе с персональными данными;
- комиссия по проведению классификации информационных систем.

4.2.2. Указанные лица ответственны за проведение следующих мероприятий по обеспечению безопасности персональных данных:

- определение и описание информационных систем персональных данных;
- классификацию информационных систем персональных данных;
- определение актуальных угроз безопасности персональных данных;

- проектирование системы защиты персональных данных, включающей организационные, физические и технические меры и средства защиты;

- закупку, установку и настройку технических средств защиты информации;

- внедрение организационных мер и разработку соответствующих регламентов и положений;

- инструктаж и обучение лиц, которые будут использовать средства защиты информации.

4.2.3. Руководители структурных подразделений, в которых происходит обработка персональных данных, являются лицами, ответственными за соблюдение требований Положения об обработке персональных данных и других установленных в Учреждении требований.

4.2.4. Для обеспечения безопасности персональных данных в Учреждении применяются следующие меры безопасности:

1) организационные меры безопасности:

- инструктаж работников по правилам обеспечения безопасности обрабатываемых персональных данных;

- учет и хранение съемных носителей информации и порядок их обращения, исключающие хищение, подмену и уничтожение;

- мониторинг и реагирование на инциденты информационной безопасности, связанные с персональными данными, включая проведение внутренних проверок, разбирательств и составление заключений;

- постоянный контроль за соблюдением требований по обеспечению безопасности персональных данных (реализуется путем внутренних аудитов);

2) меры физической безопасности:

- ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации. Приказом руководителя устанавливается контролируемая зона, вводятся в действие Список помещений с ограниченным доступом и Список лиц, имеющих право посещать помещения Учреждения с ограниченным доступом. Лица, не указанные в Списке, в том числе обеспечивающие техническое и бытовое обслуживание (уборку, ремонт оборудования и технических средств), при наличии необходимости могут посещать помещения с ограниченным доступом в сопровождении ответственных лиц;

- размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах охраняемой территории;

- организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку персональных данных;

3) технические меры безопасности:

- разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

- регистрация действий пользователей и обслуживающего персонала, контроль доступа и действий пользователей, обслуживающего персонала и посторонних лиц;

- резервирование технических средств, дублирование массивов и носителей информации;

- использование защищенных каналов связи;

- предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.

4.2.4. Ремонтно-восстановительные работы технических средств обработки информации проводятся администратором безопасности. В случае необходимости ремонт технических средств может быть проведен с привлечением сторонних специалистов на договорной основе с составлением актов выполненных работ.

5. Контроль выполнения работ по обеспечению безопасности персональных данных

5.1. Контроль выполнения работ по обеспечению безопасности персональных данных в Учреждении (далее – Контроль) осуществляется путем проведения периодических контрольных мероприятий (в рамках внутренних аудитов) и внутренних проверок по фактам произошедших инцидентов информационной безопасности.

5.2. В рамках проведения контрольных мероприятий выполняются:

- проверка наличия и актуальности планов, регистрационных журналов, актов, договоров, отчетов, протоколов и других свидетельств выполнения мероприятий по обеспечению безопасности персональных данных за истекший период;
- проверка осведомленности и соблюдения персоналом требований к обеспечению безопасности персональных данных;
- проверка соответствия перечня лиц, которым предоставлен доступ к персональным данным, фактическому состоянию;
- проверка наличия и исправности функционирования технических средств защиты информации, используемых для обеспечения безопасности персональных данных, в соответствии с требованиями эксплуатационной и технической документации;
- инструментальная проверка соответствия настроек технических средств защиты информации, требованиям к обеспечению безопасности персональных данных (при необходимости);
- проверка соответствия моделей угроз для информационных систем персональных данных условиям функционирования данных систем;

~ проверка соответствия организационно-распорядительной документации по обеспечению безопасности персональным данных действующим требованиям законодательства РФ, руководящих документов ФСБ России, ФСТЭК России.

5.3. Все собранные в ходе проведения контрольных мероприятий свидетельства и сделанные по их результатам заключения должны быть зафиксированы документально.

5.4. Контрольные мероприятия проводятся как периодически в соответствии с планом и программой аудита, так и внепланово по решению руководителя и в случае возникновения инцидентов информационной безопасности.

5.5. Внутренние проверки в Учреждении в обязательном порядке проводятся в случае выявления следующих фактов:

- нарушение конфиденциальности, целостности, доступности персональных данных;
- халатность и несоблюдение требований к обеспечению безопасности персональных данных;
- несоблюдение условий хранения носителей персональных данных;
- использование средств защиты информации, которые могут привести к нарушению заданного уровня безопасности (конфиденциальность/целостность/доступность) персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных.

5.6. Задачами внутренней проверки являются:

- установление обстоятельств нарушения, в том числе времени, места и способа его совершения;
- установление лиц, непосредственно виновных в данном нарушении;
- выявление причин и условий, способствовавших нарушению.

6. Совершенствование системы защиты персональных данных

6.1. Ежегодно ответственный за защиту персональных данных предоставляет руководителю отчет о проделанных мероприятиях по выполнению плана работ по обеспечению безопасности персональных данных вместе с перечнем предложений по совершенствованию системы защиты персональных данных.

6.2. Необходимость реализации мероприятий по совершенствованию системы защиты персональных данных может быть обусловлена:

- результатами проведенных аудитов и контрольных мероприятий;
- изменениями федерального законодательства в области персональных данных;
- изменениями структуры процессов обработки персональных данных в пенсионном фонде;
- результатами анализа инцидентов информационной безопасности;

- результатами мероприятий по контролю и надзору за обработкой персональных данных, проводимых уполномоченным органом;

- жалоб и запросов субъектов персональных данных.

6.3. На основании решения, принятого руководителем по результатам рассмотрения ежегодного отчета и предложений по совершенствованию системы защиты персональных данных, ответственный за защиту персональных данных составляет план работ по обеспечению безопасности персональных данных, обрабатываемых в Учреждении, на следующий год.