ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ СОЦИАЛЬНОГО ОБСЛУЖИВАНИЯ «КОМПЛЕКСНЫЙ ЦЕНТР СОЦИАЛЬНОГО ОБСЛУЖИВАНИЯ «ИСТОК»

П Р И К А З

«03» июня 2025 года №94-п

г. Ульяновск

Об утверждении инструкций

В соответствии со статьей 18.1 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»,

ПРИКАЗЫВАЮ:

1. Назначить ответственным за обеспечение безопасности персональных данных, администратором информационной безопасности в Областного государственном бюджетного учреждения социального обслуживания «Комплексный центр социального обслуживания «Исток» системного администратора информационно-коммуникационных систем.
2. Утвердить:

- Инструкцию пользователя информационных систем персональных данных Областного государственном бюджетного учреждения социального обслуживания «Комплексный центр социального обслуживания «Исток» согласно Приложению №1;
- Должностную инструкцию, ответственного за обеспечение безопасности персональных данных в Областного государственном бюджетного учреждения социального обслуживания «Комплексный центр социального обслуживания «Исток» согласно Приложению №2;
- Инструкцию по учету лиц, допущенных к работе с персональными данными в информационных системах персональных данных Областного государственном бюджетного учреждения социального обслуживания «Комплексный центр социального обслуживания «Исток» с формой журнала, согласно Приложению №3;
- Инструкцию по проведению инструктажа лиц, допущенных к работе с информационными системами персональных данных Областного государственном бюджетного учреждения социального обслуживания «Комплексный центр социального обслуживания «Исток» согласно Приложению №4;
- Инструкция по работе с информационными ресурсами информационно-коммуникационной сети «Интернет» в Областном государственном бюджетным учреждением социального обслуживания «Комплексный центр социального обслуживания «Исток» согласно Приложению №5

- Инструкцию по порядку учета, хранения и уничтожения персональных данных на машинных носителях в Областном государственном бюджетным учреждением социального обслуживания «Комплексный центр социального обслуживания «Исток» согласно Приложению №6;
- Инструкцию по порядку учета, хранения и уничтожения персональных данных, хранящихся на бумажных носителях в Областном государственном бюджетным учреждением социального обслуживания «Комплексный центр социального обслуживания «Исток» согласно Приложению №7;
- Инструкцию по организации антивирусной защиты информационных систем персональных данных в Областном государственном бюджетным учреждением социального обслуживания «Комплексный центр социального обслуживания «Исток» согласно Приложению №8;
- Инструкцию по организации парольной защиты информационных систем персональных данных в Областном государственном бюджетным учреждением социального обслуживания «Комплексный центр социального обслуживания «Исток» согласно Приложению №9;
- Инструкцию по организации резервного копирования и восстановления данных в информационных системах персональных данных Областного государственном бюджетного учреждения социального обслуживания «Комплексный центр социального обслуживания «Исток» согласно Приложению №10;
- Инструкцию пользователя при возникновении нештатной ситуации (инцидентах информационной безопасности) в Областного государственном бюджетного учреждения социального обслуживания «Комплексный центр социального обслуживания «Исток» согласно Приложению №11;
- Инструкция по учету машинных носителей и мобильных технических средств, предназначенных для работы с персональными данными в Областном государственном бюджетным учреждением социального обслуживания «Комплексный центр социального обслуживания «Исток» согласно Приложению №12.

Директор Н.А. Якимова

Приложение N 1
к приказу
ОГБУСО КЦСО «Исток»
от 3 июня 2025 г. N 97-п

ИНСТРУКЦИЯ

пользователя информационных систем персональных данных Областного государственного бюджетного учреждения социального обслуживания «Комплексный центр социального обслуживания «Исток»

1. ОБЩИЕ ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ОБРАБОТКИ ИНФОРМАЦИИ В ИСПДН

1.1. К защищаемой информации, обрабатываемой в информационных системах персональных данных Областного государственного бюджетного учреждения социального обслуживания «Комплексный центр социального обслуживания «Исток» (далее ИСПДн Учреждения), относятся персональные данные, служебная (технологическая) информация системы защиты, другая информация конфиденциального характера.

1.2. Обработка защищаемой информации в ИСПДн Учреждения разрешается на основании приказа директора.

1.3. Ответственность за организацию защиты информации в ИСПДн Учреждения и выполнение установленных условий ее функционирования возлагается на директора. Ответственность за выполнение мероприятий по обеспечению безопасности информации возлагается на лицо, производящее ее обработку (пользователя ИСПДн Учреждения).

1.4. Допуск пользователей к работе в ИСПДн Учреждения осуществляется в соответствии со «Списком лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения договорных (трудовых) обязанностей», утверждаемым генеральным директором.

1.5. К самостоятельной работе на автоматизированных рабочих местах (АРМ), входящих в состав ИСПДн Учреждения, допускаются лица, изучившие требования настоящей Инструкции и освоившие правила эксплуатации АРМ и технических средств защиты. Допуск производится после проверки знания настоящей Инструкции и практических навыков в работе.

1.6. Помещения, в которых размещены технические средства ИСПДн Учреждения, отвечают режимным требованиям и в нерабочее время сдаются под охрану установленным порядком.

1.7. Вход в помещения, в которых производится автоматизированная обработка защищаемой информации, разрешается постоянно работающим в нем сотрудникам, а также лицам, привлекаемым к проведению ремонтных, наладочных и других работ и посетителей (клиентов) в сопровождении сотрудника Учреждения.

1.8. Техническое обслуживание АРМ, уборка помещения и т.п. проводятся только под контролем сотрудника Учреждения. При проведении этих работ обработка защищаемой информации (ПДн) запрещается.

1.9. По фактам и попыткам несанкционированного доступа к защищаемой информации, а также в случаях ее утечки и (или) модификации (уничтожения) проводятся служебные расследования.

2. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ

2.1. При первичном допуске к работе в ИСПДн Учреждения пользователь знакомится с требованиями руководящих, нормативно-методических и организационно-распорядительных (регламентирующих) документов по вопросам безопасности при автоматизированной обработке информации, изучает настоящую Инструкцию, получает личный текущий пароль у регионального управляющего, выполняющего функции администратора безопасности информации в ИСПДн Учреждения (далее - администратор безопасности).

2.2. Каждый сотрудник Учреждения, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн Учреждения, несет персональную ответственность за свои действия <1> и обязан:

<1> Сотрудники Учреждения, виновные в нарушении режима защиты ПДн, несут дисциплинарную, гражданскую, административную, уголовную и иную предусмотренную законодательством Российской Федерации ответственность.

2.2.1. Строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн Учреждения.

2.2.2. Знать и строго выполнять правила работы со средствами защиты информации, установленными в ИСПДн Учреждения.

2.2.3. Хранить в тайне свой пароль.

2.2.4. Передавать для хранения установленным порядком при необходимости свои реквизиты разграничения доступа только администратору безопасности Учреждения.

2.2.5. Выполнять требования по антивирусной защите в части, касающейся действий пользователей.

2.2.6. Немедленно ставить в известность администратора безопасности в следующих случаях:

- при подозрении компрометации личного пароля;
- обнаружения нарушения целостности пломб (наклеек) на аппаратных средствах АРМ или иных фактов совершения в отсутствие пользователя попыток несанкционированного доступа (НСД) к ресурсам ИСПДн Учреждения;
- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн Учреждения;

- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию ИСПДн Учреждения, выхода из строя или неустойчивого функционирования узлов или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения;
- некорректного функционирования установленных средств защиты;
- обнаружения непредусмотренных отводов кабелей и подключенных устройств;
- обнаружения фактов и попыток НСД и случаев нарушения установленного порядка обработки защищаемой информации.

2.3. Пользователю категорически запрещается:

2.3.1. Использовать компоненты программного и аппаратного обеспечения ИСПДн Учреждения в неслужебных целях.

2.3.2. Самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн Учреждения или устанавливать дополнительно любые программные и аппаратные средства.

2.3.3. Осуществлять обработку защищаемой информации в присутствии посторонних (не допущенных к данной информации) лиц.

2.3.4. Записывать и хранить защищаемую информацию на неучтенных носителях информации (гибких магнитных дисках и т.п.).

2.3.5. Оставлять включенным без присмотра АРМ, не активизировав средства защиты от НСД.

2.3.6. Оставлять без личного присмотра на АРМ или где бы то ни было свои персональные реквизиты доступа, машинные носители и распечатки, содержащие защищаемую информацию.

2.3.7. Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к ознакомлению с защищаемой информацией посторонних лиц. Об обнаружении такого рода ошибок ставить в известность администратора безопасности.

2.3.8. Производить перемещения технических средств АРМ без согласования с администратором безопасности.

2.3.9. Вскрывать корпуса технических средств АРМ и вносить изменения в схему и конструкцию устройств, производить техническое обслуживание (ремонт) средств вычислительной техники без согласования с администратором безопасности и без оформления соответствующего Акта.

2.3.10. Подключать к АРМ нештатные устройства и самостоятельно вносить изменения в состав и конфигурацию.

2.3.11. Осуществлять ввод пароля в присутствии посторонних лиц.

2.3.12. Оставлять без контроля АРМ в процессе обработки конфиденциальной информации.

2.3.13. Привлекать посторонних лиц для производства ремонта (технического обслуживания) технических средств АРМ.

Приложение N 2
к приказу
ОГБУСО КЦСО «Исток»
от 3 июня 2025 г. N 97п

Должностная инструкция, ответственного за обеспечение безопасности персональных данных в Областном государственном бюджетного учреждении социального обслуживания «Комплексный центр социального обслуживания «Исток»

1. Общие положения

1.1. Настоящая Должностная инструкция ответственного за обеспечение безопасности персональных данных в Областном государственном бюджетном учреждении социального обслуживания «Комплексный центр социального обслуживания «Исток» (далее – Инструкция) определяет обязанности лица, ответственным за обеспечениебезопасности обработки персональных данных (далее – ПДн и ответственный за ПДн), обрабатываемой в информационных системах ПДн (далее - ИСПДн) и на материальных носителях в Областном государственном бюджетном учреждении социального обслуживания «Комплексный центр социального обслуживания «Исток» (далее - ОГБУСО КЦСО «Исток»).

1.2. Ответственный за ПДн назначается приказом генерального директора из числа подготовленных специалистов ОГБУСО КЦСО «Исток».

1.3. Ответственный за ПДн подчиняется директору ОГБУСО КЦСО «Исток».

1.4. Ответственный за ПДн отвечает за поддержание установленного уровня безопасности ПДн при их обработке и хранении в ОГБУСО КЦСО «Исток».

1.5. Ответственный за ПДн осуществляет методическое руководство деятельностью сотрудников ОГБУСО КЦСО «Исток», имеющих доступ к ПДн в вопросах обеспечения безопасности информации.

1.6. Требования ответственного за ПДн, связанные с выполнением им своих обязанностей, обязательны для исполнения всеми сотрудниками ОГБУСО КЦСО «Исток», имеющими доступ к ПДн.

1.7. Ответственный за ПДн несет персональную ответственность за качество проводимых им работ по контролю действий сотрудников ОГБУСО КЦСО «Исток», имеющих доступ к ПДн.

2. Задачи ответственного за обеспечение безопасности ПДн

2.1. Основными задачами ответственного за ПДн являются:

- поддержание необходимого уровня защиты ИСПДн ОГБУСО КЦСО «Исток» от несанкционированного доступа (НСД) к информации;

- обеспечение и поддержание необходимого уровня защиты ПДн на материальных носителях;
- обеспечение конфиденциальности обрабатываемой, хранимой и передаваемой информации;
- оперативное реагирование на нарушения требований по ИБ в ИСПДн ОГБУСО КЦСО «Исток» и участие в их прекращении.

2.2. В рамках выполнения основных задач ответственный за ПДн осуществляет:
- текущий контроль процесса обработки ПДн;
- участие в проведении служебных расследований фактов нарушений или угрозы нарушений безопасности ПДн;
- контроль соблюдения нормативных требований по защите информации, обеспечения комплексного использования технических средств,
методов и организационных мероприятий по безопасности информации в ОГБУСО КЦСО «Исток»;
- методическую помощь сотрудников ОГБУСО КЦСО «Исток».

3. Обязанности ответственного за обеспечение безопасности ПДн

Ответственный за ПДн обязан:

3.1. Знать и выполнять требования нормативных документов по защите информации, регламентирующих порядок защиты информации, обрабатываемой в ОГБУСО КЦСО «Исток».

3.2. Организовывать и принимать участие в мероприятиях по контролю обеспечения безопасности ПДн ОГБУСО КЦСО «Исток».

3.3. Обеспечить доступ к защищаемой информации пользователям ОГБУСО КЦСО «Исток», согласно их правам доступа.

3.4. Уточнять в установленном порядке обязанности Университета при обработке ПДн.

3.5. Вести контроль осуществления резервного копирования информации.

3.6. Анализировать состояние защиты ПДн ОГБУСО КЦСО «Исток».

3.7. Контролировать правильность функционирования средств защиты и хранения информации.

3.8. Контролировать физическую сохранность и безопасность технических средств и материальных носителей обработки информации.

3.9. Контролировать исполнение сотрудниками ОГБУСО КЦСО «Исток», имеющими доступ к ПДн введенного режима безопасности, а также правильность работы с элементами ИСПДн и средствами защиты информации.

3.10. Контролировать исполнение пользователями правил парольной политики.

3.11.Вести и периодически анализировать журнал учета событий, регистрируемых средствами защиты, с целью контроля действий пользователей и выявления возможных нарушений.

3.12.Осуществлять периодические контрольные проверки автоматизированных рабочих мест (АРМ) ОГБУСО КЦСО «Исток».

3.13.Принимать участие в проведении работ по оценке соответствия законодательству порядок обработки и хранения ПДн в ОГБУСО КЦСО «Исток».

3.14.Оказывать помощь сотрудника ОГБУСО КЦСО «Исток» по вопросам веденного режима защиты.

3.15.В случае отказа работоспособности технических средств, программного обеспечения, а также нарушению иных условий обеспечения безопасности ПДн, принимать меры по их своевременному восстановлению и выявлению причин, приведших к нарушениям.

3.16.В случае выявления нарушений режима безопасности ПДн, а также возникновения внештатных и аварийных ситуаций принимать необходимые меры с целью ликвидации их последствий.

4. Права ответственного за обеспечение безопасности ПДн

Ответственный за ПДн имеет право:

4.1. Осуществлять контроль информационных потоков ПДн ОГБУСО КЦСО «Исток» при работе с ИСПДн, корпоративной электронной почтой, съемными носителями информации, материальными носителями.

4.2. Давать сотрудникам обязательные для исполнения указания и рекомендации по вопросам ИБ.

4.3. Инициировать проведение служебных расследований по фактам нарушений установленных требований обеспечения ИБ, НСД, утраты, порчи защищаемой информации и технических средств ИСПДн ОГБУСО КЦСО «Исток».

4.4. Организовывать и участвовать в любых проверках по использованию пользователями ОГБУСО КЦСО «Исток» ПДн.

4.5. Вносить на рассмотрение руководства предложения по улучшению состояния ИБ ПДн, обрабатываемых в ОГБУСО КЦСО «Исток».

4.6. Осуществлять взаимодействие с руководством и сотрудниками ОГБУСО КЦСО «Исток» по вопросам обеспечения безопасности ПДн.

4.7. Запрещать устанавливать на серверах и автоматизированных рабочих местах нештатное программное и аппаратное обеспечение, а также копирование материальных источников ПДн.

4.8. Запрашивать и получать у сотрудников ОГБУСО КЦСО «Исток» информацию и материалы, необходимые для организации своей работы.

5. Действия ответственного за обеспечение безопасности ПДн при обнаружение НСД

5.1. К попыткам НСД относятся:

- сеансы работы с информационными ресурсами незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, либо срок действия

полномочий которых истек, либо в состав полномочий которых не входят операции доступа к определенным данным или манипулирования ими;- действия третьего лица, пытающегося получить доступ (или получившего доступ) к информационным ресурсам ОГБУСО КЦСО «Исток» с использованием учетной записи администратора или другого пользователя в целях получения коммерческой или другой личной выгоды, методом подбора пароля или другого метода (случайного разглашения пароля и т.п.) без ведома владельца учетной записи;
- доступ сотрудников ОГБУСО КЦСО «Исток» или третьих лиц к материальным носителям, содержащие ПДн, а также копирование таких носителей полностью или частично.

5.2. При выявлении факта/попытки НСД ответственный за ПДн обязан:

- прекратить доступ к информационным ресурсам со стороны выявленного участка НСД;
- доложить генеральному директору соответствующего о факте НСД, его результате (успешный, неуспешный) и предпринятых действиях;
- проанализировать характер НСД;
- по решению директора осуществить действия по выяснению причин, приведших к НСД;
- предпринять меры по предотвращению подобных инцидентов в дальнейшем.

6. Ответственность ответственного за обеспечение безопасности ПДн

6.1. Ответственный за ПДн несет ответственность, предусмотренную законодательством:

6.1.1. За организацию защиты информационных ресурсов, технических средств и материальных носителей, содержащих ПДн в ОГБУСО КЦСО «Исток».

6.1.2. За качество проводимых работ по контролю действий сотрудников, имеющих доступ к ПДн, состояние и поддержание необходимого уровня защиты информационных и технических ресурсов ПДн ответственного за обеспечение безопасности ПДн.

6.1.3. За разглашение сведений ограниченного доступа (коммерческая тайна, персональные данные и иная защищаемая информация), ставших известными ему в связи с осуществлением обязанностей ответственного за ПДн.

Приложение N 3
к приказу
ОГБУСО КЦСО «Исток»
от 3 июня 2025 г. N 97н

ИНСТРУКЦИЯ

по учету лиц, допущенных к работе с персональными данными в информационных системах персональных данных в Областном государственном бюджетного учреждении социального обслуживания «Комплексный центр социального обслуживания «Исток»

1. Настоящая инструкция определяет порядок учета лиц, допущенных к работе с персональными данными в информационных системах персональных данных в ОГБУСО КЦСО «Исток» (далее - ИСПДн).

2. Порядок допуска работника к работе с персональными данными:
утверждение распоряжением о допуске к обработке персональных данных перечня должностей, доступ которых к персональным данным, обрабатываемым в ИСПДн, необходим для выполнения договорных (трудовых) обязанностей (далее - Перечень);

прохождение первичного инструктажа, включающего ознакомление со всеми нормативными документами, регламентирующими работу с персональными данными, согласно Инструкции по проведению инструктажа лиц, допущенных к работе с персональными данными с внесением соответствующей информации в Журнал учёта прохождения первичного инструктажа сотрудниками, допущенными к работе с персональными данными в ИСПДН; внесение записи в Журнал учёта лиц, допущенных к работе с персональными данными в информационных системах.

3. В журнале указываются сведения о проведении инструктажа пользователей информационных систем персональных данных правилам работы с системой защиты персональных данных.

4. Основанием для допуска сотрудников к персональным данным является «Список лиц, доступ которых к персональным данным необходим для выполнения трудовых (договорных) обязанностей», утверждаемый генеральным директором.

5. Основанием для прекращения допуска сотрудников к персональным данным является

исключение сотрудников из перечня лиц , допущенных к персональным данным.

6. Журнал ведется администратором безопасности.

7. Форма ведения журнала определена в приложении к Инструкции.

Приложение N 4
к приказу
ОГБУСО КЦСО «Исток»
от 3 июня 2025 г. N 97/2

Инструкция по проведению инструктажа лиц, допущенных к работе с информационными системами персональных данных в Областном государственном бюджетного учреждении социального обслуживания «Комплексный центр социального обслуживания «Исток»

1. Настоящая инструкция разработана с целью обеспечения безопасности персональных данных, обрабатываемых в информационных системах персональных данных ОГБУСО КЦСО «Исток» (далее – ИСПДн).

2. При поступлении на работу сотрудника, которому для выполнения своих трудовых (договорных) обязанностей необходим доступ к ИСПДн (далее – новый сотрудник), ответственный за организацию обработки персональных данных:

а) в соответствии с п.6 ч.1 ст.18.1 Федерального закона от 27.07.2006 N 152- ФЗ «О проводит ознакомление нового сотрудника с положениями законодательства Российской Федерации о персональных данных и локальными актами обработки персональных данных, перечисленными в Приложении к данной инструкции;

б) знакомит нового сотрудника с ответственностью за неисполнение требований по сохранению персональных данных в ИСПДн, предусмотренной действующим законодательством Российской Федерации;

в) отмечает в Журнале учета прохождения первичного инструктажа данные о проведении инструктажа.

3. Новый сотрудник может приступить к исполнению своих непосредственных трудовых (договорных) обязанностей, связанных с обработкой персональных данных, только после успешного прохождения первичного инструктажа.

Приложение к Инструкции по проведению инструктажа лиц,
допущенных к работе с информационными
системами персональных данных
от 3 июня 2025 г.

Перечень законодательных актов Российской Федерации о персональных данных, документов, определяющих требования к защите персональных данных, внутренних локальных актов, определяющих политику организации в отношении обработки персональных данных, с которыми необходимо ознакомить нового сотрудника при проведении первичного инструктажа

Законодательные акты Российской Федерации о персональных данных:

1) Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (ред. от 21.07.2014).

2) Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их информационных системах персональных данных».

3) Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой использования средств автоматизации» (для сотрудников, обрабатывающих персональные данные, в том числе без использования средств автоматизации).

Внутренние локальные акты ОГБУСО КЦСО «Исток»

1) Приказ о назначении ответственного лица за организацию обработки персональных данных.

2) Политика в отношении обработки персональных данных.

3) Положение об обработке и защите персональных данных.

4) Положение о порядке доступа в помещения, в которых ведётся обработка персональных данных.

5) Должностная инструкция, ответственного за обеспечение безопасности персональных данных.

6) Должностная инструкция ответственного за организацию обработки персональных данных.

7) Инструкцию пользователя информационных систем персональных данных.

8) Инструкция по проведению инструктажа лиц, допущенных к работе с информационными системами персональных данных.

9) Инструкция по работе с информационными ресурсами информационно-коммуникационной сети «Интернет».

10) Инструкция по порядку учета, хранения и уничтожения персональных данных на машинных носителях.

11) Инструкция по порядку учета, хранения и уничтожения персональных данных, хранящихся на бумажных носителях.

12) Инструкция по организации антивирусной защиты информационных систем персональных данных.

13) Инструкция по организации парольной защиты информационных систем персональных данных.

14) Инструкция по организации резервного копирования и восстановления данных в информационных системах персональных данных.

15) Инструкция пользователя при возникновении нештатной ситуации (инцидентах информационной безопасности).

16) Инструкция по учету лиц, допущенных к работе с персональными данными в информационных системах персональных данных

17) Инструкция по учету машинных носителей и мобильных технических средств, предназначенных для работы с персональными данными.

18) Правила обработки персональных данных.

19) Правила рассмотрения запросов субъектов персональных данных или их представителей

20) Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами.

21) Правила работы с обезличенными данными в случае обезличивания персональных данных.

22) Перечень персональных данных, обрабатываемых в ОГБУСО КЦСО «Исток» в связи с реализацией договорных (трудовых) отношений, а также в связи с оказанием услуг.

23) Перечень должностей в ОГБУСО КЦСО «Исток», ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, в случае обезличивания персональных данных.

24) Перечень должностей в ОГБУСО КЦСО «Исток», замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным.

25) Типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные.

26) Типовое обязательство сотрудника, непосредственно осуществляющего обработку персональных данных о неразглашении информации, содержащей персональные данные.

27) Перечень информационных систем персональных данных, используемых в ОГБУСО КЦСО «Исток».

28) Правила обработки без использования средств автоматизации.

Приложение N 5
к приказу
ОГБУСО КЦСО «Исток»
от 3 июня 2025 г. N 97-п

Инструкция по работе с информационными ресурсами информационно-коммуникационной сети «Интернет» в Областном государственном бюджетного учреждении социального обслуживания «Комплексный центр социального обслуживания «Исток»

1. Общие положения

1.1. Настоящая инструкция предназначена для пользователей информационных систем персональных данных ОГБУСО КЦСО «Исток», доступ к сети Интернет которым необходим для исполнения договорных (трудовых) обязанностей.

1.2. Работа в сети Интернет для неавторизованных пользователей запрещена.

1.3. Устанавливаются ограничения на получение информации из сети Интернет в соответствии с настройками прокси-сервера. Доступ к социальным сетям, видеохостингам и прочим ресурсам развлекательного характера запрещен.

1.4. Контроль за соблюдением настоящей инструкции возлагается на регионального управляющего.

2. Правила работы в сети Интернет

2.1. При работе в сети Интернет запрещается:

обход учетных систем получаемого трафика, их повреждение или дезинформация;

преднамеренная рассылка вирусов посредством сети Интернет;

предоставление служебной информации для общего доступа;

предоставление информации, касающейся устройства и архитектуры локальной вычислительной сети (далее - ЛВС), в том числе схемы ЛВС и ее сегментов, точек подключения, информации о назначенных рабочим станциям IP-адресах и именах, используемых на серверах, средствах удаленного доступа и т.п.;

предоставление информации о других сотрудниках (клиентов) без их личного согласия;

распространение посредством сети Интернет информации, запрещенной законодательством Российской Федерации или не соответствующей общепринятым морально-этическим нормам, а также рассылка обманных, беспокоящих или угрожающих сообщений и рассылка незапрашиваемых сообщений (спама) за исключением служебных сообщений от администрации;

использование сети Интернет в коммерческих целях;

установка и/или удаление программного обеспечения без согласования с администратором.

Приложение N 6
к приказу
ОГБУСО КЦСО «Исток»
от 3 июня 2025 г. N 97п

Инструкция по порядку учета, хранения и уничтожения персональных данных на машинных носителях в Областном государственном бюджетного учреждении социального обслуживания «Комплексный центр социального обслуживания «Исток»

1. Общие положения

1.1. Настоящая инструкция предназначена для пользователей информационных систем персональных данных (далее - ИСПДн) в ОГБУСО КЦСО «Исток», осуществляющих использование машинных носителей персональных данных (далее - ПДн), а также администратора информационной безопасности (далее - администратор).

1.2. Под использованием носителей информации в ИСПДн понимается их подключение к инфраструктуре ИСПДн в целях обработки, приема/передачи информации между ИСПДн и носителями информации.

1.3. Ответственность за поддержание установленного в настоящей инструкции порядка использования машинных носителей ПДн возлагается на администратора.

1.4. В ИСПДн допускается использование только учтенных носителей информации, которые являются собственностью ОГБУСО КЦСО «Исток» и подвергаются регулярной ревизии и контролю.

1.5. К машинным носителям ПДн предъявляются требования информационной безопасности, что и для стационарных автоматизированных рабочих мест (целесообразность дополнительных мер обеспечения информационной безопасности определяется администратором).

1.6. Пользователи ИСПДн, нарушившие требования настоящей инструкции, несут ответственность в соответствии с законодательством Российской Федерации.

2. Порядок использования машинных носителей ПДн

2.1. Машинные носители ПДн предоставляются сотрудникам ОГБУСО КЦСО «Исток» по инициативе администратора в случаях:

необходимости выполнения вновь принятым сотрудником своих должностных обязанностей;

возникновения у сотрудника производственной необходимости.

2.2. Порядок учета, хранения и обращения с машинными носителями ПДн:

все находящиеся на хранении и в обращении машинные носители ПДн подлежат учету администратором в Журнале учета технических средств, участвующих в обработке

персональных данных в ОГБУСО КЦСО «Исток» согласно приложению №1 к настоящей Инструкции, Журнале учета и выдачи машинных носителей персональных данных в ОГБУСО КЦСО «Исток» согласно Приложению №2 к настоящей Инструкции (далее - Журнал);

каждый машинный носитель ПДн должен иметь этикетку, на которой указывается его уникальный учетный номер;

сотрудники получают учтенный машинный носитель ПДн от администратора. При выдаче делаются соответствующие записи в Журнале;

по окончании работ пользователь сдает машинный носитель ПДн для хранения администратору, о чем делается соответствующая запись в Журнале.

2.3. При использовании пользователями ИСПДн машинных носителей ПДн необходимо:

соблюдать требования настоящей инструкции;

использовать машинные носители ПДн исключительно для выполнения своих служебных обязанностей;

информировать администратора о любых фактах нарушения требований настоящей инструкции;

бережно относиться к машинным носителям ПДн;

хранить машинные носители ПДн в сейфе (шкафу, ящике) в условиях, исключающих бесконтрольный доступ к ним;

информировать администратора о фактах утраты (кражи) машинных носителей ПДн.

2.4. При использовании машинных носителей ПДн запрещено:

использовать машинные носители ПДн в личных целях;

передавать машинные носители ПДн другим лицам (за исключением администратора);

хранить машинные носители ПДн вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра;

выносить машинные носители ПДн за пределы контролируемой зоны.

2.5. Любое взаимодействие (обработка, прием/передача информации), инициированное пользователем между ИСПДн и неучтенными (личными) носителями информации, рассматривается как несанкционированное (за исключением случаев, согласованных с администратором). Администратор имеет право ограничивать использование носителей информации.

2.6. Информация об использовании сотрудником носителей информации в ИСПДн протоколируется и, при необходимости, может быть предоставлена администратором ответственному за организацию обработки ПДн.

2.7. В случае выявления фактов несанкционированного и/или нецелевого использования носителей информации инициируется служебная проверка, проводимая комиссией, состав которой определяется ответственным за организацию обработки ПДн.

2.8. По факту выясненных обстоятельств составляется акт расследования инцидента и передается ответственному за организацию обработки ПДн для принятия мер согласно правовым актам ОГБУСО КЦСО «Исток» и законодательству Российской Федерации.

2.9. Информация, хранящаяся на машинных носителях ПДн, подлежит обязательной проверке на отсутствие вредоносного программного обеспечения.

2.10. При отправке или передаче ПДн адресатам на съемные машинные носители ПДн записываются только предназначенные адресатам данные. Отправка ПДн адресатам на съемных машинных носителях ПДн осуществляется в порядке, установленном для документов для служебного пользования.

2.11. Вынос съемных машинных носителей ПДн для непосредственной передачи адресату осуществляется только с письменного разрешения администратора.

2.12. В случае утраты или уничтожения машинных носителей ПДн либо разглашения содержащихся в них сведений немедленно ставится в известность администратор. На утраченные машинные носители ПДн составляется акт. Соответствующие отметки вносятся в Журнал.

2.13. Машинные носители ПДн, пришедшие в негодность или отслужившие установленный срок, подлежат уничтожению. Уничтожение машинных носителей ПДн осуществляется уполномоченной комиссией. По результатам уничтожения машинных носителей ПДн составляется акт уничтожения ПДн.

2.14. В случае увольнения (прекращения договорных отношений), предоставленные машинные носители ПДн изымаются администратором.

Приложение №1
к Инструкции по порядку учета, хранения и уничтожения
персональных данных на машинных носителях в
ОГБУСО КЦСО «Исток»
от 3 июня 2025 г.

Журнал
учета технических средств, участвующих в обработке
персональных данных в ОГБУСО КЦСО «Исток»

Дата начала ведения: «__»_____ ____ г.

Дата окончания ведения: «__»_____ ____ г.

N п/п	Инвентарный номер	Имя компьютера	Ф.И.О. пользователя	Размещение	Примечание
1	2	3	4	5	6

Приложение №2
к Инструкции по порядку учета, хранения и уничтожения
персональных данных на машинных носителях в
ОГБУСО КЦСО «Исток»
от 3 июня 2025 г.

Журнал
учета и выдачи машинных носителей персональных данных в ОГБУСО КЦСО «Исток»

Дата начала ведения: «__»_____ ____ г.

Дата окончания ведения: «__»_____ ____ г.

N п/п	Наименование машинного носителя и его идентификационный номер	Дата приобретения и номер подтверждающего документа	Дата ввода в эксплуатацию и номер приказа о вводе в эксплуатацию	Дата вывода из эксплуатации с указанием причины вывода и номером соответствующего приказа (акта) <1>	Примечания

Лицо, ответственное за ведение журнала:
_____/_____/
(подпись) (Ф.И.О.)

Приложение N 7
к приказу
ОГБУСО КЦСО «Исток»
от 3 июня 2025 г. N 97/2

Инструкция по порядку учета, хранения и уничтожения персональных данных, хранящихся на бумажных носителях в Областном государственном бюджетного учреждении социального обслуживания «Комплексный центр социального обслуживания «Исток»

1. Общие положения

1.1. Настоящая инструкция предназначена для сотрудников, осуществляющих обработку персональных данных на бумажных носителях (далее - ПДн).

1.2. В ОГБУСО КЦСО «Исток» должны быть разработаны и утверждены следующие перечни:

- перечень сведений, составляющих персональные данные сотрудников, обрабатываемых в связи с реализацией трудовых (договорных) отношений; перечень сведений, составляющих персональные данные, обрабатываемых в связи с оказанием коммерческих (договорных) услуг;
- перечень информационных систем персональных данных ОГБУСО КЦСО «Исток»

1.3. Сотрудники, нарушившие требования настоящей инструкции, несут ответственность в соответствии с законодательством Российской Федерации.

2. Хранение и уничтожение персональных данных

2.1. ПДн на бумажном носителе хранятся в папках в сейфе или в металлическом шкафу в условиях, исключающих бесконтрольный доступ к ним.

2.2. Сотрудник, имеющий доступ к персональным данным субъектов ПДн, в связи с исполнением трудовых (договорных) обязанностей обеспечивает хранение информации, содержащей персональные данные субъекта, исключающее доступ к ним третьих лиц.

2.3. В отсутствие сотрудника на его рабочем месте не должно быть документов, содержащих персональные данные субъектов ПДн.

2.4. При уходе в отпуск и иных случаях длительного отсутствия сотрудника на своем рабочем месте, он обязан передать документы и иные носители, содержащие персональные данные субъектов ПДн администратору информационной безопасности.

2.5. При увольнении сотрудника, имеющего доступ к персональным данным субъектов ПДн, содержащие персональные данные субъектов ПДн, по указанию администратора информационной безопасности передаются другому сотруднику, имеющему доступ к персональным данным субъектов ПДн.

2.6. Повседневный контроль за выполнением требований по защите хранилищ ПДн осуществляет региональным управляющим.

2.10. Контроль эффективности мер защиты хранилищ ПДн осуществляется региональным управляющим.

2.11. Уничтожение персональных данных субъектов ПДн на бумажном носителе, а также содержащихся в ИСПДн в электронном виде, осуществляется комиссией, назначенной приказом генерального директора, на основании Акта об уничтожении персональных данных, обрабатываемых в ОГБУСО КЦСО «Исток», согласно приложению к настоящей Инструкции.

Приложение
к Инструкции по порядку учета, хранения и
уничтожения персональных данных, хранящихся
на бумажных носителях в ОГБУСО КЦСО «Исток»
от 3 июня 2025 г.

АКТ N _____
об уничтожении персональных данных, обрабатываемых в ОГБУСО КЦСО «Исток»

Комиссия в составе:

	ФИО	Должность
Председатель		
Члены комиссии		

составила настоящий Акт о том, что информация, зафиксированная на перечисленных в нем носителях информации (электронных, бумажных), подлежат уничтожению.

Учетный номер материального носителя, номер дела и т.д.	Причина уничтожения носителя информации; стирания/обезличивания информации	Тип носителя информации	Производимая операция (стирание, уничтожение, обезличивание)	Дата
1	2	3	4	5

Всего подлежит уничтожению _____ носителей.
(цифрами и прописью)

Правильность произведенных записей в акте проверена.

Регистрационные данные на носителях информации перед уничтожением (стиранием с них информации) с записями в акте сверены, произведено уничтожение путем: _____.
(стирания на устройстве гарантированного уничтожения информации, разрезания, сжигания, механического уничтожения, вымарывания и т.п.)

Отметки о стирании информации (уничтожении носителей информации) в учетных формах произведены.

Председатель комиссии: _____ / /

Члены комиссии: _____ /

Приложение N 8
к приказу
ОГБУСО КЦСО «Исток»
от 3 июня 2025 г. N 97/1

Инструкция по организации антивирусной защиты информационных систем персональных данных в Областном государственном бюджетного учреждении социального обслуживания «Комплексный центр социального обслуживания «Исток»

1. Введение

1.1. Настоящая инструкция предназначена для пользователей, хранящих и обрабатывающих информацию (персональные данные субъектов персональных данных (далее - ПДн), коммерческая информация о деятельности организации) в информационных системах персональных данных ОГБУСО КЦСО «Исток» (далее - ИСПДн).

1.2. В целях выполнения требований ФСТЭК России и ФСБ России по защите информации в ИСПДн производится антивирусный контроль.

1.3. Ответственность за поддержание установленного в настоящей инструкции порядка проведения антивирусного контроля возлагается на администратора.

1.4. К применению на программно-аппаратных средствах ИСПДн допускаются только лицензионные и сертифицированные по требованиям ФСТЭК России или ФСБ России антивирусные средства для защиты информации, не содержащей сведений, составляющих государственную тайну.

1.5. Установка средств антивирусного контроля на компьютерах, серверах и рабочих станциях ИСПДн осуществляется уполномоченными сотрудниками в соответствии с Инструкцией по модификации технических и программных средств информационных систем персональных данных Федеральной службы по аккредитации.

1.6. Настройка параметров средств антивирусного контроля осуществляется уполномоченными сотрудниками в соответствии с руководствами по применению конкретных антивирусных средств.

2. Общие положения

2.1. На программно-аппаратные средства ИСПДн запрещается установка программного обеспечения (далее - ПО), не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации, в том числе средств разработки и отладки программ.

2.2. Перед началом работы со съемными носителями информации должна проводиться их проверка на предмет отсутствия вредоносного ПО.

2.3. Администратор организует и контролирует регулярное обновление антивирусных баз (по мере выхода соответствующих обновлений, не реже одного раза в месяц).

2.4. Администратор организует и контролирует тестирование установленного программного обеспечения на предмет отсутствия вредоносного ПО.

2.5. В случае необходимости администратор организует и контролирует лечение зараженных файлов и после этого вновь инициирует проведение антивирусного контроля.

2.6. В случае обнаружения на съемном носителе нового вируса, не поддающегося лечению, администратор обязан запретить использование носителя.

2.7. В случае обнаружения на жестких дисках не поддающегося лечению вируса администратор обязан поставить в известность руководителя структурного подразделения, ответственного за обеспечение безопасности персональных данных, запретить работу на программно-аппаратных средствах ИСПДн и инициировать обновление пакета антивирусных программ.

3. Действия при обнаружении вирусов

3.1. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь ИСПДн должен привлечь администратора для проведения внеочередного антивирусного контроля своей рабочей станции с целью определить факт наличия или отсутствия компьютерного вируса.

3.2. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь ИСПДн обязан:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение безопасности ПДн, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования; инициировать лечение или уничтожение зараженных файлов;
- по факту обнаружения зараженных вирусом файлов составить служебную записку в структурное подразделение, ответственное за обеспечение безопасности персональных данных, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

4. Ответственность

4.1. Ответственность за организацию антивирусного контроля в соответствии с требованиями настоящей инструкции возлагается на администратора.

4.2. Ответственность за соблюдение требований настоящей инструкции возлагается на администратора и пользователей ИСПДн в части их касающейся.

Приложение N 9
к приказу
ОГБУСО КЦСО «Исток»
от 3 июня 2025 г. N 97/1

Инструкция по организации парольной защиты информационных систем персональных данных в Областном государственном бюджетного учреждении социального обслуживания «Комплексный центр социального обслуживания «Исток»

1. Общие положения

1.1. Настоящая инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей для информационных систем персональных данных (далее - ИСПДн) ОГБУСО КЦСО «Исток», защищенной от несанкционированного доступа, а также порядок контроля за действиями пользователей ИСПДн при работе с паролями.

1.2. Пользователи ИСПДн должны быть ознакомлены с требованиями настоящей инструкции и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

1.3. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей в ИСПДн, а также контроль за действиями пользователей ИСПДн при работе с паролями возлагается на администратора информационной безопасности (далее - администратор).

1.4. При первом входе в систему пользователь ИСПДн обязан сменить пароль, выданный ему администратором.

1.5. Пользователь ИСПДн имеет право самостоятельно выбрать пароль с учетом требований парольной политики.

1.6. Полная плановая смена паролей пользователей ИСПДн должна производиться один раз в 90 дней.

1.7. В случае возникновения подозрения в компрометации пароль пользователя ИСПДн должен быть немедленно изменен.

1.8. Пользователь ИСПДн не имеет права сообщать личный пароль иным лицам.

2. Парольная политика

2.1. При настройке парольной политики должны быть учтены следующие требования к характеристикам паролей:

минимальная длина пароля - 8 символов;

максимальный срок действия пароля - 90 дней;

в пароле должны использоваться не менее трех типов символов из следующего списка: цифры, символы в верхнем регистре, символы в нижнем регистре, специальные символы;

запрещено использовать имя учетной записи в пароле. Допускается использование не более четырех символов, содержащихся в имени учетной записи, подряд.

2.2. При создании паролей пользователями ИСПДн не рекомендуется:

- использование в составе пароля комбинаций символов, которые можно вычислить, основываясь на информации о пользователе ИСПДн (имя, фамилия, дата рождения, номер автомобиля или телефона и т.д.);

- использование в составе пароля легко вычисляемых сочетаний символов (1234, qwerty, abcd и т.д.);

- использование в составе пароля словарных слов (password, user, computer и т.д.); использование предыдущих паролей.

Приложение N 10
к приказу
ОГБУСО КЦСО «Исток»
от 3 июня 2025 г. N 97/2

Инструкция по организации резервного копирования и восстановления данных в информационных системах персональных данных Областном государственном бюджетного учреждении социального обслуживания «Комплексный центр социального обслуживания «Исток»

1. Общие положения

1.1. Настоящая инструкция разработана в соответствии с требованиями законодательства Российской Федерации в области защиты персональных данных (далее - ПДн) в целях обеспечения возможности незамедлительного восстановления данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

1.2. Целью резервного копирования является предотвращение потери информации при сбоях оборудования, программного обеспечения, в критических ситуациях и т.д.

1.3. Инструкция определяет правила и объемы резервирования, а также порядок восстановления работоспособности информационных систем персональных данных Федеральной службы по аккредитации (далее - ИСПДн).

1.4. Данная инструкция предназначена для администратора информационной безопасности (далее - администратор), а также сотрудников ОГБУСО КЦСО «Исток», участвующих в обработке ПДн (далее - пользователи).

1.5. Носители информации, используемые для резервирования конфиденциальной информации ОГБУСО КЦСО «Исток», в том числе персональных данных, подлежат защите в той же степени, что и резервируемая конфиденциальная информация.

1.6. Ответственным сотрудником за организацию резервного копирования и восстановления данных назначается администратор, осуществляющий контроль за исполнением настоящей инструкции.

2. Информационные ресурсы, подлежащие резервированию

2.1. Резервному копированию подлежат все информационные ресурсы ОГБУСО КЦСО «Исток», содержащие ПДн субъектов, а именно:

файлы, содержащиеся в базах данных (далее - БД);

электронные документы;

файлы сообщений электронной почты;

отсканированные и хранящиеся в ИСПДн изображения документов.

2.2. Резервному копированию могут также подвергаться:

системное и прикладное программное обеспечение;

средства защиты информации.

3. Порядок резервирования

3.1. Резервирование информационных ресурсов ИСПДн, содержащих ПДн (далее - резервирование), организуется администратором.

3.2. Определяется 2 вида резервирования ПДн:

полное резервирование - резервное копирование всех данных, хранящихся в БД;

неполное резервирование - резервное копирование части данных, хранящихся в БД.

3.3. Целью неполного резервирования является сохранение изменений в ИСПДн с момента полного резервирования.

3.4. Периодичность проведения работ по полному резервированию - не менее одного раза в месяц.

3.5. Периодичность проведения работ по неполному резервированию - не менее одного раза в сутки.

3.6. Резервное копирование с использованием незащищенных каналов связи общего пользования не допустимо.

3.7. Резервное копирование по локальной сети на устройство, находящееся вне ИСПДн, не допустимо.

3.8. В случае удаления ПДн субъекта из ИСПДн должна быть так же удалена резервная копия этих данных.

4. Порядок восстановления информации после сбоя

4.1. В случае сбоя в работе ИСПДн восстановление ПДн из резервных копий организует администратор.

4.2. Администратор обязан срочно уведомить генерального директора о факте сбоя в работе ИСПДн, повлекшего нарушение целостности ПДн.

4.3. Временной норматив по восстановлению ПДн устанавливается ответственным за обработку ПДн.

Приложение N 11
к приказу
ОГБУСО КЦСО «Исток»
от 03 июня 2025 г. N 97п

Инструкция пользователя при возникновении нештатной ситуации (инцидентах информационной безопасности) в Областном государственном бюджетного учреждении социального обслуживания «Комплексный центр социального обслуживания «Исток»

1. Общие положения

1.1. Инцидент информационной безопасности - возникновение одного или нескольких нежелательных событий, с которыми связана значительная вероятность реализации угрозы безопасности информации.

1.2. Общий порядок реагирования на нештатные ситуации:

обнаружение и оповещение администратора информационной безопасности о возникновении события;

оперативный сбор информации, связанной с событием, и оценка этой информации с целью определить, относится ли событие к категории инцидентов информационной безопасности;

идентификация инцидента информационной безопасности и его классификация (определение типа инцидента информационной безопасности и его источника), определение уровня потенциального риска (определение возможности и характера ущерба, оценка темпа развития инцидента информационной безопасности);

локализация инцидента информационной безопасности;

проведение расследования (внутреннего или с привлечением правоохранительных органов);

анализ результатов проведенного расследования;

установление вреда, в результате неправомерного или случайного доступа к персональным данным, уничтожения, изменения, блокирования, копирования, представления, распространения персональных данных, а также в результате совершения иных неправомерных действий с ними.

разработка и принятие мер по недопущению инцидентов информационной безопасности в дальнейшем и восстановление системы;

2. Порядок действий в случае возникновения инцидента информационной безопасности

2.1. В ОГБУСО КЦСО «Исток» должен быть предусмотрен список лиц (в том числе, замещающих), ответственных за обеспечение штатного функционирования элементов информационных систем персональных данных (далее - ИСПДн) и безопасности (как физической, так и информационной), с указанием контактной информации.

Данный список разрабатывается, ответственным за обеспечение безопасности персональных данных при их обработке в ИСПДн.

Ответственность за поддержание данного списка в актуальном состоянии возлагается на ответственного за обеспечение безопасности персональных данных.

Ответственность за доведение данного списка до сведения пользователей ИСПДн возлагается на администратора.

2.2. Пользователь ИСПДн при обнаружении нештатной ситуации (события, выходящего за рамки штатного функционирования ИСПДн) должен незамедлительно уведомить администратора. Действия пользователя ИСПДн в случае обнаружения нештатной ситуации могут дополнительно регламентироваться внутренними документами.

2.3. Администратор при поступлении уведомления о возникновении нештатной ситуации осуществляет оперативный сбор информации, и оценку этой информации с целью определить, относится ли событие к категории инцидентов информационной безопасности.

2.4. **К инцидентам информационной безопасности должны быть отнесены следующие события:**

уничтожение или блокирование данных, технических средств, инфраструктуры и элементов информационной системы вследствие стихийного бедствия, пожара, затопления или техногенных факторов (сбои, отказы программного обеспечения, технических средств, систем обеспечения функционирования информационной системы);

нежелательная сетевая активность (сканирование сети, попытки подбора пароля, взлома системы защиты или воздействия на технические (в том числе, программные) средства);

уничтожение, кража, раскрытие, модификация или блокирование информации, обрабатываемой в ИСПДн, вследствие несанкционированного проникновения в контролируемую зону;

утрата отчуждаемого носителя информации;

уничтожение, модификация, блокирование, раскрытие информации или нарушение работоспособности ИСПДн или ее отдельных элементов вследствие успешно проведенной атаки или воздействия вредоносного программного обеспечения;

уничтожение, модификация, блокирование, раскрытие информации или нарушение работоспособности ИСПДн, совершенные пользователем ИСПДн (или от его имени) с использованием назначенных ему прав в ИСПДн;

нарушение установленных в ОГБУСО КЦСО «Исток» требований по безопасности.

2.5. При отнесении события к категории инцидентов информационной безопасности (за исключением случая, когда инцидентом информационной безопасности является нарушение установленных в ОГБУСО КЦСО «Исток» требований по безопасности) вся имеющаяся информация, касающаяся инцидента информационной безопасности, должна быть сообщена ответственному за обеспечение безопасности персональных данных.

2.6. Ответственный за обеспечение безопасности персональных данных должен оценить уровень потенциального риска (путем определения возможности и характера ущерба, оценки темпа развития инцидента информационной безопасности):

уровень 1 - инцидент информационной безопасности является локальным и может быть разрешен силами ОГБУСО КЦСО «Исток»;

уровень 2 - инцидент информационной безопасности может привести к существенному ущербу субъектам информационных отношений (субъектам персональных данных, обладателям информации, сотрудниками, ОГБУСО КЦСО «Исток») и может быть разрешен силами ОГБУСО КЦСО «Исток» лишь частично;

уровень 3 - последствия инцидента информационной безопасности являются критическими, и он не может быть разрешен силами ОГБУСО КЦСО «Исток»

2.7. В случае отнесения инцидента информационной безопасности к уровню 2 или уровню 3 ответственный за обеспечение безопасности персональных данных определяет круг лиц, которые должны быть привлечены к участию в реагировании на инцидент информационной безопасности.

2.8. Ответственный за обеспечение безопасности персональных данных (с привлечением при необходимости иных специалистов) осуществляет локализацию инцидента информационной безопасности.

При локализации инцидента информационной безопасности ответственный за обеспечение безопасности персональных данных с учетом оценки реальной ситуации и существующих возможностей под свою ответственность осуществляет выбор стратегии и способа реагирования на инцидент информационной безопасности.

В рамках локализации инцидента информационной безопасности могут быть предприняты реактивные действия (отключение технических средств от внешних сетей или их изоляция; изменение настроек межсетевого экрана, маршрутизаторов, других технических средств; принятие иных экстренных мер) или проактивные действия (наблюдение, предупреждение дальнейшего развития инцидента информационной безопасности).

Допустимость реактивных действий определяется в соответствии с требованиями по обеспечению непрерывности их функционирования с учетом характера инцидента информационной безопасности и уровня потенциального риска в случае непринятия реактивных мер.

2.9. После локализации инцидента информационной безопасности ответственный за обеспечение безопасности персональных данных составляет письменный отчет об инциденте информационной безопасности. На ответственного за обеспечение безопасности персональных данных возлагается ответственность за достоверность сведений, указанных в отчете об инциденте информационной безопасности.

В отчете должны быть зафиксированы:

- дата и время, когда произошел инцидент информационной безопасности;
- перечень лиц (должность, фамилия, имя, отчество), бывших свидетелями события или сообщивших о нем;
- описание инцидента информационной безопасности;
- перечень свидетельств события и место их хранения (при наличии свидетельств);
- последовательность проведенных мероприятий и действий по локализации инцидента информационной безопасности;

- описание ущерба и иных последствий инцидента информационной безопасности, в том числе вероятных;

- выводы о возможных причинах инцидента информационной безопасности.

Данный документ хранится у ответственного за обеспечение безопасности персональных данных.

Ответственный за обеспечение безопасности персональных данных отвечает за обеспечение сохранности информации, относящейся к инциденту информационной безопасности. Указанная информация в дальнейшем может использоваться при проведении компьютерно-технической экспертизы, а также в качестве доказательной базы при судебном разбирательстве.

2.10. Для целей оценки вреда образуется комиссия по вопросам оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных» (далее - комиссия), состоящая из председателя комиссии, секретаря комиссии и членов комиссии. Состав комиссии и регламент деятельности комиссии утверждаются генеральным директором.

Комиссия определяет одну из степеней вреда в соответствии с Требованиями к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона "О персональных данных", утвержденными приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 27.10.2022 N 178 "Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона "О персональных данных", и составляет в соответствии с указанными Требованиями акт оценки вреда, который подписывается секретарем комиссии и утверждается председателем комиссии (далее - акт оценки вреда).

Акт оценки вреда хранится у ответственного за обеспечение безопасности персональных данных.

Приложение N 12
к приказу
ОГБУСО КЦСО «Исток»
от 3 июня 2025 г. N 97-п

Инструкция
по учету машинных носителей и мобильных технических средств, предназначенных для работы с персональными данными в Областном государственном бюджетного учреждении социального обслуживания «Комплексный центр социального обслуживания «Исток»

1. Общие положения

1.1. Настоящая Инструкция устанавливает основной порядок учета машинных носителей и мобильных технических средств, предназначенных для работы с персональными данными в ОГБУСО КЦСО «Исток».

1.2. К мобильным техническим средствам относятся съемные машинные носители информации (флеш-накопители, внешние накопители на жестких дисках и иные устройства), портативные вычислительные устройства и устройства связи с возможностью обработки информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные устройства).

1.3. Настоящая Инструкция разработана в соответствии с действующим законодательством Российской Федерации.

1.4. Настоящая Инструкция обязательна для соблюдения всеми сотрудниками организации.

1.5. Настоящая Инструкция вступает в действие с момента утверждения ее приказом генерального директора и действует до утверждения нового Положения.

1.6. Все изменения и дополнения к настоящей Инструкции должны быть утверждены приказом генерального директора.

2. Порядок учета машинных носителей и мобильных технических средств, предназначенных для работы с персональными данными

2.1. Учету подлежат:

съемные машинные носители информации (флеш-накопители, внешние накопители на жестких дисках и иные устройства);

портативные вычислительные устройства, имеющие встроенные носители информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства);

машинные носители информации, встроенные в корпус средств вычислительной техники (накопители на жестких дисках).

2.2. Все перечисленные в п. 2.1 носители приобретаются организацией для использования сотрудниками в служебных целях.

2.3. Каждый носитель, приобретаемый для организации, регистрируется в Журнале учета носителей информации, получает инвентарный номер, согласно приложению к настоящею Инструкции.

2.4. Ответственный за ведение Журнала – региональный управляющий.

2.5. При выдаче носителя сотруднику организации в Журнале учета делается отметка: кому, когда и в каких целях был выдан носитель, а при возврате - соответственно проставляется дата возврата.

2.6. При использовании машинных носителей персональных данных запрещается:

- хранение машинных носителей с персональными данными вместе с носителями открытой информации на рабочих столах либо оставление их без присмотра или передача на хранение другим лицам;

- вынос машинных носителей с персональными данными из служебных помещений для работы с ними на дому, в гостиницах и т.д.;

- использование для хранения и обработки персональных данных машинных носителей информации, не поставленных на учет в установленном порядке.

2.7. Использование носителя в личных целях не допускается.

2.8. Использование носителя в личных устройствах не допускается.

2.9. Вынос машинного носителя за пределы организации не допускается.

2.10. В случае поломки или утери носителя с сотрудника, которому был выдан носитель, берется объяснительная записка, а также к нему применяются следующие меры взыскания:

в случае потери носителя на территории организации - выговор и компенсация затрат на организацию поиска носителя;

в случае потери носителя за пределами организации – расторжение договора и привлечение к ответственности за нарушение Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных».

2.11. В случае кражи носителей, содержащих персональные данные, организация обязана привлечь правоохранительные органы.

Приложение
к Инструкции по учету машинных носителей и
мобильных технических средств,
предназначенных для работы с персональными данными
в ОГБУСО КЦСО «Исток»
от 3 июня 2025 г.

_____
(наименование организации или Ф.И.О. ИП)

_____
(место нахождения, контактные данные)

Журнал N _____
учета машинных носителей, предназначенных для хранения
и обработки персональных данных

Дата начала ведения журнала: «___»_____ ____ г.

Дата окончания ведения журнала: «___»_____ ____ г.

N п/п	Наименование машинного носителя и его идентификационный номер	Дата приобретения и номер подтверждающего документа	Дата ввода в эксплуатацию и номер приказа о вводе в эксплуатацию	Дата вывода из эксплуатации с указанием причины вывода и номером соответствующего приказа (акта) <1>	Примечания

Информация для сведения:

<1> Если машинный носитель был сломан, его необходимо вывести из эксплуатации по причине сдачи в ремонт, а затем заново ввести в эксплуатацию или утилизировать.