Министерство труда и социальной защиты населения Ставропольского края
Государственное бюджетное учреждение социального обслуживания
«Новоалександровский комплексный центр социального обслуживания населения»

# ПРИКАЗ

22 августа 2017 года г. Новоалександровск № 448

Об утверждении нормативно-правовых актов
в области обработки персональных данных

В соответствии с Федеральными законами № 152-ФЗ от 27.07.2006 года «О персональных данных», № 149-ФЗ от 27.07.2006 года «Об информации, информационных технологиях и о защите информации», постановлениями Правительства Российской Федерации № 1119 от 01.11.2012 года «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», № 687 от 15.09.2008 года «Об утверждении положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», приказом Федеральной службы по техническому и экспортному контролю России № 21 от 18.02.2013 года «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

ПРИКАЗЫВАЮ:

1. Утвердить следующий перечень нормативно-правовых актов:

1.1. Политику в отношении обработки персональных данных в ГБУСО «Новоалександровский КЦСОН» (Приложение № 1)

1.2. Положение об обработке и защите персональных данных работников ГБУСО «Новоалександровский КЦСОН» (Приложение № 2);

1.3. Положение об обработке и защите персональных данных, получателей социальных услуг в ГБУСО «Новоалександровский КЦСОН» (Приложение № 3).

1.4. Инструкцию администратора информационных систем персональных данных по обеспечению безопасности персональных данных в ГБУСО «Новоалександровский КЦСОН» (Приложение №4);

1.5. Инструкцию о порядке резервирования и восстановления работоспособности технических средств, программного обеспечения и баз данных в ГБУСО «Новоалександровский КЦСОН» (Приложение №5);

1.6. Инструкцию ответственного за организацию обработки персональных данных в ГБУСО «Новоалександровский КЦСОН» (Приложение №6);

1.7. Инструкцию по организации антивирусной защиты в ГБУСО «Новоалександровский КЦСОН» (Приложение №7);

1.8. Инструкцию по порядку учета и хранению документов, содержащих персональные данные в ГБУСО «Новоалександровский КЦСОН» (Приложение № 8);

1.9. Инструкцию по обеспечению безопасности эксплуатации средств криптографической защиты информации (СКЗИ) в ГБУСО «Новоалександровский КЦСОН» (Приложение № 9);

1.10. Инструкцию по организации хранения, обработки и передачи служебной информации (в том числе персональных данных) на внешних носителях (устройствах) в автоматизированной информационной системе ГБУСО «Новоалександровский КЦСОН» и за его пределами (Приложение № 10);

1.11. Инструкцию пользователя информационных систем персональных данных по обеспечению безопасности персональных данных в ГБУСО «Новоалександровский КЦСОН» (Приложение № 11);

1.12. Инструкцию по организации парольной защиты (Приложение №12);

1.13. Инструкцию по действиям персонала в нештатных ситуациях (Приложение № 13);

1.14.Порядок доступа сотрудников ГБУСО «Новоалександровский КЦСОН» в помещения, в которых ведётся обработка персональных данных (Приложение № 14);

1.15.Правила работы с обезличенными персональными данными в ГБУСО «Новоалександровский КЦСОН» (Приложение № 15);

1.16.Правила рассмотрения запросов субъектов персональных данных или их представителей на получение информации, касающейся обработки его персональных данных, обращений уполномоченного органа по защите прав субъектов персональных данных в ГБУСО «Новоалександровский КЦСОН» (Приложение № 16);

1.17.Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в ГБУСО «Новоалександровский КЦСОН» (Приложение № 17);

1.18.Разрешительную систему доступа сотрудников к ресурсам информационных систем персональных данных в ГБУСО «Новоалександровский КЦСОН» (Приложение № 18);

1.19.Частную модель угроз персональных данных для информационных систем модель угроз персональных данных для информационных систем «1С «зарплата и кадры»», «1С «Бухгалтерия»», «УРМ АС «Бюджет»», «СБиС ++ «Электронная отчетность и документооборот»», «Учет клиентов ЦСО», «Автоматизированная система «Адресная социальная помощь»» (Приложение №19).

2. Ответственному за организацию обработки персональных данных довести до сведения всех работников, обрабатывающих персональные данные, положения утверждаемых нормативно-правовых актов.

3. Контроль за исполнением настоящего приказа оставляю за собой.

4. Настоящий приказ вступает в силу со дня его подписания.

Директор Государственного бюджетного учреждения социального обслуживания «Новоалександровский комплексный центр социального обслуживания населения» Т.В. Степанова

Исп. Абакумова Т.С.

Приложение № 1
к приказу директора ГБУСО
«Новоалександровский КЦСОН»
от 22 августа 2017 года № 448

**ПОЛИТИКА**
**в отношении обработки персональных данных в ГБУСО «Новоалександровский КЦСОН»**

**1. Общие положения**

1.1. Настоящая Политика в отношении обработки персональных данных (далее по тексту – Политика) в Государственном бюджетном учреждении социального обслуживания «Новоалександровский комплексный центр социального обслуживания населения» (далее по тексту – Учреждение, Оператор) разработана в соответствии со статьей 18.1 Федерального закона от 27.07.2006 года №152-ФЗ «О персональных данных» (далее – Закон №152-ФЗ), а также иных нормативно-правовых актов Российской Федерации в области защиты и обработки персональных данных и действует в отношении всех персональных данных, которые Учреждение может получить от субъекта персональных данных, являющегося стороной по договору оказания социальных услуг (получатель социальных услуг или его законный представитель), гражданско-правовому договору, а так же от субъекта персональных данных, состоящего с Учреждением в отношениях, регулируемых трудовым законодательством (далее – Работника).

1.2. Основные понятия, используемые в настоящей Политике:

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

Информационная система персональных данных (ИСПД) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

**1.3. Основные права субъекта персональных данных.**

Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных Оператором;
- правовые основания и цели обработки персональных данных;
- цели и применяемые Оператором способы обработки персональных данных;
- наименование и место нахождения оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных»;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» или другими федеральными законами.

**1.4. Права и обязанности Оператора**

1.4.1. Оператор вправе:

- отстаивать свои интересы в судебных органах;
- предоставлять персональные данные субъектов третьим лицам, если это предусмотрено действующим законодательством Российской Федерации (правоохранительные, налоговые органы и др.), а также связано с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;
- отказывать в предоставлении персональных данных в случаях предусмотренных законодательством Российской Федерации;
- использовать персональные данные субъекта без его согласия, в случаях предусмотренных законодательством Российской Федерации.

1.4.2. Оператор обязан:

- при сборе персональных данных предоставить информацию об обработке персональных данных;
- в случаях, если персональные данные были получены не от субъекта персональных данных, уведомить субъекта;
- при отказе в предоставлении персональных данных субъекту разъясняются последствия такого отказа;
- опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных;
- принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных а также от иных неправомерных действий в отношении персональных данных;
- давать ответы на запросы и обращения Субъектов персональных данных, их представителей и уполномоченного органа по защите прав субъектов персональных данных.

## 2. Цели сбора персональных данных

2.1. Цели сбора персональных данных в Учреждении:

2.2.1. Осуществление уставной деятельности Учреждения: социальное обслуживание граждан, признанных нуждающимися в социальном обслуживании вследствие существования следующих обстоятельств, которые ухудшают или могут ухудшить условия их жизнедеятельности:

1) полная или частичная утрата способности либо возможности осуществлять самообслуживание, самостоятельно передвигаться, обеспечивать основные жизненные потребности в силу заболевания, травмы, возраста или наличия инвалидности;

2) наличие в семье инвалида или инвалидов, в том числе ребенка-инвалида или детей-инвалвдов, нуждающихся в постоянном постороннем уходе;

3) наличие ребенка или детей (в том числе находящихся под опекой, попечительством), испытывающих трудности в социальной адаптации;

4) отсутствие возможности обеспечения ухода (в том числе временного) за инвалидом, ребенком, детьми, а также отсутствие попечения над ними;

5) наличие внутрисемейного конфликта, в том числе с лицами с наркотической или алкогольной зависимостью, лицами, имеющими пристрастие к азартным играм, лицами, страдающими психическими расстройствами, наличие насилия в семье;

6)отсутствие определенного места жительства;

7)отсутствие работы и средств к существованию;

8) нахождение несовершеннолетнего ребенка в социально опасном положении и (или) в трудной жизненной ситуации.

2.2.2. Ведение кадрового учета работников Учреждения;

2.2.3. Оплата услуг лицам по договорам гражданско-правового характера.

## 3. Правовые основания обработки персональных данных

3.1. Политика обработки персональных данных в Учреждении осуществляется соответствии со следующими нормативными правовыми актами:

- Трудовой кодекс Российской Федерации;
- Гражданский Российской Федерации;
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Указ Президента Российской Федерации от 06 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера»;
- постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- постановление Правительства Российской Федерации от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;

- постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- приказ Роскомнадзора от 05 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;

иные нормативные правовые акты Российской Федерации и нормативные документы уполномоченных органов государственной власти.

3.2. В целях реализации положений Политики в Учреждении разрабатываются соответствующие локальные нормативные акты и иные документы, в том числе:

- Положение об обработке и защите персональных данных работников ГБУСО «Новоалександровский КЦСОН»;

- Положение об обработке и защите персональных данных, получателей социальных услуг в ГБУСО «Новоалександровский КЦСОН»;

- Порядок доступа сотрудников ГБУСО «Новоалександровский КЦСОН» в помещения, в которых ведётся обработка персональных данных;

- Правила рассмотрения запросов субъектов персональных данных или их представителей на получение информации, касающейся обработки его персональных данных, обращений уполномоченного органа по защите прав субъектов персональных данных в ГБУСО «Новоалександровский КЦСОН»;

- иные локальные нормативные акты и документы, регламентирующие в Учреждении вопросы обработки персональных данных.

## 4. Объем и категории обрабатываемых персональных данных, категории субъектов персональных данных

4.1. Категории субъектов персональных данных.

В Учреждении обрабатываются персональные данные следующих субъектов:

- физические лица, признанные нуждающимися в социальном обслуживании;

- лица, состоящие с Учреждением в гражданско-правовых отношениях;

- физические лица, состоящие с Учреждением в трудовых отношениях;

4.2. Перечень обрабатываемых персональных данных:

- перечень персональных данных, обрабатываемых в Учреждении, определяется в соответствии с законодательством Российской Федерации и локальными нормативными актами Учреждения с учетом целей обработки персональных данных, указанных в разделе 2 Политики.

4.3. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни в Учреждении не осуществляется.

## 5. . Порядок и условия обработки персональных данных

5.1. Обработка персональных данных в Учреждении осуществляется на основе следующих принципов:

- на законной и справедливой основе;

- обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей;

- не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

- не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

- обработке подлежат только персональные данные, которые отвечают целям их обработки;

- содержание и объем обрабатываемых персональных данных соответствует заявленным целям обработки. Не допускается избыточность обрабатываемых персональных данных по отношению к заявленным целям их обработки;

- при обработке персональных данных обеспечиваются точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных.

- хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем того требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;

- обрабатываемые персональные данные уничтожаются либо обезличиваются по достижении целей обработки. Уничтожение осуществляется способом, исключающим возможность их восстановления.

5.2. Учреждение при осуществлении обработки персональных данных:

- принимает организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных;

- принимает меры, необходимые и достаточные для обеспечения выполнения требований

законодательства Российской Федерации и локальных нормативных актов Учреждения в области персональных данных;

- издает локальные нормативные акты, определяющие политику и вопросы обработки и защиты персональных данных в Учреждении;

- публикует или иным образом обеспечивает неограниченный доступ к настоящей Политике;

- прекращает обработку и уничтожает персональные данные в случаях, предусмотренных законодательством Российской Федерации в области персональных данных;

- совершает иные действия, предусмотренные законодательством Российской Федерации в области персональных данных.

5.3. Обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных, если иное не предусмотрено законодательством Российской Федерации в области персональных данных.

5.4. Все персональные данные следует получать от самого субъекта. Если персональные данные субъекта можно получить только у третьей стороны, то Субъект должен быть уведомлен об этом или от него должно быть получено согласие.

5.5. Оператор должен сообщить Субъекту о целях, предполагаемых источниках и способах получения персональных данных, характере подлежащих получению персональных данных, перечне действий с персональными данными, сроке, в течение которого действует согласие и порядке его отзыва, а также о последствиях отказа Субъекта дать письменное согласие на их получение.

5.6. Оператор передает персональные данные третьим лицам в следующих случаях:

- субъект выразил свое согласие на такие действия;

- передача предусмотрена Российским или иным применимым законодательством в рамках установленной законодательством процедуры.

5.7. Перечень третьих лиц, которым передаются персональные данные:

- Пенсионный фонд РФ для учета (на законных основаниях);
- Налоговые органы РФ (на законных основаниях);
- Фонд социального страхования (на законных основаниях);
- Территориальный фонд обязательного медицинского страхования (на законных основаниях);
- Банки для начисления заработной платы (на основании договора);
- ГКУ «Центр занятости Новоалександровского района;
- Органы МВД и другие в случаях, установленных законодательством.

5.8. Обработка персональных данных в Учреждении осуществляется следующими способами:

- с использованием средств автоматизации;
- без использования средств автоматизации

Трансграничная передача персональных данных не осуществляется.

5.9. Оператор и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено Федеральными законами Российской Федерации

5.10. Сроки обработки персональных данных субъектов персональных данных определяются в соответствии с действующим законодательством Российской Федерации и иными нормативными правовыми актами.

5.11. Хранение персональных данных.

5.11.1. Персональные данные Субъектов могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде.

5.11.2. Персональные данные, зафиксированные на бумажных носителях хранятся в запираемых шкафах, либо в запираемых помещениях с ограниченным правом доступа.

5.11.3. Персональные данные Субъектов, обрабатываемые с использованием средств автоматизации в разных целях, хранятся в разных папках (вкладках).

5.11.4. Не допускается хранение и размещение документов, содержащих персональные данные, в открытых электронных каталогах (файлообменниках) в ИСПД.

5.11.5. Хранение персональных данных в форме, позволяющей определить субъекта персональных данных, осуществляется не дольше, чем этого требуют цели их обработки и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

5.12. Уничтожение персональных данных.

5.12.1. Уничтожение документов (носителей), содержащих персональные данные производится путем сожжения, дробления (измельчения), химического разложения, превращения в бесформенную массу или порошок. Для уничтожения бумажных документов допускается применение шредера.

5.12.2. Персональные данные на электронных носителях уничтожаются путем стирания или форматирования носителя.

5.12.3. Уничтожение производится комиссией. Факт уничтожения персональных данных подтверждается документально актом об уничтожении носителей, подписанным членами комиссии.

## 6. Заключительные положения

6.1. Контроль исполнения требований настоящей Политики осуществляется ответственным за обеспечение безопасности персональных данных.

6.2. Настоящая Политика является общедоступной и подлежит размещению на официальном сайте Учреждения в течении 10 дней после ее утверждения.

Приложение № 2
к приказу директора ГБУСО
«Новоалександровский КЦСОН»
от 22 августа 2017 года № 448

**ПОЛОЖЕНИЕ**
**об обработке и защите персональных данных работников ГБУСО «Новоалександровский КЦСОН»**

**1. Общие положения**

1.1. Настоящее Положение об обработке и защите персональных данных работников (далее — Положение) ГБУСО «Новоалександровский КЦСОН» (далее - Учреждение) разработано в соответствии с Конституцией Российской Федерации, Федеральным законом от 27.07.2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 года № 152-ФЗ «О персональных данных», иными нормативными актами, действующими на территории Российской Федерации.

1.2. Цель разработки Положения — определение порядка обработки персональных данных в Учреждении, обеспечение защиты прав и свобод работников персональных данных при обработке их персональных данных, а также установление ответственности работников, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.3. Все работники Учреждения, имеющие доступ к персональным данным, должны быть ознакомлены с настоящим Положением под роспись.

1.4. Режим конфиденциальности персональных данных снимается только в случаях их обезличивания.

**2. Основные понятия и состав персональных данных**

2.1. Для целей настоящего Положения используются следующие основные понятия:

– блокирование персональных данных — временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

– документированная информация — зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

– информация — сведения (сообщения, данные) независимо от формы их представления;

– использование персональных данных — действия (операции) с персональными данными, совершаемые работниками в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъектов персональных данных либо иным образом затрагивающих их права и свободы или права и свободы других лиц;

– конфиденциальность персональных данных — обязательное требование для работника, получившего доступ к персональным данным, не допускать их распространения без согласия субъекта персональных данных или иного законного основания;

– обезличивание персональных данных — действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;

– обработка персональных данных — сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение персональных данных;

– общедоступные персональные данные — персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;

– персональные данные — любая информация, относящаяся к определенному или определяемому на основании такой информации субъекту, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы и прочая дополнительная информация;

– работник (сотрудник) - физическое лицо, состоящее в трудовых отношениях или иных договорных отношениях с оператором и являющееся субъектом персональных данных.

– распространение персональных данных — действия, направленные на передачу персональных данных определенному кругу лиц или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

– субъект персональных данных – физическое лицо, которому принадлежат те или иные персональные данные;

– уничтожение персональных данных — действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;

2.2. В состав персональных данных входят сведения, содержащие информацию о паспортных данных, образовании, отношении к воинской обязанности, семейном положении, месте жительства,

состоянии здоровья и другая информация, позволяющая идентифицировать субъекта персональных данных и получить о нём дополнительную информацию.

## 3. Цели обработки персональных данных их состав и сроки обработки

3.1. Обработка персональных данных работников осуществляется в целях обеспечения соблюдения Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации, учета результатов исполнения им должностных обязанностей, ведения кадрового и бухгалтерского учета, и выполнения функций возложенных законодательством Российской Федерации.

3.2. Состав обрабатываемых персональных данных определяется в соответствии с перечнем персональных данных, обрабатываемых в ГБУСО «Новоалександровский КЦСОН» (Приложение № 1 к данному Положению).

3.3. Персональные данные работников обрабатываются до момента увольнения после чего передаются в архив и хранятся в течении 75 лет.

## 4. Сбор, обработка и защита персональных данных

4.1. Порядок получения персональных данных

4.1.1. Доступ к персональным данным разрешен работникам, указанным в перечне должностей сотрудников ГБУСО «Новоалександровский КЦСОН», допущенных к обработке персональных данных, утвержденном директором Учреждения.

4.1.2. Перед допуском к работе с персональными данными, предоставлением персональных данных для выполнения служебных обязанностей с работника необходимо взять письменное обязательство о неразглашении персональных данных (Приложение № 2 к данному Положению).

4.1.3. Все персональные данные следует получать у субъекта персональных данных. Если персональные данные субъекта возможно получить только у третьей стороны, то субъект персональных данных должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работник Учреждения должен сообщить субъекту персональных данных о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа дать письменное согласие на их получение.

4.2. Порядок обработки персональных данных.

4.2.1. Субъект персональных данных предоставляет сотруднику Учреждению достоверные сведения о себе. Сотрудник Учреждения проверяет достоверность сведений, сверяя данные, предоставленные субъектом, с имеющимися у субъекта документами, удостоверяющими личность и иными документами подтверждающие достоверность сведений о субъекте персональных данных.

4.2.2. В соответствии со ст. 6 ФЗ-152 «О Персональных данных» работники Учреждения при обработке персональных данных должны соблюдать следующие общие требования:

4.2.2.1. Обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных. (Приложение № 3 к данному Положению).

4.2.3. Принятие решений, порождающих юридические последствия субъектов персональных данных или иным образом затрагивающих их права и законные интересы, на основании исключительно автоматизированной обработки их персональных данных, осуществляется при условии получения их письменного согласия (Приложение № 4 к настоящему Положению).

4.2.3.1. Обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных.

4.2.3.2. Обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

4.2.3.3. Защита персональных данных от неправомерного их использования или утраты обеспечивается Учреждением за счет средств Учреждения в порядке, установленном законодательством.

4.2.4. Обработка персональных данных в Учреждении осуществляется как с использованием информационных систем персональных данных Учреждения, перечисленных в перечне информационных систем персональных данных, принадлежащих Учреждению, так и без использования средств автоматизации, в соответствии с требованиями, установленными законодательством Российской Федерации.

4.2.5. Уполномоченные лица Учреждения с учетом установленной компетенции сообщают субъекту персональных данных о составе персональных данных, обрабатываемых в Учреждении, и целях их обработки. Разъяснение юридических последствий отказа субъекта персональных данных представить свои персональные данные доводится до сведения субъектов персональных данных (Приложение № 5 к настоящему Положению).

4.2.6. Передача персональных данных субъектов персональных данных третьим лицам, не допускается без письменного согласия субъекта персональных данных на передачу персональных данных третьим лицам, за исключением случаев, установленных законодательством Российской Федерации (Приложение № 6 к настоящему Положению).

4.2.7. Размещение персональных данных субъектов персональных данных в общедоступных источниках персональных данных осуществляется с письменного согласия субъекта персональных данных (Приложение № 7 к настоящему Положению);

4.2.8. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. (Приложение № 8 к настоящему Положению).

## 5. Передача и хранение персональных данных

5.1. При передаче персональных данных необходимо соблюдать следующие требования:

5.1.1. Не сообщать персональные данные субъекта третьей стороне без его письменного согласия, за исключением случаев, установленных федеральным законодательством.

5.1.2. Предупредить лиц, получивших персональные данные субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц письменное подтверждение того, что это правило соблюдено. Лица, получившие персональные данные, обязаны соблюдать режим конфиденциальности. Данное Положение не распространяется на обмен персональными данными субъектов в порядке, установленном федеральными законами.

5.1.3. Осуществлять передачу персональных данных субъектов в пределах Учреждения в соответствии с настоящим Положением и другими внутренними нормативно-правовыми актами по защите информации.

5.1.4. При передаче персональных данных за пределы Учреждения в другие организации в целях выполнения производственных функций заключать договоры с указанием в них о том, что переданные персональные данные могут быть использованы только в целях, для которых они сообщены.

5.1.5. Разрешать доступ к персональным данным субъектов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретной функции.

5.2. Персональные данные субъектов могут обрабатываться и храниться, как на бумажных носителях, так и в электронном виде.

## 6. Уничтожение персональных данных

6.1. Уничтожение документов, содержащих персональные данные, в том числе черновиков, бракованных листов и испорченных копий, должно производиться комиссией.

6.2. Комиссия производит уничтожение персональных данных в следующих случаях:

- по требованию субъекта ПДн, в определенных законом случаях;
- по истечении срока хранения;
- в случае выявления неправомерных действий с персональными данными и невозможности устранения допущенных нарушений;
- в случае достижения цели обработки ПДн;
- в случае утраты необходимости достижения цели обработки.

6.3. Порядок уничтожения документов, черновиков, испорченных листов, неподписанных проектов документов, содержащих персональные данные:

- документы, черновики документов, испорченные листы, варианты и неподписанные проекты документов разрываются таким образом, чтобы было невозможно дальнейшее восстановление информации. В учетных данных документа (карточке, журнале) делается отметка об уничтожении черновика с указанием количества листов и проставлением подписи сотрудника и даты;
- уничтожение документов, содержащих персональные данные, производится в строгом соответствии со сроками хранения.

6.4. Уничтожение персональных данных в электронном виде осуществляется путём удаления информации со всех носителей и резервных копий без возможности дальнейшего восстановления.

6.5. Разрешение на уничтожение персональных данных дает директор Учреждения.

## 7. Доступ к персональным данным

7.1. Доступ работников к персональным данным осуществляется на основании разрешительной системы доступа.

7.2. Копировать и делать выписки персональных данных разрешается исключительно в служебных целях с письменного разрешения директора Учреждения.

7.3. Передача персональных данных третьей стороне возможна только при письменном согласии субъекта персональных данных, либо на основании законодательства Российской Федерации.

7.4. Передача персональных данных третьей стороне в случаях, не предусмотренных законодательством Российской Федерации осуществляется на договорной основе с указанием в договоре о том, что переданные персональные данные могут быть использованы только в целях, для которых они сообщены.

## 8. Правила работы с обезличенными данными

8.1. Обезличиванием персональных данных называются действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных (например, статистические данные).

8.2. Обезличивание персональных данных в Учреждении при обработке персональных данных с использованием средств автоматизации осуществляется с помощью специализированного программного обеспечения на основании нормативно правовых актов, правил, инструкций, руководств, регламентов, инструкций на такое программное обеспечение и иных документов для достижения заранее определенных и заявленных целей.

8.3. Допускается обезличивание персональных данных при обработке персональных данных без использования средств автоматизации - производить способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

8.4. Работа с обезличенными данными осуществляется в порядке установленным законодательством Российской Федерации и внутренними нормативно-правовыми актами, регулирующими работу с персональными данными.

## 9. Порядок внутреннего контроля за соблюдением требований по обработке и обеспечению безопасности данных

9.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в Учреждении организуется проведение периодических проверок условий обработки персональных данных. Проверки осуществляются ответственным за организацию обработки персональных данных в Учреждении либо комиссией, образуемой директором не реже одного раза в 3 года.

9.2. При осуществлении внутреннего контроля соответствия обработки персональных данных установленным требованиям в Учреждении производится проверка:

- соблюдения принципов обработки персональных данных в Учреждении;
- соответствия локальных актов в области персональных данных Учреждения, действующему законодательству Российской Федерации;
- выполнения работниками Учреждения требований и правил (в том числе особых) обработки персональных данных в информационных системах персональных данных Учреждения;
- правильность осуществления сбора, систематизации, сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления, уничтожения персональных данных в каждой информационной системе персональных данных Учреждения;
- актуальность перечня должностей работников Учреждения, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;
- соблюдение прав субъектов персональных данных, чьи персональные данные обрабатываются в информационных системах персональных данных Учреждении;
- соблюдение обязанностей Учреждением, предусмотренных действующим законодательством в области персональных данных;
- порядка взаимодействия с субъектами персональных данных, чьи персональные данные обрабатываются в информационных системах персональных данных Учреждения, в том числе соблюдения сроков предусмотренных действующим законодательством в области персональных данных, соблюдения требований по уведомлениям, порядка разъяснения субъектам персональных данных необходимой информации, порядка реагирования на обращения субъектов персональных данных, порядка действий при достижении целей обработки персональных данных и отзыве согласий субъектами персональных данных;
- наличие необходимых согласий субъектов персональных данных, чьи персональные данные обрабатываются в информационных системах персональных данных Учреждении;
- актуальность сведений, содержащихся в уведомлении Учреждения об обработке персональных данных;
- актуальность перечня информационных систем персональных данных в Учреждении;
- наличие и актуальность сведений, содержащихся в Правилах обработки персональных данных для каждой информационной системы персональных данных Учреждения;
- знания и соблюдение работниками Учреждения положений действующего законодательства Российской Федерации в области персональных данных;
- знания и соблюдение работниками Учреждения положений локальных актов Учреждении в области обработки и обеспечения безопасности персональных данных;
- знания и соблюдение работниками Учреждения инструкций, руководств и иных эксплуатационных документов на применяемые средства автоматизации, в том числе программное обеспечение, и средства защиты информации;
- соблюдение работниками Учреждения конфиденциальности персональных данных;
- актуальность локальных актов Учреждения в области обеспечения безопасности персональных данных;
- соблюдение работниками Учреждения требований по обеспечению безопасности персональных данных;
- наличие локальных актов Учреждения, технической и эксплуатационной документации технических и программных средств информационных систем персональных данных Учреждения;
- иных вопросов.

9.3. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, директору докладывает ответственный за организацию обработки персональных данных, либо председатель комиссии.

## 10. Права субъекта персональных данных

10.1. Субъект персональных данных имеет право получать доступ к своим персональным данным и ознакомление с ними, включая право на безвозмездное получение копий любой записи, содержащей его персональные данные.

10.2. Субъект персональных данных имеет право требовать от работников Учреждения уточнения, исключения или исправления неполных, неверных, устаревших, недостоверных, незаконно полученных или не являющих необходимыми для работы Учреждении персональных данных.

10.3. Субъект персональных данных имеет право получать информацию, которая касается обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных;
- правовые основания и цели обработки персональных данных;
- цели и применяемые способы обработки персональных данных;
- наименование и место нахождения Учреждения, сведения о лицах (за исключением работников Учреждения), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных ФЗ-№152 «О персональных данных»;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные ФЗ-№152 «О персональных данных» или другими федеральными законами.

10.4. Субъект персональных данных имеет право требовать извещения работниками Учреждения всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях.

## 11. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

11.1. Работники Учреждения, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

Приложение № 1
к Положению об обработке
персональных данных работников в
ГБУСО «Новоалександровский КЦСОН»

**ПЕРЕЧЕНЬ**
**персональных данных, обрабатываемых в ГБУСО «Новоалександровский КЦСОН» с использованием средств автоматизации и без использования таких средств**

В ГБУСО «Новоалександровский КЦСОН» обрабатывается следующий перечень персональных данных:

− анкетные и биографические данные;
− занимаемая должность;
− документы, содержащие сведения о заработной плате, доплатах и надбавках;
− паспортные данные или иной документ, удостоверяющий личность;
− адрес регистрации;
− адрес проживания;
− свидетельство о постановке на учет в налоговый орган и присвоения ИНН;
− номер страхового свидетельства государственного пенсионного страхования;
− медицинское заключение о состоянии здоровья, сведения об ограничении трудоспособности;
− информация о постановке на воинский учет;
− номер телефона;
− документы об образовании, о квалификации или наличии специальных знаний или специальной подготовки;
− данные о детях;
− данные о семейном положении;
− содержание трудового договора;
− подлинники и копии приказов по личному составу, приказы о приеме лица на работу, об увольнении, а так же о переводе лица на другую должность;
− личные дела и трудовые книжки работников;
− основания к приказам по личному составу (заявления работника);
− карточка Т-2;
− другие документы, содержащие сведения, предназначенные для использования в служебных целях;
− локальные нормативные акты, содержащие любую информацию о физическом лице (фамилию, имя, отчество, адрес, образец подписи и т.д.);
− дела, содержащие материалы по повышению квалификации и переподготовке работников, их аттестации, служебным расследованиям.

Директор Государственного бюджетного
учреждения социального обслуживания
«Новоалександровский комплексный центр
социального обслуживания населения» Т.В. Степанова

Приложение № 2
к Положению об обработке
персональных данных работников в
ГБУСО «Новоалександровский КЦСОН»

**ОБЯЗАТЕЛЬСТВО**
**о неразглашении персональных данных**
**в ГБУСО «Новоалександровский КЦСОН»**

Я, _____
(ФИО сотрудника)

паспорт серии _____№_____ выдан_____

_____,
(орган, выдавший паспорт и дата выдачи)

Исполняющий (ая) должностные обязанности _____
(должность)

предупрежден(а), что на период исполнения должностных обязанностей мне будет предоставлен допуск к персональным данным. Настоящим добровольно принимаю на себя обязательства:

1. Не разглашать третьим лицам персональные данные, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей.

2. В случае попытки третьих лиц получить от меня персональные данные, сообщать непосредственному руководителю.

3. Не использовать персональные данные с целью получения выгоды.

4. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты персональных данных.

5. После прекращения права на допуск к персональным данным не разглашать и не передавать третьим лицам известные мне персональные данные.

Я предупрежден (а), что в случае нарушения данного обязательства буду привлечен(а) к ответственности в соответствии с законодательством Российской Федерации.

_____ _____ _____
(Фамилия, Имя, Отчество) (Дата) (Подпись)

Приложение № 3
к Положению об обработке
персональных данных работников в
ГБУСО «Новоалександровский КЦСОН»

**СОГЛАСИЕ**
**на обработку персональных данных**

Я, _____,
(фамилия, имя, отчество)
проживающий(ая) _____,
(адрес регистрации)
_____
_____,
_____,
(документ, удостоверяющий личность, серия, номер, кем выдан и дата выдачи)
даю согласие государственному бюджетному учреждению социального обслуживания «Новоалександровский комплексный центр социального обслуживания населения», расположенному по адресу: г. Новоалександровск, пер.Красноармейский 1, на автоматизированную, а также без использования средств автоматизации обработку в соответствии с Федеральным законом «О персональных данных» моих персональных данных, содержащихся в моем личном деле, в целях, связанных с осуществлением трудовой деятельности в учреждениях, подведомственных министерству социальной защиты населения Ставропольского края и осуществлением всех действий, направленных на реализацию положений Трудового кодекса Российской Федерации, иных нормативных правовых актов Российской Федерации и нормативных правовых актов Ставропольского края, касающихся вопросов обработки персональных данных, в том числе по направлению запросов, содержащих мои персональные данные, в компетентные органы в целях осуществления проверки достоверности представленных мною сведений, любыми способами, предусмотренными законодательством Российской Федерации для обработки персональных данных в пределах реализации указанных целей, для обеспечения соблюдения трудового законодательства и иных нормативных правовых актов, обеспечения личной безопасности, контроля количества и качества выполняемой работы и обеспечения сохранности государственного имущества, а именно использовать мои персональные данные для: формирования кадровых документов, включения в резерв, представления к награждению соответствующими наградами и для выполнения всех требований трудового законодательства.

Я даю согласие на совершение следующих действий оператора с моими персональными данными: сбор, систематизацию, накопление, уточнение (обновление, изменение), хранение, использование, передачу, уничтожение персональных данных в соответствии с законодательством Российской Федерации и законодательством Ставропольского края.

Срок действия настоящего Согласия определяется в соответствии с законодательством Российской Федерации и законодательством Ставропольского края в соответствии с порядком обработки персональных данных и действует со дня его подписания до дня его отзыва в письменной форме. При этом уничтожение персональных данных, содержащихся в моем личном деле, не производится.

Об ответственности за достоверность представленных мною персональных данных предупрежден(а).

«____»_____20___ г. _____ _____
(подпись) (расшифровка подписи)

Приложение №4
к Положению об обработке
персональных данных работников в
ГБУСО «Новоалександровский КЦСОН»

**СОГЛАСИЕ**
**на принятие решений, порождающих юридические последствия**

Я,
_____
(Ф.И.О. полностью)

проживающий(-ая)_____
_____,
(документ, удостоверяющий личность, серия, номер, кем выдан и дата выдачи)

в соответствии со статьей 16 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» даю согласие ГБУСО «Новоалександровский КЦСОН», расположенному по адресу: 356000, Ставропольский край, Новоалександровский район, г. Новоалександровск, пер. Красноармейский, 1, на принятие решений, порождающих юридические последствия в отношении меня или иным образом затрагивающих мои права и законные интересы, на основании исключительно автоматизированной обработки моих персональных данных, а именно _____
(указать, на принятие каких именно решений субъектом

_____
персональных данных дается согласие)

_____.

Настоящее Согласие действует до момента принятия оператором решения о прекращении обработки персональных данных и (или) уничтожения документов, содержащих персональные данные.

Настоящее Согласие может быть отозвано мною в любое время на основании моего письменного заявления.

«____»_____20___г. _____
(подпись и фамилия, имя, отчество прописью полностью)

Приложение № 5
к Положению об обработке
персональных данных работников в
ГБУСО «Новоалександровский КЦСОН»

**Разъяснения юридических последствий отказа предоставить свои персональные данные**

Мне, _____
(Ф.И.О. полностью)

разъяснены юридические последствия отказа предоставить свои персональные данные ГБУСО «Новоалександровский КЦСОН».

В соответствии со 57, 65 Трудового кодекса Российской Федерации субъект персональных данных, поступающих на работу или работающий в ГБУСО «Новоалександровский КЦСОН», обязан представить определенный перечень информации о себе.

Без предоставления субъектом персональных данных обязательных для заключения контракта (трудового договора) сведений, контракт (трудовой договор) не может быть заключен.

На основании пункта 11 части 1 статьи 77 Трудового кодекса Российской Федерации контракт (трудовой договор) прекращается вследствие нарушения установленных обязательных правил его заключения, если это нарушение исключает возможность замещения должности (продолжения работы).

В случае непредставления гражданином персональных данных требуемых для предоставления государственных и муниципальных услуг, ему будет отказано в предоставлении такой услуги.

В случае непредставления субъектом персональных данных, требуемых для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, в том числе в случае реализации оператором своего права на уступку прав (требований) по такому договору, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем, данный договор заключен не будет.

«____»_____20___г. _____
(подпись и фамилия, имя, отчество прописью полностью)

Приложение № 6
к Положению об обработке персональных
данных работников в ГБУСО
«Новоалександровский КЦСОН»

**СОГЛАСИЕ**
**на передачу персональных данных третьим лицам**

Я, _____
(Ф.И.О. полностью)

проживающий(-ая)_____
_____,
(документ, удостоверяющий личность, серия, номер, кем выдан и дата выдачи)

в соответствии со статьями 7 и 12 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» даю согласие ГБУСО «Новоалександровский КЦСОН», расположенному по адресу: 356000, Ставропольский край, г. Новоалександровск, пер. Красноармейский, 1, на передачу моих персональных данных, а именно _____
(указать перечень персональных данных,

_____
на передачу которых дается согласие)

_____
(указать перечень третьих лиц, на передачу персональных данных которым

_____
дается согласие, в том числе в случае трансграничной передачи - указать, на территорию какого иностранного государства, какому органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу субъектом персональных данных дается согласие на трансграничную передачу его персональных данных)

в целях _____
(указать цели передачи персональных данных третьим лицам)

Настоящее Согласие действует до момента принятия оператором решения о прекращении обработки персональных данных и (или) уничтожения документов, содержащих персональные данные.

Настоящее Согласие может быть отозвано мною в любое время на основании моего письменного заявления.

«____»_____20___г. _____
(подпись и фамилия, имя, отчество прописью полностью)

Приложение № 7
к Положению об обработке
персональных данных работников в
ГБУСО «Новоалександровский КЦСОН»

**СОГЛАСИЕ**
**на размещение персональных данных в общедоступных источниках персональных данных**

Я,

_____,
(фамилия, имя, отчество)

проживающий(ая)_____,
(адрес регистрации по месту жительства, адрес фактического проживания)

_____,
паспорт серии _____№_____ выдан_____
_____,
(орган, выдавший паспорт и дата выдачи)

в соответствии со статьей 8 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» даю согласие ГБУСО «Новоалександровский КЦСОН», расположенному по адресу: 356000, Ставропольский край, г. Новоалександровск, пер. Красноармейский, 1, на размещение моих персональных данных в целях
_____
_____
_____
(указать цель размещения персональных данных в общедоступном источнике персональных данных)

в общедоступных источниках персональных данных, в том числе в
_____
_____
(указать наименование общедоступного источника
персональных данных и перечень персональных данных, размещаемых в общедоступном
источнике персональных данных)

Настоящее Согласие действует до принятия в установленном порядке решения об освобождении от должности.

Настоящее Согласие может быть отозвано мною в любое время на основании моего письменного заявления.

«____»_____20___г. _____
(подпись и фамилия, имя, отчество прописью полностью)

Приложение № 8
к Положению об обработке персональных данных работников в ГБУСО «Новоалександровский КЦСОН»

**Отзыв согласия на обработку персональных данных**

« ____» _____ 201__ г.

Во исполнение положений Федерального закона «О персональных данных» № 152-ФЗ от 27 июля 2006 г.
я, _____
(фамилия, имя, отчество)

_____
_____
(серия, номер паспорта, кем выдан)

_____
_____
(место регистрации)

**отзываю** у ГБУСО «Новоалександровский КЦСОН» **свое согласие на обработку персональных данных**. **Прошу прекратить обработку персональных данных** не позднее трех рабочих дней с даты поступления настоящего Отзыва, а также уничтожить всю персональную информацию, касающуюся меня лично.

«____»_____20___г. _____
(подпись и фамилия, имя, отчество прописью полностью)

Приложение № 3
к приказу директора ГБУСО
«Новоалександровский КЦСОН»
от 22 августа 2017 года № 448

**ПОЛОЖЕНИЕ**
**об обработке и защите персональных данных, получателей социальных услуг в ГБУСО «Новоалександровский КЦСОН»**

**1. Общие положения**

1.1. Настоящее Положение об обработке и защите персональных данных получателей социальных услуг в ГБУСО «Новоалександровский КЦСОН» (далее — Положение) разработано в соответствии с Конституцией Российской Федерации, Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»; Федеральным законом от 28.12.2013 №442-ФЗ «Об основах социального обслуживания граждан в Российской Федерации», Федеральным законом от 24.04.2008 №48-ФЗ «Об опеке и попечительстве», Постановлением Правительства Российской Федерации от 15.09.2008 N 687 «Об утверждении Положения об особенностях Обработки персональных данных, осуществляемой без использования средств автоматизации», Приказами Министерства труда и социальной защиты Российской Федерации от 24.11.2014 №935н «Об утверждении Примерного порядка предоставления социальных услуг в стационарной форме социального обслуживания», №938н «Об утверждении Примерного порядка предоставления социальных услуг в полустационарной форме социального обслуживания», №939н «Об утверждении Примерного порядка предоставления социальных услуг в форме социального обслуживания на дому»; Постановлением Правительства Ставропольского края от 29.12.2014 № 560-п «Об утверждении порядков предоставления социальных услуг поставщиками социальных услуг в Ставропольском крае».

1.2. Цель данного Положения – определение порядка обработки персональных данных в Учреждении, обеспечение требований защиты прав граждан, обратившихся за оказанием социальных услуг, при обработке их персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также установление ответственности должностных лиц, уполномоченных на обработку персональных данных, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.3. Персональные данные могут обрабатываться только для целей, непосредственно связанных с деятельностью ГБУСО «Новоалександровский КЦСОН» (далее – Учреждение), в частности осуществление уставной деятельности Учреждения: социальное обслуживание граждан, признанных нуждающимися в социальном обслуживании вследствие обстоятельств, которые ухудшают или могут ухудшить условия их жизнедеятельности (далее получатели социальных услуг). Учреждение собирает данные только в объеме, необходимом для достижения названных целей.

1.2. Сбор, хранение, использование и распространение, в том числе передача третьим лицам, персональных данных без письменного согласия получателя социальных услуг не допускается. Режим конфиденциальности персональных данных снимается в случаях обезличивания или включения их в общедоступные источники персональных данных, если иное не определено законом.

1.3. Работники Учреждения в обязанность которых входит обработка персональных данных получателя социальных услуг, обязаны обеспечить каждому получателю социальных услуг возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

1.4. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда получателю социальных услуг, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.

1.5. Настоящее положение утверждается директором Учреждения и является обязательным для исполнения всеми работниками Учреждения, имеющим доступ к персональным данным получателя социальных услуг.

**2. Понятие и состав персональных данных**

2.1. Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

2.2. В состав персональных данных получателя социальных услуг входят:

- анкетные и биографические данные;
- образование;
- сведения о трудовом и общем стаже;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- доходы получателей соц. услуг;

- сведения о социальных льготах;
- специальность,
- наличие судимостей;
- адрес места жительства;
- домашний телефон;
- место работы или учебы членов семьи и родственников;
- характер взаимоотношений в семье;
- содержание договора о предоставлении социальных услуг;
- другие персональных данные, позволяющие идентифицировать получателя социальных услуг.

2.3. Данные документы являются конфиденциальными, хотя, учитывая их массовость и единое место обработки и хранения - соответствующий гриф ограничения на них не ставится.

### 3. Принципы обработки персональных данных получателя социальных услуг

3.1. Обработка персональных данных должна осуществляться на основе принципов:

– законности целей и способов обработки персональных данных и добросовестности;

– соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Учреждения;

– соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

– достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

– недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных;

– уничтожения персональных данных после достижения целей обработки или в случае утраты необходимости в их достижении;

– личной ответственности работников Учреждения за сохранность и конфиденциальность персональных данных, а также носителей этой информации;

– наличие четкой разрешительной системы доступа работников Учреждения к документам и базам данных, содержащим персональные данные.

### 4. Обязанности работников Учреждения

4.1. В целях обеспечения прав и свобод человека и гражданина работники Учреждения при обработке персональных данных получателя социальных услуг обязаны соблюдать следующие общие требования:

4.1.1. При сборе персональных данных работники Учреждения обязаны предоставить получателю социальных услуг по его просьбе информацию, содержащую:

– подтверждение факта обработки персональных данных получателя социальных услуг, а также цель такой обработки;

– способы обработки персональных данных;

– сведения о работниках Учреждения, которые имеют доступ к персональным данным получателя социальных услуг или которым может быть предоставлен такой доступ;

– перечень обрабатываемых персональных данных получателя социальных услуг и источник их получения;

– сроки обработки персональных данных получателя социальных услуг в том числе сроки их хранения;

– сведения о том, какие юридические последствия для получателя социальных услуг может повлечь за собой обработка его персональных данных.

4.1.2. Если обязанность предоставления персональных данных установлена федеральным законом, работники Учреждения обязаны разъяснить получателю социальных услуг юридические последствия отказа предоставить свои персональные данные.

4.1.3. Если персональные данные были получены не от получателя социальных услуг, за исключением случаев, если персональные данные были предоставлены работниками Учреждения на основании федерального закона или если персональные данные являются общедоступными, до начала обработки таких персональных данных работник Учреждения обязан предоставить получателю социальных услуг следующую информацию:

– наименование (фамилия, имя, отчество) и адрес оператора или его представителя;

– цель обработки персональных данных и ее правовое основание;

– предполагаемые пользователи персональных данных;

– права получателя социальных услуг

4.2. Работники Учреждения не имеют права получать и обрабатывать персональные данные получателя социальных услуг о его расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, за исключением случаев, предусмотренных законом. В частности, работники Учреждения вправе обрабатывать указанные персональные данные гражданина только с его письменного согласия, при наличии надлежащим образом оформленного запроса предоставлять получателю социальных услуг доступ к его персональным данным, хранение и защита персональных данных получателя социальных услуг от неправомерного их

использования или утраты должна быть обеспечена работниками Учреждения за счет средств Учреждения в порядке, установленном законодательством.

4.3. Работники Учреждения должны быть ознакомлены под расписку с данным положением, устанавливающими порядок обработки персональных данных получателей социальных услуг, а также о правах и обязанностях в этой области.

**5. Права получателя социальных услуг**

5.1. Получатель социальных услуг имеет право на получение сведений о наличии у работников Учреждения своих персональных данных, а также на ознакомление с такими персональными данными. Получатель социальных услуг вправе требовать от работников Учреждения уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

5.2. Сведения о наличии персональных данных должны быть предоставлены получателю социальных услуг работниками Учреждения в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим получателям социальных услуг

5.3. Доступ к своим персональным данным предоставляется получателю социальных услуг или его законному представителю работниками Учреждения при обращении либо при получении запроса получателя социальных услуг или его законного представителя. Запрос должен содержать номер основного документа, удостоверяющего личность получателя социальных услуг или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись получателя социальных услуг или его законного представителя. Запрос может быть направлен в электронной форме и подписан электронной цифровой подписью в соответствии с законодательством Российской Федерации.

5.4. Получатель социальных услуг имеет право на получение при обращении или при получении запроса информации, касающейся обработки его персональных данных, в том числе содержащей:

– подтверждение факта обработки персональных данных, а также цель такой обработки;

– способы обработки персональных данных;

– сведения о работниках Учреждения, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

– перечень обрабатываемых персональных данных и источник их получения;

– сроки обработки персональных данных, в том числе сроки их хранения;

– сведения о том, какие юридические последствия для получателя социальных услуг может повлечь за собой обработка его персональных данных.

5.5. Право получателя социальных услуг на доступ к своим персональным данным ограничивается в случае, если:

– обработка персональных данных, в том числе персональных данных, полученных в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

– обработка персональных данных осуществляется органами, осуществившими задержание получателя социальных услуг по подозрению в совершении преступления, либо предъявившими получателю социальных услуг обвинение по уголовному делу, либо применившими к получателю социальных услуг меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

– предоставление персональных данных нарушает конституционные права и свободы других лиц.

5.6. Если получатель социальных услуг считает, что работники Учреждения осуществляют обработку его персональных данных с нарушением требований Федерального закона или иным образом нарушает его права и свободы, получатель социальных услуг вправе обжаловать их действия или бездействие в уполномоченный орган по защите прав или в судебном порядке.

5.7. Получатель социальных услуг имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

**6. Сбор, обработка и хранение персональных данных получателя социальных услуг**

6.1. Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

6.2. Порядок (сбора) получения персональных данных*:* получатель социальных услуг принимает решение о предоставлении своих персональных данных и дает согласие на их обработку своей волей и в своем интересе.

6.3. Документы, содержащие персональные данные получателя социальных услуг, создаются путём:

– создания документов, методом внесения сведений в учётные формы (на бумажных и электронных носителях);

– копирования оригиналов документов (паспорта, свидетельств и т.д.);

– получения оригиналов необходимых документов (справка о составе семьи, медицинское заключение и т.д.).

6.4. При передаче персональных данных получателя социальных услуг работники Учреждения должны соблюдать следующие требования:

6.4.1. не сообщать персональные данные получателя социальных услуг третьей стороне без его письменного согласия, за исключением случаев:

– обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является получатель социальных слуг;

– обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

– обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов гражданина, если получение его согласия невозможно.

6.4.2. Предупредить лиц, получающих персональные данные получателя социальных услуг о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные граждан, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется в случае обезличивание персональных данных и в отношении общедоступных данных

6.4.3. Разрешать доступ к персональным данным получателя социальных услуг только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные гражданина, которые необходимы для выполнения конкретных функций

6.5. Персональные данные получателя социальных услуг хранятся в его личном деле или карточке учёта. Персональные данные получателя социальных услуг могут храниться, как на бумажных носителях, так и в электронном виде.

6.6. В Учреждении персональные данные получателей социальных услуг на бумажных носителях хранятся в специально отведенном шкафу и на стеллажах.

6.7. Персональные данные получателей социальных услуг могут также храниться в электронном виде в компьютерной программе «Адресная социальная помощь». Доступ к электронным базам данных, содержащим персональные данные получателей социальных услуг обеспечивается системой паролей.

6.8. Персональные данные, содержащиеся на бумажных носителях, сдаются в архив после истечения установленного срока хранения.

6.9. Организация работы с получателем социальных услуг должна быть подчинена, в том числе, решению задач обеспечения безопасности персональных данных, их защиты:

– при работе с получателем социальных услуг работник Учреждения не должен выполнять функции, не связанные с приемом, вести служебные и личные переговоры по телефону. На его столе не должно быть никаких документов, кроме тех, которые касаются данного посетителя;

– не допускается отвечать на вопросы, связанные с передачей персональных данных по телефону.

6.10. Личные дела получателей социальных услуг, журналы и карты учета хранятся в рабочее и нерабочее время в специализированных шкафах. Работникам Учреждения не разрешается при выходе из помещения оставлять какие-либо документы, содержащие персональные данные, на рабочем столе или оставлять кабинеты незапертыми.

6.11. На рабочем столе сотрудника должен всегда находиться только тот массив документов и учетных карточек, с которым в настоящий момент он работает. Другие документы, дела, карточки, журналы должны находиться в шкафу. Исполняемые документы не разрешается хранить в россыпи. Их следует помещать в папки, на которых указывается вид производимых с ними действий (подшивка в личные дела, для отправки и пр.).

6.12. В конце рабочего дня все документы, дела, листы бумаги и блокноты с рабочими записями, инструктивные и справочные материалы должны быть убраны в шкафы, сейфы. На рабочем столе не должно оставаться ни одного документа. Черновики и редакции документов, испорченные бланки, листы со служебными записями в конце рабочего дня уничтожаются.

## 7. Доступ к персональным данным получателя социальных услуг.

7.1. К обработке персональных данных получателя социальных услуг могут иметь доступ только работники Учреждения, допущенные к работе с персональными данными получателя социальных услуг и подписавшие Обязательство о соблюдении конфиденциальности персональных данных.

7.2. Перечень должностей сотрудников ГБУСО «Новоалександровский КЦСОН», допущенных к обработке персональных данных утверждается приказом директора Учреждения.

7.3. Право доступа к своим персональным данным в Учреждении имеют:

– ПСУ, как субъект персональных данных.

7.4. Обработка персональных данных может осуществляться исключительно в целях установленных Положением и соблюдения законов и иных нормативных правовых актов РФ.

## 8. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

8.1. Персональная ответственность является одним из главных требований к организации функционирования системы защиты персональных данных и обязательным условием обеспечения эффективности функционирования данной системы.

8.2. Работники Учреждения, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

Приложение № 4
к приказу директора ГБУСО
«Новоалександровский КЦСОН»
от 22 августа 2017 года № 448

**ИНСТРУКЦИЯ**
**администратора информационных систем персональных данных по обеспечению безопасности персональных данных в ГБУСО «Новоалександровский КЦСОН»**

**1. Общие положения**

1.1. Настоящая Инструкция определяет обязанности, полномочия и ответственность администратора информационных систем персональных данных (ИСПДн) по обеспечению безопасности персональных данных в ГБУСО «Новоалександровский КЦСОН».

1.2. Администратор ИСПДн (далее – администратор) назначается приказом директора ГБУСО «Новоалександровский КЦСОН».

1.3. Администратор ИСПДн подчиняется директору ГБУСО «Новоалександровский КЦСОН».

1.4. Администратор ИСПДн в своей работе руководствуется настоящей Инструкцией, а также руководящими и нормативными документами ФСТЭК России и внутренними регламентирующими документами по защите информации в ГБУСО «Новоалександровский КЦСОН».

1.5. Администратор ИСПДн отвечает за обеспечение устойчивой работоспособности элементов ИСПДн и средств защиты, при обработке персональных данных.

**2. Обязанности по обеспечению безопасности информации**

Администратор ИСПДн обязан:

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2.2. Ознакомить всех пользователей ИСПДн с внутренними нормативно-правовыми актами по обеспечению безопасности персональных данных (под роспись).

2.3. Обеспечивать установку, настройку и своевременное обновление элементов ИСПДн:

– программного обеспечения автоматизированных рабочих мест (далее – АРМ) и серверов (операционные системы, прикладное и специальное ПО);

– аппаратных средств;

– аппаратных и программных средств защиты.

2.4. Обеспечивать работоспособность элементов ИСПДн и локальной вычислительной сети.

2.5. Осуществлять контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов (если не назначен другой ответственный).

2.6. Обеспечивать функционирование и поддерживать работоспособность средств защиты.

2.7. В случае отказа работоспособности технических средств и программного обеспечения элементов ИСПДн, в том числе средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.8. Осуществлять регистрацию пользователей, выдачу временных паролей пользователей, осуществлять контроль за правильностью использования пароля пользователем ИСПДн.

2.9. Обеспечивать постоянный контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности информации.

2.10. Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты.

2.11. Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств и отправке их в ремонт.

2.12. Присутствовать при выполнении технического обслуживания элементов ИСПДн сторонними физическими лицами и Компаниями.

2.13. Принимать меры по реагированию в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

**3. Ответственность**

3.1. В случае нарушения положений настоящей Инструкции Администратор ИСПДн несёт ответственность в соответствии с действующим законодательством.

Директор ГБУСО
«Новоалександровский КЦСОН» Т.В. Степанова

Приложение № 5
к приказу директора ГБУСО
«Новоалександровский КЦСОН»
от 22 августа 2017 года № 448

**ИНСТРУКЦИЯ**
**о порядке резервирования и восстановления работоспособности технических средств, программного обеспечения и баз данных в ГБУСО «Новоалександровский КЦСОН»**

## 1. Назначение и область действия

1.1 Данная Инструкция определяет действия, связанные с мерами и средствами поддержания непрерывной работы и восстановления работоспособности информационных систем в ГБУСО «Новоалександровский КЦСОН».

1.2. Настоящая Инструкция регламентирует:

- меры защиты от потери информации;
- действия по восстановлению в случае потери информации.

1.3. Действие настоящей Инструкции распространяется на администраторов информационных систем, ответственных за резервное копирование информации.

## 2. Меры обеспечения надежной работы и восстановления ресурсов при возникновении инцидентов

2.1. Технические меры.

2.1.1. К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения инцидентов, такие как:

- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;

2.1.2. Системы жизнеобеспечения ИСПДн включают:

- пожарные сигнализации;
- системы вентиляции и кондиционирования;

2.1.3. Все критичные помещения (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации.

2.1.4. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

- локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;
- источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;

2.1.5. Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на носитель (ленту, жесткий диск и т.п.).

2.2. Организационные меры.

2.2.1. Резервное копирование и хранение данных должно осуществлять на периодической основе:

- для обрабатываемых персональных данных – не реже раза в неделю или по требованию пользователя ИСПДн;
- для системной информации – не реже раза в месяц;

2.2.2. Данные о проведение процедуры резервного копирования должны отражаться в специально созданном Журнале учета, по форме согласно приложения к настоящей Инструкции.

2.2.3. Носители должны храниться в несгораемом шкафу или помещении, оборудованном системой пожаротушения.

2.2.4. Носители и резервные копии данных должны храниться не менее года для возможности восстановления данных.

## 3. Порядок проведения резервирования информации

3.1. Перед проведением процедуры резервного копирования необходимо убедиться в том, что все пользователи информационной системы завершили свою работу с информационной системой.

3.2. Резервирование информации в информационных системах персональных данных проводится при помощи штатных средств, поставляемых в составе специализированного программного обеспечения для построения информационной системы, либо, в случае отсутствия таковых, штатными средствами операционной системы или системы управления базами данных (при использовании таковой).

3.3. Архивация может производиться как штатными средствами, поставляемыми в составе специализированного программного обеспечения для построения информационной системы, так и сторонним программным обеспечением (например, 7zip, WinRar).

3.4. Резервные копии должны сохраняться на носители, не входящие в состав технических средств информационной системы персональных данных (внешние жесткие диски, CD/DVD диски, flash диски).

3.5. После завершения процедуры резервного копирования информации и записи резервной копии на носитель, необходимо поместить носитель с резервной копией в специально отведённое для хранения место и проставить соответствующую отметку в Журнале.

## 4. Порядок проведения восстановления информации

4.1. Перед проведением процедуры восстановления информации необходимо убедиться в том, что все пользователи информационной системы завершили свою работу с информационной системой.

4.2. Восстановление информации следует проводить из наиболее актуальной резервной копии.

4.3. В случае, если специализированное программное обеспечение для построения информационной системы не позволяет работать с заархивированными резервными копиями, то перед восстановлением информации необходимо разархивировать файлы резервной копии при помощи стороннего программного обеспечения (например 7zip, WinRar).

4.4. Восстановление информации в информационных системах персональных данных проводится при помощи штатных средств, поставляемых в составе специализированного программного обеспечения для построения информационной системы, либо, в случае отсутствия таковых, штатными средствами операционной системы или системы управления базами данных (при использовании таковой).

4.5. После завершения процедуры восстановления необходимо убедиться в работоспособности информационной системы персональных данных.

4.6. В случае успешного восстановления оповестить пользователей информационной системы о возможности продолжения работы. В противном случае необходимо изучить документацию, прилагаемую к программному обеспечению либо обратиться в службу технической поддержки.

## 5. Ответственность

5.1. Работники, нарушившие требования данной Инструкции, несут ответственность в соответствии с действующим законодательством.

Приложение
к Инструкции о порядке резервирования и восстановления работоспособности технических средств,
программного обеспечения
и баз данных в ГБУСО «Новоалександровский КЦСОН»

**ЖУРНАЛ**
**учета резервного копирования и восстановления данных**

количество листов_____

начат_____

окончен_____

| № п.п. | Дата проведения резервного копирования/восстановления | Наименование информационной системы/базы данных | Ф.И.О., подпись ответственного |
|---|---|---|---|
| 1. | 2. | 3. | 4. |
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |
| 6. | | | |
| 7. | | | |

Приложение № 6
к приказу директора ГБУСО
«Новоалександровский КЦСОН»
от 22 августа 2017 года № 448

**ИНСТРУКЦИЯ**
**ответственного за организацию обработку персональных данных в ГБУСО «Новоалександровский КЦСОН»**

**1. Общие положения**

1.1. Настоящая Инструкция разработана в соответствии со ст. 22.1 Федерального закона от 27.07.2006 № 152 - ФЗ «О персональных данных» и определяет обязанности, полномочия и ответственность лиц, ответственных за обработку персональных данных в ГБУСО «Новоалександровский КЦСОН».

1.2. Ответственный за обработку персональных данных назначается приказом директора из числа работников ГБУСО «Новоалександровский КЦСОН».

1.3. Ответственный за обработку персональных данных подчиняется директору .

1.4. Ответственный за организацию обработки персональных данных в своей деятельности руководствуется Трудовым кодексом РФ, Федеральным законом от 27 июля 2006 № 152-ФЗ «О персональных данных», постановлением Правительства РФ от 15 сентября 2008г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства РФ от 21 марта 2012г. № 211 «Перечень мер направленных на обеспечение выполнения обязанностей предусмотренных Федеральным законом «О персональных данных» и, настоящей должностной инструкцией и внутренними документами ГБУСО «Новоалександровский КЦСОН» по защите информации.

**2. Обязанности**

2.1. Предоставлять субъекту персональных данных либо его представителю по запросу информацию об обработке его персональных данных.

2.2. Осуществлять внутренний текущий контроль за соблюдением требований законодательства Российской Федерации и правил обработки персональных данных в ГБУСО «Новоалександровский КЦСОН» при обработке персональных данных, в том числе требований к защите персональных данных.

2.3. Доводить до сведения работников ГБУСО «Новоалександровский КЦСОН» содержание положений законодательства РФ о персональных данных, внутренних нормативно - правовых актов ГБУСО «Новоалександровский КЦСОН» по вопросам обработки персональных данных, требований по защите персональных данных.

2.4. Организовать прием и обработку обращений и запросов субъектов персональных данных или их представителей и осуществлять контроль за приемом и обработкой таких обращений и запросов:

- в соответствии с ФЗ-152 «О персональных данных» субъект персональных данных или его представитель имеет право на получение информации, касающейся обработки его персональных данных на основании обращения либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации;
- все обращения и запросы субъектов персональных данных подлежат обязательному учету;
- ответственный за обработку обязан фиксировать все обращения и запросы в журнале учета обращений граждан (субъектов персональных данных).

2.4. Организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

2.5. Организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

2.6. Получать обязательство о прекращении обработки персональных данных у лиц, непосредственно осуществляющих обработку персональных данных, в случае расторжения с ним договора (контракта).

2.7. Получать согласия на обработку персональных данных у субъектов персональных данных.

2.8. Разъяснять субъекту персональных данных юридические последствия отказа предоставления его персональных данных.

2.9. Обеспечивать постоянный контроль выполнения установленного комплекса мероприятий по обеспечению безопасности информации пользователями информационной системы персональных.

**3. Ответственность**

3.1. В случае нарушения положений настоящей Инструкции ответственные за обработку персональных данных лица несут ответственность в соответствии с действующим законодательством.

Приложение № 7
к приказу директора ГБУСО
«Новоалександровский КЦСОН»
от 22 августа 2017 года № 448

# ИНСТРУКЦИЯ
# по организации антивирусной защиты в ГБУСО «Новоалександровский КЦСОН»

## 1. Общие положения

1.1. Настоящая Инструкция предназначена для организации порядка проведения антивирусного контроля в ГБУСО «Новоалександровский КЦСОН» и предотвращения возникновения фактов заражения вредоносным программным обеспечением.

1.2. Данная Инструкция распространяется на всех пользователей и администраторов информационных систем персональных данных (далее – ИСПДн) в ГБУСО «Новоалександровский КЦСОН».

## 2. Установка и обновление антивирусных средств

2.1. Установка и настройка антивирусных средств осуществляется только администратором информационной системы персональных данных.

2.2. Обновление антивирусных баз осуществляется по расписанию в автоматическом режиме, либо вручную при необходимости.

## 3. Требования к проведению мероприятий по антивирусной защите

3.1. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, flash дисках, CD-ROM и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

3.2. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие заражения вредоносным программным обеспечением.

3.3. Контроль информации на съёмных носителях производится непосредственно перед её использованием.

3.4. Особое внимание следует обратить на недопустимость использования съёмных носителей, принадлежащих лицам, временно допущенным к работе на ЭВМ. Работа этих лиц должна проводиться под непосредственным контролем сотрудника или ответственного за информационную безопасность.

3.5. Ежедневно, в начале работы, должно выполняться обновление антивирусных баз и проводиться антивирусный контроль всех загружаемых в память файлов персонального компьютера.

3.6. Периодические проверки компьютеров должны проводиться не реже одного раза в неделю.

3.7. Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера должен выполняться:

– непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка;

– 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.).

## 4. Действия работников при обнаружении компьютерного вируса

4.1. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователи обязаны:

– приостановить работу;

– немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора информационной системы персональных данных;

– провести лечение или уничтожение зараженных файлов.

4.2. При возникновении подозрения на наличие компьютерного вируса пользователь или администратор информационной системы персональных данных должны провести внеочередной антивирусный контроль.

## 5. Ответственность при организации антивирусной защиты

5.1. Ответственность за организацию антивирусной защиты возлагается на администратора информационной системы персональных данных.

5.2. Ответственность за выполнение требований данной Инструкции возлагается на Пользователей и администратора информационной системы персональных данных.

5.3. Периодический контроль за соблюдением положений данной Инструкции возлагается на администратора информационной системы персональных данных.

Приложение № 8
к приказу директора ГБУСО
«Новоалександровский КЦСОН»
от 22 августа 2017 года № 448

# ИНСТРУКЦИЯ
## по порядку учета и хранению документов, содержащих персональные данные, в ГБУСО «Новоалександровский КЦСОН»

### 1. Общие положения

1.1. Настоящая Инструкция разработана с целью обеспечения безопасности персональных данных при работе с документами, содержащими персональные данные.

1.2. Действие настоящей Инструкции распространяется на ответственных лиц по работе с персональными данными.

### 2. Порядок учета, хранения и обращения с документами, которые содержат персональные данные

2.1. Все находящиеся на хранении и в обращении документы с персональными данными в ГБУСО «Новоалександровский КЦСОН» подлежат учёту.

2.2. Каждый документ, личное дело или журнал должны иметь уникальный учетный номер.

2.3. Учет и выдачу документов с персональными данными осуществляют работники ГБУСО «Новоалександровский КЦСОН», на которых возложены функции хранения документов, содержащих персональные данные. Факт выдачи документов фиксируется в журнале учета.

2.4. При работе с документами, которые содержат персональные данные необходимо:

- соблюдать требования настоящей Инструкции;
- использовать полученные документы исключительно для выполнения своих служебных обязанностей;
- ставить в известность ответственного за обработку персональных данных о любых фактах нарушения требований настоящей Инструкции;
- бережно относится к документам, содержащим персональные данные;
- обеспечивать физическую безопасность документов всеми разумными способами;
- обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях;
- извещать ответственного за организацию обработки персональных данных о фактах утраты (кражи) документов, содержащих персональные данные;
- осуществлять вынос документов с персональными данными для непосредственной передачи адресату только с письменного разрешения руководителя;
- при передаче персональных данных передаётся минимальный объем данных, который необходим для выполнения служебных обязанностей адресата.

2.5. В случае утраты или уничтожения документов, которые содержат персональные данные либо разглашении содержащихся в них сведений, немедленно ставится в известность директор. Отметки об утрате вносятся в журнал учета документов с персональными данными.

2.6. В случае увольнения или перевода работника в другое структурное подразделение, предоставленные документы с персональными данными информации изымаются.

### 3. Работа с журналом регистрации посетителей

3.1. Журнал регистрации посетителей необходим исключительно в целях контроля посещаемости.

3.2. В Журнале учёта посещаемости разрешается фиксация следующих персональных данных:

– Фамилия, Имя, Отчество;

– Наименование и номер документа, удостоверяющего личность (паспорт, водительское удостоверение, удостоверение личности и т.д.);

3.3. Порядок учёта, хранения и обращения с журналом регистрации посетителей осуществляется в соответствии с п. 2 настоящей инструкции.

3.4. В случае окончания журнала, его необходимо сдать в архив или уничтожить.

### 4. Запрещается

4.1. Использовать документы с персональными данными в личных целях.

4.2. Передавать документы с персональными данными третьим лицам без соответствующего разрешения директора.

4.3. Хранить документы с персональными данными вместе с документами с открытой информацией на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам.

4.4. Выносить документы с персональными данными из служебных помещений для работы с ними на дому и т. д.

4.5. Оставлять документы с персональными данными без присмотра.

4.6. Изготавливать и хранить копии паспортов или иных документов, удостоверяющих личность, за исключением случаев, предусмотренных законодательством.

### 5. Ответственность

5.1. Работники, нарушившие требования данной Инструкции, несут ответственность в соответствии с действующим законодательством Российской Федерации.

Приложение № 9
к приказу директора ГБУСО
«Новоалександровский КЦСОН»
от 22 августа 2017 года № 448

**ИНСТРУКЦИЯ**
**по обеспечению безопасности эксплуатации средств криптографической защиты информации (СКЗИ) в ГБУСО «Новоалександровский КЦСОН»**

**1. Общие положения**

1.1. Настоящая Инструкция определяет порядок учета, хранения и использования средств криптографической защиты информации (СКЗИ) и криптографических ключей, а также порядок изготовления, смены, уничтожения и компрометации криптографических ключей в целях обеспечения безопасности эксплуатации в ГБУСО «Новоалександровский КЦСОН».

1.2. Пользователь должен выполнять все требования настоящей Инструкции, правила, изложенные в эксплуатационной документации на СКЗИ, а также другие документы, регламентирующие порядок работы с СКЗИ.

**2. Обязанности Пользователя**

2.1. Пользователь обязан соблюдать требования по обеспечению безопасности функционирования СКЗИ.

2.2. Пользователь обязан обеспечить конфиденциальность всей информации ограниченного распространения, доступной по роду выполняемых функциональных обязанностей.

2.3. Пользователь обязан сдать носители ключевой информации (далее – НКИ) при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ, ответственному за обработку персональных данных.

2.4. Пользователь обязан сдать носители ключевой информации (далее – НКИ) по окончании срока действия сертификата ключа, а также в случае компрометации ключа.

2.5. Пользователь обязан немедленно уведомлять Ответственного за обработку персональных данных о компрометации криптографических ключей.

2.6. Пользователь обязан немедленно уведомлять Ответственного за обработку персональных данных о фактах утраты или недостачи СКЗИ, НКИ.

**3. Порядок обращения со средствами криптографической защиты информации**

3.1. Монтаж и установка СКЗИ осуществляются только уполномоченным лицом, либо организацией, имеющей необходимые лицензии.

3.2. Все СКЗИ и НКИ должны учитываться в журнале.

3.3. Для хранения носителей ключевой информации помещения обеспечиваются сейфами (металлическими шкафами).

3.4. Несанкционированное изготовление дубликатов ключей ЗАПРЕЩЕНО. В случае утери ключа механизм (секрет) замка (либо сам сейф) должен быть заменён.

3.5. К эксплуатации СКЗИ допускаются лица, изучившие правила пользования данным СКЗИ.

3.6. Все программное обеспечение ПЭВМ, предназначенной для установки СКЗИ, должно иметь соответствующие лицензии. Установка средств разработки и отладки программ на рабочую станцию, использующую СКЗИ, не допускается.

**4. Порядок обращения с ключами ЭЦП**

4.1. Криптографический ключ применяется для подписания (проверки электронной цифровой подписи) электронных документов до окончания срока его действия или наступления события, трактуемого как компрометация криптографических ключей.

4.2. Изготовление и выдача ключей ЭЦП осуществляется только Удостоверяющим центром.

4.3. НКИ являются объектами особой важности, т.к. они содержат информацию, предназначенную для гарантированной идентификации владельца ключа, защиты электронного документа от подделки и обеспечения конфиденциальности документа.

4.4. Владельцы ключей несут персональную ответственность за обеспечение конфиденциальности ключевой информации и защиту НКИ от несанкционированного использования.

4.5. Для хранения носителей ключевой информации Пользователь должен быть обеспечен личным сейфом.

**5. Запрещается**

5.1. Осуществлять несанкционированное и без учётное копирование ключевых данных.

5.2. Хранить НКИ вне сейфов и помещений, гарантирующих их сохранность и конфиденциальность.

5.3. Передавать НКИ третьим лицам.

5.4. Во время работы оставлять НКИ без присмотра (например, на рабочем столе или в разъеме системного блока ПЭВМ).

5.5. Хранить на НКИ какую-либо информацию, кроме ключевой.

5.6. Использование выведенных из действия криптографических ключей.

## 6. Действия при компрометации действующих ключей и восстановлении конфиденциальной связи

6.1. Под компрометацией криптографического ключа понимается утрата доверия к тому, что данный ключ обеспечивает однозначную идентификацию Владельца и конфиденциальность информации, обрабатываемой с его помощью. К событиям, связанным с компрометацией действующих криптографических ключей, относятся:

- Утрата (хищение) НКИ, в том числе – с последующим их обнаружением;
- Передача закрытых (конфиденциальных) ключей по линии связи в открытом виде;
- Нарушение правил хранения криптографических ключей;
- Вскрытие фактов утечки передаваемой информации или её искажения (подмены, подделки);
- Отрицательный результат при проверке наложенной ЭЦП;
- Несанкционированное или без учётное копирование ключевой информации;
- Все случаи, когда нельзя достоверно установить, что произошло с НКИ (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута вероятность того, что данный факт произошел в результате злоумышленных действий).

6.2. При наступлении любого из перечисленных выше событий Владелец ключа должен немедленно прекратить связь с другими абонентами и сообщить о факте компрометации (или предполагаемом факте компрометации) в Удостоверяющий центр, производивший генерацию ключей ЭЦП.

6.3. При подтверждении факта компрометации действующих ключей Пользователь обязан обеспечить немедленное изъятие из обращения скомпрометированных криптографических ключей.

6.4. Для восстановления конфиденциальной связи после компрометации действующих ключей Пользователь получает в Удостоверяющем центре новые ключи ЭЦП.

## 7. Ответственность Пользователя

7.1. Владелец ключа несет персональную ответственность за конфиденциальность личных ключевых носителей.

7.2. В случае неисполнения или ненадлежащего выполнения требований настоящей Инструкции Пользователь несёт ответственность в соответствии с действующим Законодательством Российской Федерации.

Приложение
к Инструкции по обеспечению безопасности эксплуатации
средств криптографической защиты информации (СКЗИ)
в ГБУСО «Новоалександровский КЦСОН»

ЖУРНАЛ
учета средств криптографической защиты информации

количество листов_____

начат_____

окончен_____

| № | Наименование СКЗИ | Серийный номер | Место установки СКЗИ (номера аппаратных средств, в которые установлены СКЗИ) | Ф.И.О. сотрудника, проводившего установку | Дата установки и подписи лиц, произведших установку | Ф.И.О пользователя СКЗИ |
|---|---|---|---|---|---|---|
| 1. | 2. | 3. | 4. | 5. | 6. | 7. |
| 1. | | | | | | |
| 2. | | | | | | |

Приложение № 10
к приказу директора ГБУСО
«Новоалександровский КЦСОН»
от 22 августа 2017 года № 448

**ИНСТРУКЦИЯ**
**по организации хранения, обработки и передачи служебной информации (в том числе персональных данных) на внешних носителях (устройствах) в ГБУСО «Новоалександровский КЦСОН» и за его пределами**

**1. Общие положения**

1.1. Настоящая Инструкция определяет основные требования по организации хранения, обработки и передачи служебной информации (в том числе персональных данных) на внешних носителях (устройствах) в автоматизированной информационной системе государственного бюджетного учреждения социального обслуживания «Новоалександровский комплексный центр социального обслуживания населения» (далее ГБУСО «Новоалександровский КЦСОН») и за ее пределами.

1.2. Под внешним носителем информации подразумевается любое компьютерное оборудование, представляющее собой устройство (оборудованное устройствами) записи, чтения и долговременного хранения данных.

**2. Порядок учета внешних носителей информации допущенных для работы в ГБУСО «Новоалександровский КЦСОН»)**

2.1. Все внешние носители информации или устройства, оборудованные подобными носителями, обязаны учитываться в системе обеспечения информационной безопасности посредством отображения их в соответствующем журнале учета внешних носителей.

2.2. За каждым носителем информации, допущенным к использованию в ГБУСО «Новоалександровский КЦСОН», должен быть закреплен сотрудник учреждения, несущий ответственность за соблюдение правил использования носителя в, ознакомленный с настоящей инструкцией.

2.3. Каждому носителю информации в системе обеспечения информационной безопасности в ГБУСО «Новоалександровский КЦСОН»), должен присваиваться учетный номер.

2.4. Все носители информации, используемые для хранения, обработки и передачи персональных данных, должны обеспечиваться постоянным защищенным местом хранения (сейфом).

2.5. Выдача внешних носителей информации осуществляется работниками ГБУСО «Новоалександровский КЦСОН» после заведения соответствующей записи в журнале учета внешних носителей. Под роспись лица ответственного за эксплуатацию носителя.

**3. Требования, предъявляемые к внешним носителям информации, допущенным к работе в ГБУСО «Новоалександровский КЦСОН»**

3.1. Все внешние носители информации, подключаемые к сети ГБУСО «Новоалександровский КЦСОН», должны быть сертифицированными исходя из требований законодательства РФ. Запрещается использование в ГБУСО «Новоалександровский КЦСОН» любого не сертифицированного оборудования имеющего устройства записи (чтения) и долгосрочного хранения информации.

3.2. Запрещается использование в ГБУСО «Новоалександровский КЦСОН» любого неисправного оборудования имеющего устройства записи (чтения) и долгосрочного хранения информации.

3.3. После каждого использования, с внешнего носителя, используемого для обработки, хранения, передачи персональных данных, информация уничтожается.

**4. Полномочия администратора информационной безопасности**

4.1. Для обеспечения безопасности ЛВС при работе работников ГБУСО «Новоалександровский КЦСОН» с использованием внешних устройств обработки, хранения и передачи информации администратор информационной безопасности:

- обеспечивает доступ к портам ввода-вывода данных (информации) на внешние устройства с помощью имеющихся в его распоряжении аппаратных и программных средств;

- еженедельно анализирует журнал учета событий, регистрируемых средствами защиты локальной вычислительной сети, с целью выявления возможных нарушений прав доступа пользователями при подключении внешних носителей информации к рабочим станциям.

4.2. Администратор информационной безопасности имеет право отключать порты подключения внешних устройств на рабочей станции пользователя, который нарушил требования настоящей Инструкции. До выявления и устранения причин, повлекших нарушение правил эксплуатации внешних устройств хранения, передачи и обработки данных (информации).

4.3. Администратор информационной безопасности имеет право потребовать предоставить внешнее устройство хранения, передачи и обработки информации для проведения как плановой, так и внеплановой проверки на наличие вирусов, других вредоносных программ, а так же качества и уровня обеспечения криптозащиты персональных данных.

Приложение
к Инструкции по организации хранения, обработки и передачи служебной информации (в том числе персональных данных) на внешних носителях (устройствах) в автоматизированной информационной системе ГБУСО «Новоалександровский КЦСОН» и за его пределами

**ПЕРЕЧЕНЬ**
**внешних устройств (носителей информации), используемых в ГБУСО «Новоалександровский КЦСОН»**

| № | Номер носителя в системе учета информационной безопасности АИС | Конфигурация носителя | Могут использоваться для хранения персональных данных |
|---|---|---|---|
| 1 | F001 | Kingston DT101G2 (4GB) | Нет |
| 2 | F002 | Kingston (2GB) | Нет |
| 3 | F003 | Transcend (2GB) | Нет |
| 4 | F004 | Kingston DT101G2 (4GB) | Нет |
| 5 | F005 | Kingston DT101G2 (4GB) | Нет |
| 6 | F006 | Kingston DT101G2 (4GB) | Нет |

Приложение № 11
к приказу директора ГБУСО
«Новоалександровский КЦСОН»
от 22 августа 2017 года № 448

**ИНСТРУКЦИЯ**
**пользователя информационных систем персональных данных по обеспечению безопасности персональных данных в ГБУСО «Новоалександровский КЦСОН»**

## 1. Общие положения

1.1. Пользователь информационной системы персональных данных (далее – Пользователь) осуществляет обработку персональных данных в информационных системах персональных данных в ГБУСО «Новоалександровский КЦСОН».

1.2. Пользователем является каждый работник ГБУСО «Новоалександровский КЦСОН», участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки персональных данных и имеющий доступ к аппаратным средствам, программному обеспечению, персональным данным и средствам защиты информации (далее – пользователь).

1.3. Пользователь несет персональную ответственность за свои действия.

1.4. Пользователь в своей работе руководствуется настоящей Инструкцией, руководящими и нормативными документами Федеральной службы по техническому и экспортному контролю (ФСТЭК) России и другими внутренними нормативно-правовыми актами ГБУСО «Новоалександровский КЦСОН» по защите информации.

## 2. Обязанности пользователя

2.1.. Пользователь обязан:

2.1.1. Знать и выполнять требования законодательства Российской Федерации, нормативных и руководящих документов Федеральной службы по техническому и экспортному контролю, а также организационно-распорядительных документов ГБУСО «Новоалександровский КЦСОН» по вопросам обработки и защиты персональных данных;

2.1.2. Выполнять на автоматизированном рабочем месте (далее – АРМ) только те процедуры обработки персональных данных, которые определены для него должностной инструкцией.

2.1.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности персональных данных, а также руководящих и организационно-распорядительных документов.

2.1.4. Соблюдать требования парольной политики.

2.1.5. Соблюдать правила при работе в сетях общего доступа и международного обмена – Интернет (Раздел 3).

2.1.6. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на нём информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.1.7. Обо всех выявленных нарушениях, связанных с информационной безопасностью в ГБУСО «Новоалександровский КЦСОН», а также для получений консультаций по вопросам информационной безопасности, необходимо обратиться к Администратору информационной системы персональных данных или ответственному за обработку персональных данных.

2.1.8. Для получения консультаций по вопросам работы и настройке элементов информационной системы персональных данных необходимо обращаться к Администратору информационной системы персональных данных.

2.1.9. Принимать меры реагирования в случае возникновения внештатных или аварийных ситуаций с целью ликвидации их последствий в пределах возложенных на него обязанностей.

2.1.10. Пользователям запрещается:

- разглашать защищаемую информацию третьим лицам;
- копировать защищаемую информацию на внешние носители без письменного разрешения директора ГБУСО «Новоалександровский КЦСОН»;
- самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;
- несанкционированно открывать общий доступ к ресурсам;
- запрещено подключать к АРМ и корпоративной информационной сети личные внешние носители и мобильные устройства;

отключать (блокировать) средства защиты информации, в том числе антивирусную защиту;

- обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к информационной системе персональных данных;

– сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам информационной системе персональных данных;

– привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с Администратором информационной системы персональных данных.

2.1.11. При отсутствии визуального контроля за рабочей станцией: доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>

2.1.12. Принимать меры по реагированию в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в рамках возложенных на него функций.

## 3. Правила работы в сетях общего доступа и (или) международного обмена

3.1. Работа в сетях общего доступа и международного обмена (сети Интернет) (далее – Сеть) на элементах информационной системы персональных данных должна проводиться при служебной необходимости.

3.2. При работе в Сети запрещается:

– осуществлять работу при отключенных средствах защиты (антивирус и других);

– передавать по Сети защищаемую информацию без использования средств шифрования;

– запрещается скачивать из Сети программное обеспечение и исполняемые файлы (файлы с расширением exe, dll, msi);

– запрещается посещение сайтов сомнительной репутации (порно-сайты, сайты содержащие нелегально распространяемое ПО и другие);

– запрещается нецелевое использование подключения к Сети.

## 4. Ответственность

4.1 Работники, нарушившие требования данной Инструкции, несут ответственность в соответствии с действующим законодательством.

Приложение № 12
к приказу директора ГБУСО
«Новоалександровский КЦСОН»
от 22 августа 2017 года № 448

**ИНСТРУКЦИЯ**
**по организации парольной защиты**

Настоящая инструкция определяет порядок организации парольной защиты на объекте информатизации «Информационная система персональных данных государственного бюджетного учреждения социального обслуживания «Новоалександровский комплексный центр социального обслуживания населения» (далее - ИСПДн).

**1. Общие положения**

1.1. Настоящая Инструкция предназначена для использования в работе в ИСПДн и определяет порядок обеспечения защиты информации (далее – ЗИ) при использовании подсистемы парольной защиты от несанкционированного доступа (далее – НСД).

1.2. Парольная защита при работе в ИСПДн осуществляется с целью предотвращения НСД к конфиденциальной информации, содержащей персональные данные.

1.3. Парольная защита ИСПДн является составной частью подсистемы управления доступом общей системы защиты от НСД.

К основным видам (категориям) паролей относятся:

пароли BIOS;

пароль доступа средств защиты информации (далее – СЗИ) от НСД;

пароли систем доступа, встроенных в используемые операционные системы (далее – ОС);

пароли доступа к прикладным программам, обеспечивающим доступ к защищаемой информации;

пароли доступа к специализированному программному обеспечению (далее - СПО), предназначенному для работы с защищаемой информацией.

1.4. Порядок работы с паролями вводится с момента подписания данной Инструкции.

**2. Требования к организации парольной защитыобъекта информатизации**

Личные пароли доступа к ИСПДн, СЗИ от НСД ИСПДн, первично назначаются пользователям Администратором информационной системы при формировании персонального идентификатора, при этом необходимо руководствоваться следующими требованиями:

длина пароля должна быть не менее 8 символов;

пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, дни рождения и другие памятные даты, номер телефона, автомобиля, адрес местожительства, наименования ИСПДн, общепринятые сокращения (ЭВМ, ЛВС, USER, SYSOP, GUEST, ADMINISTRATOR и т.д.), и другие данные, которые могут быть подобраны путем анализа информации об ответственном исполнителе;

не использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

не использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т. п.);

при смене пароля новое значение должно отличаться от предыдущего не менее, чем в 5 позициях;

в числе символов пароля могут присутствовать латинские буквы, цифры, символьные знаки;

не использовать ранее использовавшиеся пароли.

2.1. Лица, использующие пароли, обязаны:

четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по использованию парольной защиты;

своевременно сообщать Администратору информационной системы обо всех нештатных ситуациях, нарушениях работы подсистем защиты от НСД, возникающих при работе с паролями.

2.2. При организации парольной защиты запрещается:

записывать свои пароли в очевидных местах (внутренности ящика стола, на мониторе ПЭВМ, на обратной стороне клавиатуры и т.п.);

хранить пароли в записанном виде в рабочих тетрадях, на отдельных листах бумаги;

сообщать посторонним лицам свои пароли, а также сведения о применяемой системе защиты от НСД.

2.2. Специалист, в ведении которого находится ИСПДн, несет личную ответственность за организацию работ по безусловному выполнению требований настоящей инструкции и других документов, регламентирующих использование парольной защиты.

2.3. Ответственность за непосредственную работу с паролями (своевременный ввод, замену и уничтожение) возлагается на Администратора информационной системы.

2.4. На Администратора информационной системы возлагаются следующие задачи:

обеспечение руководства над функционированием системы парольной защиты;

контроль над реализацией требований по обеспечению безопасности информации при использовании паролей и их своевременную смену в ИСПДн.

## 3. Порядок применения парольной защиты

3.1. Порядок применения парольной защиты основанной на использовании СЗИ от НСД приведен в руководствах Администратора БИ и пользователя ИСПДн.

Защита с применением паролей других программно – технических средств и программных продуктов осуществляется, при их наличии, в соответствии с эксплуатационной документацией на эти средства.

Полная плановая смена паролей в ИСПДн проводится регулярно Администратором информационной системы и пользователями, не реже одного раза в 2 (два) месяца.

3.2. Удаление (в т.ч. внеплановая смена) личного пароля должна производиться в следующих случаях:

по окончании срока действия;

в случае прекращения полномочий пользователя (увольнение, переход на другуюработу, не связанную с обработкой персональных данных);

по указанию начальника подразделения или администратора информационной безопасности отдела.

3.3. Пароли, используемые для локального доступа к ресурсам ИСПДн, вводятся пользователем с клавиатуры.

3.4. Компрометация действующих паролей является нештатной ситуацией, о чем администратор информационной системы незамедлительно сообщает руководителю.

3.5. Под компрометацией понимается хищение, утрата действующих паролей, передача или сообщение их лицам, не имеющим на то право, другие действия должностных лиц, приведшие к получению его пароля лицами, не имеющими на то права.

3.6. Скомпрометированные пароли и связанные с ними персональные идентификаторы пользователей выводятся из действия.

Порядок внеплановой смены пароля аналогичен плановой смене паролей.

Приложение № 13
к приказу директора ГБУСО
«Новоалександровский КЦСОН»
от 22 августа 2017 года № 448

**ИНСТРУКЦИЯ**
**по действиям персонала в нештатных ситуациях**

Инструкция по действиям персонала в нештатных ситуациях предназначена для определения порядка действий работников государственного бюджетного учреждения социального обслуживания «Новоалександровский комплексный центр социального обслуживания (далее – ГБУСО «Новоалександровский КЦСОН») при возникновении нештатных ситуаций.

В случае наличия нештатной ситуации порядок действий, при которой не регламентируется настоящей Инструкцией, Администратором информационной безопасности информационных систем персональных данных (далее - АИБ ИСПДн) совместно с директором, вырабатывается конкретный план действий с учетом текущей ситуации.

Для эффективной реализации мероприятий по реагированию в случае нештатных ситуаций должны проводиться регулярные тренировки по различным нештатным ситуациям. По результатам тренировки в случае необходимости проводится уточнение настоящей Инструкции.

Должностные лица ГБУСО «Новоалександровский КЦСОН» знакомятся с основными положениями Инструкции в части их касающейся и по мере необходимости.

Ознакомление с требованиями Инструкции работников ГБУСО «Новоалександровский КЦСОН» осуществляют АИБ ИСПДн под подпись с выдачей электронных копий соответствующих приложений и разделов Инструкции непосредственно для повседневного использования в работе.

Нештатными (кризисными) ситуациям являются:

1. Разглашение конфиденциальной информации, представленной в Перечне сведений конфиденциального характера подлежащих защите в ГБУСО «Новоалександровский КЦСОН» сотрудниками, имеющими к ней право доступа, в том числе:
   - разглашение информации лицам, не имеющим права доступа кзащищаемой информации;
   - передача информации по открытым линиям связи;
   - обработка информации на незащищенных технических средствах обработки информации;
   - опубликование информации в открытой печати и других средствах массовой информации;
   - передача носителя информации лицу, не имеющему права доступа к ней;
   - утрата носителя с информацией.
2. Неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации:
   - несанкционированное изменение информации;
   - несанкционированное уничтожение информации;
   - несанкционированное копирование информации.
3. Несанкционированный доступ к защищаемой информации:
   - подключение технических средств, к системам объекта информатизации;
   - маскировка под зарегистрированного пользователя;
   - использование дефектов программного обеспечения объекта информатизации (ОИ);
   - использование программных закладок;
   - применение программных вирусов;
   - хищение носителя защищаемой информации;
   - нарушение функционирования технических средств (ТС) обработки информации;
4. Дефекты, сбои, отказы, аварии ТС и систем ОИ.
5. Дефекты, сбои и отказы программного обеспечения ОИ.
6. Сбои, отказы и аварии систем обеспечения ОИ.
7. Природные явления, стихийные бедствия:
   - термические, климатические факторы (пожары, наводнения и т. д.);
   - механические факторы (землетрясения и т. д.);
   - электромагнитные факторы (грозовые разряды и т. д.).

**1. Порядок действий при обнаружении нештатных ситуаций**

| Нештатная ситуация | | Оценка ситуации | Действия персонала |
|---|---|---|---|
| Разглашение защищаемой информации сотрудниками, имеющими к ней право доступа | | Обнаружился случившийся факт | 1. Сотрудник учреждения сообщает об инциденте начальнику своего структурного подразделения.<br>2. Создается комиссия по расследованию инцидента. |
| | | Производится в текущий момент | 1. Сотрудник учреждения прерывает несанкционированный процесс.<br>2. Сотрудник учреждения сообщает об инциденте начальнику своего структурного подразделения.<br>3. Создается комиссия по расследованию инцидента. |
| Неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации | Несанкционированное копирование, изменение, уничтожение конфиденциальной информации | Обнаружился случившийся факт | 1. Администратор ИБ блокирует доступ в ИСПДн.<br>2. Начальник структурного подразделения совместно с Администратором ИБ предпринимает действия по сбору и обеспечению сохранности улик.<br>3. Создается комиссия для расследования инцидента. |
| | | Производится в текущий момент | 1. Администратор ИБ прерывает несанкционированный процесс.<br>2. Администратор ИБ блокирует доступ в ИСПДн.<br>3. Начальник структурного подразделения совместно с Администратором ИБ предпринимает действия по сбору и обеспечению сохранности улик.<br>4. Создается комиссия для расследования инцидента. |
| Несанкционированный доступ к защищаемой информации | Подключение технических средств к средствам и системам объекта информатизации (ОИ) | Обнаружился случившийся факт | 1. Администратор ИБ блокирует доступ в ИСПДн для нарушителя.<br>2. Администратор ИБ сообщает об инциденте структурного подразделения.<br>3. При необходимости создается комиссия для расследования инцидента. |
| | | Производится в текущий момент | 1. Администратор ИБ прерывает процесс работы нарушителя.<br>2. Администратор ИБ блокирует доступ в ИСПДн для нарушителя.<br>3. Администратор ИБ сообщает об инциденте начальнику структурного подразделения.<br>4. При необходимости создается комиссия для расследования инцидента. |
| | Маскировка под зарегистрированного пользователя | Внешним злоумышленником в текущий момент | 1. Администратор ИБ прерывает процесс работы нарушителя.<br>2. Администратор ИБ предпринимает действия для задержания нарушителя.<br>3. Администратор ИБ сообщает об инциденте начальнику структурного подразделения.<br>4. Создается комиссия для расследования инцидента с привлечением правоохранительных органов. |
| | | Внутренним злоумышленником, либо производилась в прошлом | 1. Администратор ИБ прерывает процесс работы нарушителя.<br>2. Администратор ИБ сообщает об инциденте начальнику структурного подразделения.<br>3. Создается комиссия для расследования инцидента. |
| | Использование дефектов программного обеспечения ОИ | Внешним злоумышленником в текущий момент | 1. Администратор ИБ прерывает процесс работы нарушителя.<br>2. Администратор ИБ блокирует доступ в ИСПДн для нарушителя.<br>3. Администратор ИБ сообщает об инциденте начальнику структурного подразделения.<br>4. При необходимости создается комиссия для расследования инцидента. |

| Нештатная ситуация | | Оценка ситуации | Действия персонала |
|---|---|---|---|
| | | Внутренним злоумышленником, либо производилось в прошлом | 1. Администратор ИБ прерывает процесс работы нарушителя.<br>2. Администратор ИБ блокирует доступ в ИСПДн для нарушителя.<br>3. Администратор ИБ сообщает об инциденте начальнику структурного подразделения.<br>4. При необходимости создается комиссия для расследования инцидента. |
| | Использование программных закладок | Внешним злоумышленником в текущий момент | 1. Администратор ИБ прерывает процесс работы нарушителя.<br>2. Администратор ИБ блокирует доступ в ИСПДн для нарушителя.<br>3. Администратор ИБ определяет возможный ущерб, нанесенный программной закладкой.<br>4. Администратор ИБ составляет акт об инциденте. |
| | | Внутренним злоумышленником, либо производилось в прошлом | 1. Администратор ИБ прерывает процесс работы нарушителя.<br>2. Администратор ИБ блокирует доступ в ИСПДн для нарушителя.<br>3. Администратор ИБ определяет возможный ущерб, нанесенный программной закладкой<br>4. Администратор ИБ составляет акт об инциденте. |
| | Обнаружение программных вирусов | | 1. Администратор ИБ прерывает процесс работы ИСПДн.<br>2. Администратор ИБ определяет возможный ущерб, нанесенный программно-математическим воздействием.<br>3. Администратор ИБ проводит контроль ИСПДн в соответствии с инструкцией по организации антивирусной защиты.<br>4. Администратор ИБ составляет акт об инциденте. |
| | Хищение носителя защищаемой информации | | Создается комиссия для расследования инцидента. |
| | Нарушение функционирования ТС обработки информации злоумышленником | Производится в текущий момент | 1. Администратор ИБ принимает меры по немедленному удалению злоумышленника от средств вычислительной техники.<br>2. В случае если злоумышленник является пользователем системы, Администратор ИБ блокирует доступ к ИСПДн для злоумышленника.<br>3. В случае наличия повреждений Администратор ИБ определяет ущерб, нанесенный ТС и информации.<br>4. Администратор ИБ производит восстановление работоспособности системы.<br>5. Создается комиссия для расследования инцидента |
| | | Обнаружился случившийся факт | 1. В случае наличия повреждений Администратор ИБ определяет возможный круг лиц, причастных к нарушению, ущерб, нанесенный ТС и информации.<br>2. Администратор ИБ производит восстановление работоспособности системы.<br>3. Создается комиссия для расследования инцидента |

| Нештатная ситуация | Оценка ситуации | Действия персонала |
|---|---|---|
| Ошибки пользователей системы при эксплуатации программных средств, ТС, средств и систем защиты информации | Ошибка повлекла утерю, повреждение защищаемой информации или привела к нарушению работоспособности | 1. Администратор ИБ проводит анализ и идентификацию причин инцидента.<br>2. В случае возможности злоумышленных действий выполняется последовательность действий, предусмотренная в соответствующем разделе Инструкции.<br>3. Администратор ИБ определяет ущерб, нанесенный нештатной ситуацией.<br>4. Администратор ИБ проводит мероприятия по восстановлению работоспособности системы и информации.<br>5. Проводится проверка знаний сотрудника виновного в инциденте, а в случае необходимости его обучение.<br>6. Администратор ИБ составляет акт об инциденте, в случае необходимости выносят предложение начальнику структурного подразделения о применении дисциплинарной меры в отношении нарушителя. |
| | ТС и ПО | |
| Дефекты, сбои, отказы, аварии ТС, программных средств и систем ОИ | | 1. Администратор ИБ выявляют возможные причины проявления дестабилизирующих факторов.<br>2. В случае наличия злоумышленных действий выполняется порядок действий соответствующего раздела Инструкции.<br>3.Администратор БИ восстанавливает работоспособность систем.<br>4. В случае потери данных Администратором БИ по возможности проводится восстановление их из резервных копий.<br>5. Администратором ИСПДн производится составление акта |
| Сбои, отказы и аварии систем обеспечения ОИ | | 1. В случае если наблюдается продолжительное отключение электропитания. Администратором БИ производится отключение серверов до момента истечения резервов системы бесперебойного питания.<br>2. Ответственным за материально-техническое обеспечение организуются работы по максимально быстрому восстановлению систем обеспечения.<br>3. В случае потери защищаемых данных Администратором БИ по возможности проводится восстановление их из резервных копий.<br>4. В случае отключения электропитания в выходные и праздничные дни, работники охраны обязаны доложить об отключении руководству и лицу, ответственному за функционирование объекта информатизации. |

## 2. Порядок действий по защите информации и носителей при возникновении пожара

В целях противопожарной подготовки работников, ответственный за противопожарные мероприятия по согласованию со своим непосредственным руководителем:

разрабатывает план эвакуации носителей информации, средств вычислительной техники и имущества;

определяет очередность эвакуации (в первую очередь подлежат эвакуации и охране носители защищаемой информации и технические средства ее обработки);

определяет места складирования эвакуированного имущества и порядок его охраны;

разрабатывает пожарный расчет работников подразделения в соответствии со штатным расписанием и инструкции на случай пожара номерам расчета;

организует взаимодействие с ответственными за противопожарное состояние других подразделений, размещаемых в здании, по оповещению руководства в случае возникновения пожара (особенно во внерабочее время);

организует обучение работников.

При возникновении пожара в помещениях в рабочее время сотрудник подразделения:

немедленно сообщает руководителю подразделения (в его отсутствии - старшему по штатному расписанию);

оповещает работников подразделения;

приступает в соответствии с обязанностями по пожарному расчету или по указанию руководства к ликвидации очага возгорания, эвакуации закрепленных за ним носителей информации и средств вычислительной техники, их охране;

АИБ ИСПДн:

контролирует очередность эвакуации БД и в автоматизации (по возможности) и непосредственно организует охрану носителей в местах эвакуации;

руководитель звена пожаротушения:

осуществляет общее руководство тушением пожара, эвакуацией имущества и персонала;

руководит действиями работников в соответствии с утвержденным пожарным расчетом;

При возникновении пожара в помещениях в нерабочее время руководитель подразделения или лицо его замещающее (первый из прибывших старший по штатному расписанию):

вызывает должностное лицо соответствующего подразделения и работников согласно пожарному расчету;

уточняет место складирования и организует во взаимодействии с пожарным подразделением эвакуацию носителей защищаемой информации и технических средств ее обработки;

организует их охрану;

назначает комиссию по проверке наличия служебных документов;

сообщает о происшествии и результатах проверки АИБ ИСПДн.

## 3. Общий порядок действий

При обнаружении любых нештатных ситуаций, которые повлекли утечку или повреждение защищаемой информации, либо созданы внутренним злоумышленником, создается комиссия.

При нештатных ситуациях, связанных с:

разглашением конфиденциальной информации;

обнаружением несанкционированно скопированной или измененной конфиденциальной информации;

обнаружением подключения технических средств системам объекта информатизации;

маскировкой под зарегистрированного пользователя внутренним злоумышленником или обнаружением факта маскировки в прошлом (как внутренним, так и внешним злоумышленником);

использованием дефектов программного обеспечения ОИ внутренним злоумышленником или обнаружением факта их использования в прошлом (как внутренним, так и внешним злоумышленником);

использованием программных закладок внутренним злоумышленником или обнаружением факта их использования в прошлом (как внутренним, так и внешним злоумышленником);

хищением носителя защищаемой информации.

в первую очередь АИБ предпринимаются действия по сбору и обеспечению сохранности улик незаметно для злоумышленника.

Комиссия, дополнительно к общему порядку должна:

если это возможно, локализовать место где, произошла утечка конфиденциальной информации;

определить возможные контрмеры, призванные уменьшить потери от утечки информации.

## 4. Производство расследований

Для расследования опасных ситуаций в случаях предусмотренных настоящей Инструкцией пораспоряжению директора ГБУСО «Новоалександровский КЦСОН»создаваться комиссия. В состав комиссии должны входить:

председатель;

АИБ;

юрисконсульт;

инспектор по кадрам;

другие лица по решению директора учреждения.

Деятельность комиссии должна по возможности происходить в режиме строгой конфиденциальности.

В общем случае комиссия проводит:

анализ и идентификацию причин инцидента, определение виновных;

определение ущерба, нанесенного нештатной ситуацией;

планирование мер для предотвращения повторения, нейтрализации последствий (если это возможно);

анализ и сохранение доказательств, следов инцидента, улик и свидетельств;

определение меры взыскания с виновного;

взаимодействие, при необходимости, с правоохранительными органами.

При сохранении улик:

если есть возможность, АИБ производится резервное копирование системной и защищаемой информации технических средств вовлеченных в инцидент,включая журналы событий (контрольные записи);

По результатам деятельности комиссии составляется акт с описанием ситуации. К акту прилагаются поясняющие материалы (копии экрана, распечатки журнала событий, и др.).

По результатам расследования администраторами организуются мероприятия по реализации предложенных комиссией мер для предотвращения либо уменьшения вероятности появления, подобных инцидентов в дальнейшем.

При проведении расследований, кроме того, необходимо ответить на следующие вопросы:

можно ли было предусмотреть нештатную ситуацию?

вызвана ли она слабостью средств защиты и регистрации?

это первая кризисная ситуация такого рода?

достаточно ли имеющегося резерва?

есть ли необходимость пересмотра системы защиты?

есть ли необходимость пересмотра настоящей инструкции?

## 5. Ответственные за контроль выполнения инструкции

Ответственным за постоянный контроль выполнения требований данной Инструкции является:

АИБ в части задач, возложенных на него настоящей инструкцией.

ответственный за материально-техническое обеспечение в части задач, возложенных на него настоящей инструкцией.

## 6. Порядок пересмотра инструкции

Инструкция подлежит полному пересмотру при изменении приоритетов угроз безопасности ИСПДнс целью проверки соответствия положений данного документа реальным условиям применения их в ИСПДн.

Инструкция подлежит частичному пересмотру в следующих случаях:

при изменении местоположения, состава и объема информационных ресурсов, подлежащих резервному копированию;

при определении такой необходимости комиссией по результатам расследования нештатной ситуации;

в целях повышения эффективности мероприятий, определенных в настоящей инструкции;

при изменении состава, обязанностей и полномочий должностных лиц ГБУСО «Новоалександровский КЦСОН», которые задействованы в мероприятиях настоящей Инструкции.

Полный пересмотр данного документа проводится АИБ ИСПДнс целью проверки соответствия определенных данным документом мер защиты реальным условиям применения их в ИСПДн.

## 7. Средства обеспечения непрерывной работы и восстановления

Резервному копированию (РК) подлежит следующая информация:

системные программы и наборы данных -не возобновляемому (однократному, эталонному) РК;

прикладное программное обеспечение и наборы данных – не возобновляемому РК;

наборы данных, генерируемые в течение рабочего дня и содержащие ценную информацию (журналы транзакций, системный журнал и т.д.) - периодическому возобновляемому РК.

Резервному копированию в ИСПДн подлежат следующие программные и информационные ресурсы управления:

| Наименование информационного ресурса | Где размещается ресурс в системе | Вид резервного копирования | Ответственный за резервное копирование (используемые технические средства) | Где хранится резервная копия | Частота периодического резервирования |
|---|---|---|---|---|---|
| Информация пользователей | Определяется АИБ | Периодическое, возобновляемое | АИБ | | Определяется АИБ |
| Защищаемые ресурсы | Определяется АИБ | Периодическое, возобновляемое | АИБ | | Определяется АИБ |
| Эталонное программное обеспечение | Вне системы на магнитных, либо оптических носителях | Не возобновляемое | АИБ | | Обновляется при появлении нового ПО |

**8. Планобеспечения непрерывной работы и восстановления информации**

| Тип кризисной ситуации | Критерии кризисной ситуации | Кому и в какие сроки докладывается | | Срок реализации первоочередных действий | Максимальное время для выполнения всех мероприятий |
|---|---|---|---|---|---|
| | | В рабочее время | В нерабочее время | | |
| Неправомерные действия со стороны лиц, допущенных к защищаемой информации | | | | | |
| Разглашение защищаемой информации сотрудниками, имеющими к ней право доступа | | АИБ сразу после обнаружения инцидента | АИБ как можно скорее, в дневное время, но не позднее 8 часов после инцидента | | |
| Обнаружение несанкционированно скопированной или измененной конфиденциальной информации | | АИБ сразу после обнаружения инцидента | АИБ как можно скорее, в дневное время, но не позднее 8 часов после инцидента | | |
| Несанкционированное копирование или изменение конфиденциальной информации в текущий момент времени со стороны лиц имеющих право доступа к ней | | АИБ сразу после обнаружения инцидента | АИБ сразу после обнаружения инцидента | 10 минут в рабочее время (1 час в нерабочее) | |
| Несанкционированный доступ к информации | | | | | |
| Обнаружение подключения технических средств к средствам и системам объекта информатизации | | АИБ сразу после обнаружения инцидента | АИБ как можно скорее, в дневное время, но не позднее 8 часов после инцидента | | |
| Подключение технических средств к средствам и системам ОИ в текущий момент времени | | АИБ сразу после обнаружения инцидента | АИБ сразу после обнаружения инцидента | 10 минут в рабочее время (1 час в нерабочее) | |
| Маскировка под зарегистрированного пользователя внешним злоумышленником в текущий момент времени | | АИБ сразу после обнаружения инцидента | АИБ сразу после обнаружения инцидента | 5 минут в рабочее время (1 час в нерабочее) | |
| Маскировка под зарегистрированного пользователя внутренним злоумышленником или обнаружением факта маскировки | | АИБ сразу после обнаружения инцидента | АИБ как можно скорее, в дневное время, но не позднее 8 часов после инцидента | | |

| Тип кризисной ситуации | Критерии кризисной ситуации | Кому и в какие сроки докладывается | | Срок реализации первоочередных действий | Максимальное время для выполнения всех мероприятий |
|---|---|---|---|---|---|
| | | В рабочее время | В нерабочее время | | |
| Использование дефектов программного обеспечения ОИ внешним нарушителем в текущий момент времени | | АИБ сразу после обнаружения инцидента | АИБ сразу после обнаружения инцидента | 10 минут в рабочее время (1 час в нерабочее) | |
| Использование программных закладок внешним нарушителем в текущий момент времени | | АИБ сразу после обнаружения инцидента | АИБ сразу после обнаружения инцидента | 10 минут в рабочее время (1 час в нерабочее) | |
| Использование программных закладок внутренним злоумышленником или обнаружение факта использования | | АИБ сразу после обнаружения инцидента | АИБ как можно скорее, в дневное время, но не позднее 8 часов после инцидента | | |
| Обнаружение программных вирусов | | АИБ сразу после обнаружения инцидента | АИБ как можно скорее, в дневное время, но не позднее 8 часов после инцидента | | 12 часов |
| Хищение носителя защищаемой информации | | АИБ сразу после обнаружения инцидента | АИБ как можно скорее, в дневное время, но не позднее 8 часов после инцидента | | |
| Нарушение функционирования ТС обработки информации в текущий момент времени злоумышленником | Нарушена работа одного пользователя | АИБ сразу после обнаружения инцидента | АИБ сразу после обнаружения инцидента | 10 минут в рабочее время (1 час в нерабочее) | 2 дня |
| | Нарушена работа группы пользователей | АИБ сразу после обнаружения инцидента | АИБ сразу после обнаружения инцидента | 10 минут в рабочее время (1 час в нерабочее) | 1 день |
| Обнаружение нарушения функционирования ТС обработки информации произведенного злоумышленником | Нарушена работа одного пользователя | АИБ сразу после обнаружения инцидента | АИБ сразу после обнаружения инцидента | | 2 дня |
| | Нарушена работа группы пользователей | АИБ сразу после обнаружения инцидента | АИБ сразу после обнаружения инцидента | | 1 день |
| Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку | | | | | |

| Тип кризисной ситуации | Критерии кризисной ситуации | Кому и в какие сроки докладывается | | Срок реализации первоочередных действий | Максимальное время для выполнения всех мероприятий |
|---|---|---|---|---|---|
| | | В рабочее время | В нерабочее время | | |
| Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку внешним злоумышленником в текущий момент времени | | АИБ сразу после обнаружения инцидента | АИБ как можно скорее, в дневное время, но не позднее 8 часов после инцидента | 20 минут в рабочее время (1 час в нерабочее) | 7 дней |
| Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку внутренним злоумышленником в текущий момент времени | | АИБ сразу после обнаружения инцидента | АИБ как можно скорее, в дневное время, но не позднее 8 часов после инцидента | 20 минут в рабочее время (1 час в нерабочее) | 1 день |
| Обнаружение произошедшего факта блокировки доступа к защищаемой информации | | АИБ сразу после обнаружения инцидента | АИБ как можно скорее, в дневное время, но не позднее 8 часов после инцидента | | 1 день |
| Ошибки пользователей системы | | | | | |
| Ошибки пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие утерю или повреждение защищаемой информации | | АИБ сразу после обнаружения инцидента | АИБ как можно скорее, в дневное время, но не позднее 8 часов после инцидента | 2 часа в рабочее время (12 часов в нерабочее) | 1 день |
| Ошибки пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие нарушение работоспособности ТС и ПО | Нарушена работа одного пользователя | АИБ сразу после инцидента | АИБ в первый рабочий день после инцидента | 20 минут | 2 дня |
| | Нарушена работа группы пользователей | АИБ сразу после обнаружения инцидента | АИБ сразу после обнаружения инцидента | 20 минут | 1 день |

| Тип кризисной ситуации | Критерии кризисной ситуации | Кому и в какие сроки докладывается | | Срок реализации первоочередных действий | Максимальное время для выполнения всех мероприятий |
|---|---|---|---|---|---|
| | | В рабочее время | В нерабочее время | | |
| Объективные факторы | | | | | |
| Дефекты, сбои, отказы, аварии ТС, программных средств и систем ОИ | Сбой ТС и систем ОИ | АИБ сразу после инцидента | АИБ сразу после инцидента | 1 час | 2 дня |
| | Отказ ТС и систем ОИ, затронувший работу группы пользователей | АИБ сразу после обнаружения инцидента | АИБ как можно скорее, в дневное время, но не позднее 8 часов после инцидента | 1 час в рабочее время (8 часов в нерабочее) | 1 день |
| | Отказ ТС и систем ОИ, затронувший работу одного пользователя | АИБ сразу после инцидента | АИБ в первый рабочий день после инцидента | 1 час | 2 дня |
| | Авария ТС и систем ОИ | АИБ сразу после обнаружения инцидента | АИБ как можно скорее, в дневное время, но не позднее 8 часов после инцидента | 1 час | 1 день |
| Сбои, отказы и аварии систем обеспечения ОИ | Сбой систем обеспечения ОИ | Ответственному за материально-техническое обеспечение сразу после инцидента | Ответственному за материально-техническое обеспечение в первый рабочий день после инцидента | | |
| | Отказ систем обеспечения ОИ, затронувший работу группы пользователей | Ответственному за материально-техническое обеспечение и АИБ сразу после обнаружения инцидента | Ответственному за материально-техническое обеспечение и АИБ сразу после обнаружения инцидента | | 1 день |

| Тип кризисной ситуации | Критерии кризисной ситуации | Кому и в какие сроки докладывается | | Срок реализации первоочередных действий | Максимальное время для выполнения всех мероприятий |
|---|---|---|---|---|---|
| | | В рабочее время | В нерабочее время | | |
| | Отказ систем обеспечения ОИ, затронувший работу одного пользователя | Ответственному за материально-техническое обеспечение сразу после инцидента | Ответственному за материально-техническое обеспечение в первый рабочий день после инцидента | | 2 дня |
| | Авария систем обеспечения ОИ | Ответственному за материально-техническое обеспечение, АИБ сразу после обнаружения инцидента | Ответственному за материально-техническое обеспечение, АИБ как можно скорее, в дневное время, но не позднее 8 часов после инцидента | | 1 день |
| Природные явления, стихийные бедствия, несущие угрозу жизни человека | | Руководителю, заместителям руководителя, которые оповещают всех своих работников сразу после получения информации | Руководителю, заместителям руководителя, которые оповещают всех своих работников сразу после получения информации | | 30 минут |
| Природные явления, стихийные бедствия, не несущие угрозу жизни человека | | Руководителю, заместителям руководителя, Администратору БИ | Руководителю, заместителям руководителя, Администратору БИ | | 30 минут |

**9. Журнал учета нештатных ситуаций**
**Список нештатных ситуаций**

| № | Нештатная ситуация |
|---|---|
| Разглашение конфиденциальной информации, представленной в перечне сведений конфиденциального характера подлежащих защите в ГБУСО «Новоалександровский КЦСОН», сотрудниками учреждения , имеющими к ней право доступа: | |
| 1 | Разглашение информации лицам, не имеющим права доступа к защищаемой информации |
| 2 | Передача информации по открытым линиям связи |
| 3 | Обработка информации на незащищенных технических средствах обработки информации |
| 4 | Опубликование информации в открытой печати и других средствах массовой информации |
| 5 | Передача носителя информации лицу, не имеющему права доступа к ней |
| 6 | Утрата носителя с информацией |
| Неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации: | |
| 7 | Несанкционированное изменение информации |
| 8 | Несанкционированное уничтожение информации |
| 9 | Несанкционированное копирование информации |
| Несанкционированный доступ к защищаемой информации: | |
| 10 | Подключение технических средств к средствам и системам объекта информатизации |
| 11 | Маскировка под зарегистрированного пользователя |
| 12 | Использование дефектов программного обеспечения объекта информатизации |
| 13 | Использование программных закладок |
| 14 | Обнаружение программных вирусов |
| 15 | Хищение носителя защищаемой информации |
| 16 | Нарушение функционирования технических средств обработки информации |
| 17 | Дефекты, сбои, отказы, аварии технических средств и систем объекта информатизации |
| 18 | Дефекты, сбои и отказы программного обеспечения объекта информатизации |
| 19 | Сбои, отказы и аварии систем обеспечения объекта информатизации |
| Природные явления, стихийные бедствия: | |
| 20 | Термические, климатические факторы (пожары, наводнения и т. д |
| 21 | Механические факторы (землетрясения и т. д.); |
| 22 | Электромагнитные факторы (грозовые разряды и т. д.). |

| № п/п | Дата | Нештатная ситуация | Выполненные работы | Подпись исполнителя | Подпись администратора ИБ |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

## 10. База данных нештатных ситуаций

Для ведения единой базы информации о нештатных ситуациях АИБ создается электронная база данных.

Доступ к созданной базе данных должны иметь АИБ и другие должностные лица ГБУСО «Новоалександровский КЦСОН», задействованные в выполнении положений настоящей Инструкции.

Участвовавшим в нейтрализации нештатной ситуации АИБ, а в случае его неучастия либо отсутствия, другими лицами создается запись в электронной базе данных нештатных ситуаций. Запись создается по происшествию не более 8 часов после инцидента.

Электронная база данных ежегодно анализируется АИБ и директором ГБУСО «Новоалександровский КЦСОН».

Записи о нештатных ситуациях должны иметь следующую форму:

Вид нештатной ситуации: Могут быть указаны следующие виды нештатной ситуации:

неправомерные действия со стороны лиц, допущенных к защищаемой информации;

несанкционированный доступ к информации;

блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками;

ошибки пользователей системы;

объективные факторы.

Тип: общее название нештатной ситуации в соответствии с названием подраздела настоящей Инструкции.

Описание: детализация нештатной ситуации, например, обрыв канала связи в Internet и т.п.

Документы по нештатной ситуации: номера актов, протоколов и т.п. нештатной ситуации. Если это возможно электронные копии документов.

Приложение № 14
к приказу директора ГБУСО
«Новоалександровский КЦСОН»
от 22 августа 2017 года № 448

**ПОРЯДОК**
**доступа сотрудников ГБУСО «Новоалександровский КЦСОН» в помещения, в которых ведётся обработка персональных данных**

## 1. Общие положения

1.1. Настоящий Порядок определяет процедуру доступа сотрудников Государственного бюджетного учреждения социального обслуживания «Новоалександровский комплексный центр социального обслуживания населения» (далее – Учреждение) в помещения, в которых ведётся обработка персональных данных и разработан в соответствии с постановлением Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных».

1.2. Целью настоящего Порядка является обеспечение исключения неправомерного или случайного доступа к материальным носителям персональных данных и техническим средствам их обработки, а также иных неправомерных действий в отношении персональных данных.

## 2. Порядок доступа в помещения, в которых ведётся обработка персональных данных

2.1. Доступ сотрудников ГБУСО «Новоалександровский КЦСОН» в помещения, в которых ведется обработка персональных данных, осуществляется согласно перечню перечень должностей сотрудников ГБУСО «Новоалександровский КЦСОН», допущенных к обработке персональных данных, утвержденным приказом директора.

2.2. Допуск в помещения, в которых ведется обработка персональных данных, иных лиц, осуществляется сотрудниками, указанными в Разрешительной системе доступа сотрудников ГБУСО «Новоалександровский КЦСОН» в помещения, в которых ведется обработка персональных данных. Пребывание посторонних лиц в кабинетах, в которых ведется обработка персональных данных, допускается только в присутствии сотрудников, указанных в Разрешительной системе доступа сотрудников ГБУСО «Новоалександровский КЦСОН», допущенных в помещения, в которых ведется обработка персональных данных.

2.3. Работники контролирующих органов допускаются в помещение (отделения), в котором ведется обработка персональных данных, при наличии соответствующего предписания на проведение контрольных мероприятий с разрешения руководителя ГБУСО «Новоалександровский КЦСОН» (лица, его замещающего) в его присутствии или лица, его замещающего.

2.4. Работники сторонних организаций, прибывшие в помещение, в котором ведется обработка персональных данных, для выполнения работ, оказания услуг в соответствии с заключенными ГБУСО «Новоалександровский КЦСОН» государственными контрактами (договорами) допускаются в помещение с разрешения руководителя ГБУСО «Новоалександровский КЦСОН» (лица его замещающего) на основании информации, полученной от юрисконсульта, ответственного за организацию и выполнение работ по государственному контракту (договору).

2.5. При проведении таких работ работники отделения обязаны принять меры по исключению ознакомления работников сторонних организаций с персональными данными.

## 3. Запрещается

3.1. Запрещается оставлять помещения, в которых ведётся обработка персональных данных, без присмотра работников, имеющих допуск в помещения, где ведётся обработка персональных данных.

3.2. Запрещается оставлять без присмотра находящихся в помещении, в которых ведётся обработка персональных данных, посторонних лиц, а также, работников, не имеющих допуск в помещения, в которых ведётся обработка персональных данных.

## 4. Внутренний контроль

4.1. Внутренний контроль за соблюдением порядка доступа в помещения, в которых ведётся обработка персональных данных, осуществляется лицом, ответственным за обработку персональных данных.

## 5. Ответственность

5.1. Работники, нарушившие нормы настоящего Порядка, несут ответственность в соответствии с действующим законодательством

Приложение № 15
к приказу директора ГБУСО
«Новоалександровский КЦСОН»
от 22 августа 2017 года № 448

**ПРАВИЛА**
**работы с обезличенными персональными данными в ГБУСО «Новоалександровский КЦСОН»**

## 1. Общие положения

1.1. Настоящие Правила работы с обезличенными персональными данными в ГБУСО «Новоалександровский КЦСОН» разработаны в соответствии с Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных», постановлением Правительства РФ от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами ГБУСО «Новоалександровский КЦСОН»

1.2. Настоящие Правила определяют порядок работы с обезличенными персональными данными в ГБУСО «Новоалександровский КЦСОН».

## 2. Термины и определения

2.1. Персональные данные – любая информация, относящаяся прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных).

2.2. Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

2.3. Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

2.4. Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

2.5. Конфиденциальность персональных данных – обязательное для соблюдения оператора или иных лиц, получивших доступ к персональным данным, требование не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

2.6. Обезличивание персональных данных проводится с целью ведения статистических данных и снижения ущерба от разглашения защищаемых персональных данных.

## 3. Цели и методы обезличивания

3.1. Обезличивание персональных данных в ГБУСО «Новоалександровский КЦСОН» может быть проведено с целью повышения безопасности персональных данных, защиты от несанкционированного использования, ведения статистических данных, ведения бухгалтерского и кадрового учета, снижения ущерба от разглашения защищаемых персональных данных, снижения класса защищенности информационных систем персональных данных (далее - ИСПДн).

3.2. Методы обезличивания персональных данных в соответствии с «Методические рекомендации по применению приказа Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»:

- введения идентификаторов (замена части персональных данных идентификаторами с созданием таблиц (справочников) соответствия идентификаторов исходным данным);
- изменения состава или семантики (изменение состава или семантики
персональных данных путем замены результатами статистической обработки, обобщения или удаления части сведений);
- декомпозиции (разбиение персональных данных на несколько частей с последующим их раздельным хранением);
- перемешивания (перестановка отдельных записей, а так же групп записей в массиве персональных данных);
- другие методы обезличивания, исходя из целей обезличивания.

## 4. Порядок работы с обезличенными персональными данными

4.1. Мероприятия по обезличиванию персональных данных проводят работники, ответственные за обработку персональных данных.

4.2. Обезличенные персональные данные могут обрабатываться как автоматизированным так и не автоматизированным способами.

4.3. Обработка обезличенных персональных данных осуществляется с соблюдением конфиденциальности.

4.4. При работе с обезличенными персональными данными в автоматизированном и не автоматизированном режимах необходимо соблюдать правила и требования по обеспечению безопасности персональных данных, действующие в ГБУСО «Новоалександровский КЦСОН».

4.5. Передача обезличенных персональных данных третьим лицам разрешается с письменного разрешения директора ГБУСО «Новоалександровский КЦСОН», либо без такового в случаях, предусмотренных действующим законодательством.

## 5. Ответственность

5.1. Лица, нарушившие настоящие Правила, несут ответственность в соответствии с действующим законодательством.

Приложение № 16
к приказу директора ГБУСО
«Новоалександровский КЦСОН»
от 22 августа 2017 года № 448

**ПРАВИЛА**
**рассмотрения запросов субъектов персональных данных или их представителей на получение информации, касающейся обработки его персональных данных, обращений уполномоченного органа по защите прав субъектов персональных данных в ГБУСО «Новоалександровский КЦСОН»**

**1.1. Общие положения**

1.1. Настоящие Правила определяют порядок рассмотрения в ГБУСО «Новоалександровский КЦСОН» (далее – Учреждение) запросов субъектов персональных данных или их представителей на получение информации, касающейся обработки персональных данных заявителя, а также обращений уполномоченного органа по защите прав субъектов персональных данных.

1.2. Настоящие Правила разработаны в соответствии с Федеральными законами от 27.07.2006 № 152-ФЗ «О персональных данных», 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», Трудовым кодексом Российской Федерации, Постановлениями Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативными правовыми актами и инструкциями в области защиты информации ГБУСО «Новоалександровский КЦСОН».

**2. Термины и определения**

1.1. Персональные данные - любая информация, прямо или косвенно относящаяся к определенному или определяемому физическому лицу (субъекту персональных данных);

1.2. Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

1.3. Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

1.4. Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

1.5. Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

1.6. Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

1.7. Заявитель - субъект персональных данных (физическое лицо) или его представитель.

1.8. Запрос – обращение заявителя в ГБУСО «Новоалександровский КЦСОН» в письменной форме или в форме электронного документа, заявление или жалоба, а также устное обращение заявителя, либо обращение уполномоченного органа по защите прав субъектов персональных данных.

**3. Права заявителя на доступ к его персональным данным**

3.1. Заявитель имеет право на получение информации, касающейся обработки его персональных данных, содержащей:

1) подтверждение факта обработки персональных данных Учреждением;

2) правовые основания и цели обработки персональных данных;

3) применяемые способы обработки персональных данных;

4) наименование и место нахождения Учреждения, осуществляющего обработку персональных данных;

5) сведения о лицах (за исключением работников Учреждения), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Учреждением или на основании федерального закона;

5) обрабатываемые персональные данные, относящиеся к заявителю, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

6) сроки обработки персональных данных, сроки их хранения;

7) порядок осуществления заявителем прав, предусмотренных настоящим Федеральным законом;

8) информацию об осуществленной или о предполагаемой трансграничной передаче персональных данных;

9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего

обработку персональных данных по поручению Учреждения, если обработка поручена или будет поручена такому лицу;

10) иные сведения, предусмотренные нормативными правовыми актами в области защиты персональных данных.

3.2. Право заявителя на доступ к его персональным данным может быть ограничено в соответствии с частью 8 статьи 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

3.3. Заявитель вправе требовать от Учреждения уточнения его персональных

данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

3.4. Сведения, указанные в пункте 3.1. настоящих Правил, должны быть предоставлены заявителю в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

3.5. Запрос должен содержать номер основного документа, удостоверяющего личность заявителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие заявителя в отношениях с Учреждением (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Учреждением, подпись заявителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

3.6. В случае, если сведения, указанные в пункте 3.1. настоящих Правил, а также обрабатываемые персональные данные были предоставлены для ознакомления заявителю по его запросу, заявитель вправе обратиться повторно в Учреждение или направить повторный запрос в целях получения сведений и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является заявитель.

3.7. Заявитель вправе обратиться повторно в Учреждение или направить повторный запрос в целях получения сведений, указанных в пункте 3.1. настоящих Правил, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в пункте 3.6. настоящих Правил, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в пункте 3.5. настоящих Правил, должен содержать обоснование направления повторного запроса.

3.8. Учреждение вправе отказать заявителю в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 3.6, 3.7. настоящих Правил. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Учреждении.

## 4. Права уполномоченного органа по защите прав субъектов персональных данных при рассмотрении обращения заявителя

4.1. Уполномоченный орган по защите прав субъектов персональных

данных имеет право:

- запрашивать у Учреждения информацию необходимую для реализации своих полномочий, и безвозмездно получать такую информацию;
- проводить проверки соблюдения обязательных требований в сфере обработки персональных данных;
- требовать от Учреждения уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;
- принимать в установленном законодательством Российской Федерации порядке меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований федеральных законов.

4.2. Учреждение обязано сообщить в уполномоченный орган по защите прав субъектов персональных данных по его запросу необходимую информацию в

течение тридцати дней с даты получения такого запроса.

4.3. Учреждение обязано принять необходимые меры по устранению нарушений, выявленных в ходе проведения проверки соблюдения обязательных требований в сфере обработки персональных данных и выполнения требований уполномоченного органа по защите прав субъектов персональных данных.

## 5. Обязанности Учреждения при обращении заявителя

5.1. Все запросы заявителей в Учреждение на получение информации, касающейся обработки его персональных данных, подлежат регистрации и учету.

5.2. Учреждение обязано сообщить заявителю информацию о наличии персональных данных, относящихся к нему, а также предоставить возможность ознакомления с ними в течение тридцати дней со дня обращения заявителя, либо с даты получения запроса.

5.3. В случае отказа в предоставлении заявителю информации о наличии персональных данных о нем, Учреждение обязано предоставить в письменной форме мотивированный ответ в срок, не превышающий тридцати дней со дня обращения заявителя, либо с даты получения запроса.

5.4. Предоставление информации о наличии персональных данных заявителя осуществляется безвозмездно.

5.5. Учреждение обязано, при предоставлении заявителем информации, подтверждающей, что его персональные данные являются неполными, неточными или неактуальными, внести в них необходимые изменения в срок, не превышающий семи рабочих дней со дня поступления информации.

5.6. Учреждение обязано при предоставлении заявителем информации, подтверждающей, что его персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, уничтожить такие персональные данные в срок, не превышающий семи рабочих дней со дня поступления информации.

5.7. Учреждение обязано уведомить о внесенных изменениях в его персональные данные и принятых мерах заявителя и третьих лиц, которым

персональные данные этого заявителя были переданы.

## 6. Ответственность

6.1. Лица, нарушившие настоящие Правила, несут ответственность в соответствии с действующим законодательством.

Приложение № 1
к Правилам
Форма 1 «Запрос субъекта ПДн

Директору ГБУСО «Новоалександровский КЦСОН»
Т.В. Степановой

От

Паспорт серия номер

(Когда и кем выдан)

Проживающий по адресу:

Контактный номер телефона

Руководствуясь ст. 14 Федерального закона «О персональных данных», прошу Вас предоставить мне следующую информацию:

1. Какова цель обработки моих персональных данных в ГБУСО «Новоалександровский КЦСОН»;
2. Каковы способы обработки моих персональных данных, применяемые в ГБУСО «Новоалександровский КЦСОН», как оператором персональных данных;
3. Какие лица имеют доступ к моим персональным данным и каким лицам может быть предоставлен такой доступ;
4. Каков перечень обрабатываемых в ГБУСО «Новоалександровский КЦСОН» принадлежащих мне персональных данных и каков источник их получения;
5. Каковы сроки обработки моих персональных данных и каковы сроки их хранения;
6. Какие юридические последствия для меня, как для субъекта персональных данных, может повлечь за собой обработка моих персональных данных.

Фамилия И.О. (Подпись) (Дата)

Приложение № 2
к Правилам
Форма 1 «Запрос субъекта ПДн

Фамилия Имя Отчество
Адрес

Уважаемый(ая) _____!

Руководствуясь положениями ст. ст. 14, 20 Федерального закона РФ «О персональных данных» от 27.07.2006 г. № 152-ФЗ сообщаем Вам, что Государственное бюджетное учреждение социального обслуживания «Новоалександровский комплексный центр социального обслуживания населения» обрабатывает Ваши персональные данные

1. Цель обработки Ваших персональных – _____ (указать цель, заранее определенную до начала обработки)

2. Способы обработки Ваших персональных данных – автоматизированная обработка, неавтоматизированная обработка, смешанная обработка.

3. Лица, имеющие доступ к Вашим персональным данным:
   - Должность1;
   - Должность2;
   - Должность3;

4. Доступ к Вашим персональным данным может быть предоставлен: (тут указать тех лиц, которым МОЖЕТ быть предоставлен доступ). Также, по основаниям, предусмотренным действующим законодательством, доступ к Вашим персональным данным может быть предоставлен органам, осуществляющим оперативно-розыскную деятельность, органам дознания, следствия, суда.

5. Перечень обрабатываемых персональных данных: (Перечислить перечень) Источник получения персональных данных – (Указать источник получения).

6. Срок обработки Ваших персональных данных – (указать срок)

7. Обработка Ваших персональных данных может повлечь следующие юридические последствия – указать какие. (В теории права под юридическими последствиями понимают возникновение, изменение и прекращение в результате наступления какого-либо юридического факта тех или иных прав и обязанностей. По смыслу п.6 ч.4 ст.14 ФЗ 152 под таким юридическим фактом в Законе понимается именно сам факт обработки ПДн, т.е. факт совершения каких-либо действий с ПДн. Очевидно, что для человека факт совершения с его ПДн каких-либо операций (т.е. факт обработки ПДн) порождает возникновение у него комплекса прав, присущих субъекту ПДн и прямо предусмотренных ФЗ 152, а именно: право на доступ к своим ПДн, право на получение сведений об операторе, право требовать уточнения, блокирования или уничтожения ПДн, право отозвать согласие на обработку ПДн и т.п. Таким образом, юридически корректным было бы указание в ответе на запрос следующего: обработка Ваших ПДн влечет для Вас в качестве юридических последствий возникновение у Вас прав, присущих субъекту ПДн и предусмотренных ст.14 ФЗ «О персональных данных»).

Приложение № 3
к Правилам

ЖУРНАЛ
обращений субъектов персональных данных

количество листов_____

начат_____

окончен_____

| № п.п. | Фамилия, Имя, Отчество субъекта персональных данных или его законного представителя | Входящий номер, дата обращения субъекта персональных данных | Исходящий номер, дата ответа на запрос субъекта персональных данных |
|---|---|---|---|
| 3. | 4. | 5. | 6. |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |
| 6. | | | |
| 7. | | | |
| 8. | | | |

Директор ГБУСО
«Новоалександровский КЦСОН» Т.В. Степанова

Приложение № 17
к приказу директора ГБУСО
«Новоалександровский КЦСОН»
от 22 августа 2017 года № 448

**ПРАВИЛА**
**осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в ГБУСО «Новоалександровский КЦСОН»**

## 1. Общие положения

1.1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в ГБУСО «Новоалександровский КЦСОН» разработаны с учетом Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним внутренними нормативными правовыми актами.

1.2. Настоящие Правила определяют порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

## 2. Тематика внутреннего контроля

2.1. Тематика проверок обработки персональных данных с использованием средств автоматизации:

- соответствие полномочий пользователя разрешительной системе доступа;
- соблюдение пользователями информационных систем персональных данных парольной политики;
- соблюдение пользователями информационных систем персональных данных антивирусной политики;
- соблюдение пользователями информационных систем персональных данных правил работы со съемными носителями персональных данных;
- соблюдение правил работы с средствами криптографической защиты;
- соблюдение порядка доступа в помещения, где расположены элементы информационных систем персональных данных;
- соблюдение порядка резервирования баз данных и хранения резервных копий;
- соблюдение порядка работы со средствами защиты информации.

2.2. Соблюдение правил хранения и работы с бумажными носителями персональных данных.

## 3. Порядок проведения внутренних проверок

3.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям ГБУСО «Новоалександровский КЦСОН» организует проведение периодических проверок условий обработки персональных данных.

3.2. Проверки осуществляются ответственным за организацию обработки персональных данных (далее – Ответственный) либо комиссией.

3.3. Внутренние проверки проводятся в соответствии с Планом внутренних проверок, составленным Ответственным либо Председателем комиссии и утвержденным директором ГБУСО «Новоалександровский КЦСОН». Форма Плана приведена в Приложении 1 к настоящей Инструкции. При необходимости План может быть изменен.

3.4. План внутренних проверок составляется в декабре текущего года на следующий год и включает в себя все тематики проверок, равномерно распределенные на весь год.

3.5. Очередность и объем проверок определяется Ответственным либо Председателем комиссии самостоятельно.

3.6. Проверки осуществляются Ответственным либо комиссией непосредственно на месте обработки персональных данных путем опроса, либо, при необходимости, путем осмотра рабочих мест работников, участвующих в процессе обработки персональных данных.

3.7. Для каждой проверки составляется Протокол проведения внутренней проверки. Форма Протокола приведена в Приложении 2 к настоящей Инструкции.

3.8. При выявлении нарушений в ходе проверки Ответственным либо Председателем комиссии в Протоколе делается запись о мероприятиях по устранению нарушений и сроках исполнения.

3.9. Протоколы хранятся у Ответственного либо Председателя комиссии в течение текущего года. Уничтожение Протоколов проводится Ответственным либо комиссией самостоятельно в январе следующего за проверочным годом.

3.10. О результатах проверки и мерах, необходимых для устранения нарушений, руководителю докладывает Ответственный либо Председатель комиссии.

Приложение №1
к Инструкции осуществления внутреннего контроля
соответствия обработки персональных данных
требованиям к защите персональных данных
в ГБУСО «Новоалександровский КЦСОН»

Утверждаю
Директор ГБУСО «Новоалександровский
КЦСОН»

_____Т.В. Степанова

**План**
**внутренних проверок условий обработки персональных данных в ГБУСО «Новоалександровский КЦСОН»**

| № | Тема проверки | Нормативный документ предъявляющий требования | Срок проведения | Исполнитель |
|---|---|---|---|---|
| 1. | Соответствие полномочий пользователя разрешительной системе доступа | Разрешительная система доступа | | |
| 2. | Соблюдение пользователями информационных систем персональных данных парольной политики | Инструкция по организации парольной защиты | | |
| 3. | Соблюдение пользователями информационных систем персональных данных антивирусной политики | Инструкция по антивирусной защите | | |
| 4. | Соблюдение пользователями информационных систем персональных данных правил работы со съемными носителями персональных данных | Инструкция по организации хранения, обработки и передачи служебной информации (в том числе персональных данных) на внешних носителях (устройствах) в автоматизированной информационной системе ГБУСО «Новоалександровский КЦСОН» и за его пределами | | |
| 5. | Соблюдение правил работы с средствами криптографической защиты | Инструкция по обеспечению безопасности эксплуатации средств криптографической защиты информации | | |
| 6. | Соблюдение порядка доступа в помещения, где расположены элементы информационных систем персональных данных | Порядок доступа сотрудников ГБУСО «Новоалександровский КЦСОН» в помещения, в которых ведётся обработка персональных данных | | |
| 7. | Соблюдение порядка резервирования баз данных и хранения резервных копий | Инструкция о порядке резервирования и восстановления работоспособности технических средств, программного обеспечения и баз данных | | |
| 8. | Соблюдение порядка работы со средствами защиты информации | Инструкция пользователя информационных систем персональных данных, инструкция администратора информационных систем персональных данных по обеспечению безопасности персональных данных | | |
| 9. | Соблюдение правил хранения и работы с бумажными носителями персональных данных. | Инструкция по порядку учета и хранению документов, содержащих персональные данные | | |

Приложение 2
к Инструкции осуществления внутреннего контроля
соответствия обработки персональных данных
требованиям к защите персональных данных
в ГБУСО «Новоалександровский КЦСОН»

**Протокол**
**проведения внутренней проверки условий обработки персональных данных**

Настоящий Протокол составлен в том, что __.__.201_ ответственным за организацию обработки персональных данных/ комиссией по внутреннему контролю проведена проверка

_____
(тема проверки)

Проверка осуществлялась в соответствии с требованиями

_____
_____.
(название документа)

В ходе проверки проверено:

_____
_____
_____
_____
_____
_____
_____

Выявленные нарушения:

_____
_____
_____
_____.

Меры по устранению нарушений:

_____
_____
_____
_____
_____
_____
_____

Срок устранения нарушений: _____.

Должность Ответственного _____И.О. Фамилия
**либо**
Председатель комиссии _____И.О. Фамилия
Члены комиссии:
Должность _____И.О. Фамилия
Должность _____И.О. Фамилия
Должность _____И.О. Фамилия

Приложение № 18
к приказу директора ГБУСО
«Новоалександровский КЦСОН»
от 22 августа 2017 года № 448

**Разрешительная система доступа**
**сотрудников к ресурсам информационных систем персональных данных в ГБУСО «Новоалександровский КЦСОН», расположенном по адресу 356000, Ставропольский край, Новоалександровский район, г. Новоалександровск, пер. Красноармейский, 1**

1. Для обеспечения безопасности персональных данных при их обработке в информационной системе «1С «Зарплата и кадры»», разрешить доступ к работе с информационной системой следующим лицам:

| Должность | Права доступа | |
|---|---|---|
| | База данных С ПДн | Системная информация |
| - Главный бухгалтер<br>- Специалист по кадровому делопроизводству | Чтение, запись, удаление | Чтение, запись, удаление |

2. Для обеспечения безопасности персональных данных при их обработке в информационной системе «1С Бухгалтерия»», разрешить доступ к работе с информационной системой следующим лицам:

| Должность | Права доступа | |
|---|---|---|
| | База данных С ПДн | Системная информация |
| - Главный бухгалтер<br>- Заместитель главного бухгалтера<br>- Экономист<br>- Бухгалтер | Чтение, запись, удаление | Чтение, запись, удаление |

3. Для обеспечения безопасности персональных данных при их обработке в информационной системе «УРМ АС «Бюджет»», разрешить доступ к работе с информационной системой следующим лицам:

| Должность | Права доступа | |
|---|---|---|
| | База данных С ПДн | Системная информация |
| - Бухгалтер | Чтение, запись, удаление | Чтение, запись, удаление |

4. Для обеспечения безопасности персональных данных при их обработке в информационной системе «СБиС ++ «Электронная отчетность и документооборот», разрешить доступ к работе с информационной системой следующим лицам:

| Должность | Права доступа | |
|---|---|---|
| | База данных С ПДн | Системная информация |
| - Главный бухгалтер<br>- Специалист по кадровому делопроизводству | Чтение, запись, удаление | Чтение, запись, удаление |

5. Для обеспечения безопасности персональных данных при их обработке в информационной системе «Учет клиентов ЦСО», разрешить доступ к работе с информационной системой следующим лицам:

| Должность | Права доступа | |
|---|---|---|
| | База данных С ПДн | Системная информация |
| - Заместитель директора<br>- Специалист по социальной работе<br>- Заведующий отделением | Чтение, запись, удаление | Чтение, запись, удаление |

| | | |
|---|---|---|
| срочного социального обслуживания;<br>- Заведующий отделением дневного пребывания граждан пожилого возраста и инвалидов;<br>- Заведующий отделением специализированного отделения социально – медицинского обслуживания на дому;<br>- Заведующий отделением социального обслуживания на дому (город);<br>-Заведующие отделениями социального обслуживания на дому (село);<br>- Программист | | |

6. Для обеспечения безопасности персональных данных при их обработке в информационной системе «Автоматизированная система «Адресная социальная помощь»», разрешить доступ к работе с информационной системой следующим лицам:

| Должность | Права доступа | |
|---|---|---|
| | База данных С ПДн | Системная информация |
| - Заместитель директора<br>- Программист<br>- Специалист по социальной работе отделения реабилитации детей и подростков с ограниченными возможностями здоровья;<br>- Специалист по социальной работе социального приюта для детей и подростков «Солнышко» | Чтение, запись | Чтение, запись, удаление |

Директор Государственного бюджетного
учреждения социального обслуживания
«Новоалександровский комплексный центр
социального обслуживания населения» Т.В. Степанова

Приложение № 19
к приказу директора ГБУСО
«Новоалександровский КЦСОН»
от 22 августа 2017 года № 448

**Частная модель угроз безопасности персональных данных для информационных систем «1С «Зарплата и кадры»», «1С «Бухгалтерия»», «УРМ АС «Бюджет»», «СБиС ++ «Электронная отчетность и документооборот»», «Учет клиентов ЦСО», «Автоматизированная система «Адресная социальная помощь»**

Модель угроз безопасности персональных данных (далее – Модель) при их обработке в информационных системах персональных данных «1С «зарплата и кадры»», «1С «Бухгалтерия»», «УРМ АС «Бюджет»», «СБиС ++ «Электронная отчетность и документооборот»», «Учет клиентов ЦСО», «Автоматизированная система «Адресная социальная помощь»», принадлежащих ГБУСО «Новоалександровский КЦСОН» (далее – Учреждение), установленные по адресу: 356000, Ставропольский край, Новоалександровский район, г. Новоалександровск, пер. Красноармейский, 1, строится на основании следующих документов:

1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г.);
2. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Утверждена Заместителем директора ФСТЭК России 14 февраля 2008 г.).

В модели угроз представлены характеристики информационных систем персональных данных (ИСПДн) Учреждения, состав и режим обработки персональных данных (ПДн), классификация потенциальных нарушителей, оценка исходного уровня защищенности, анализ угроз безопасности персональных данных (УБПДн).

**Описание информационных систем персональных данных**

**Описание информационной системы «1С «Зарплата и кадры»»**

Информационная система развёрнута на двух компьютере. Компьютеры имеют подключения к локальной сети и выход в сеть Интернет. Обработка персональных данных осуществляется в программах «1С Зарплата и кадры», «Microsoft Office». Операционная система – «Windows 7».

**Описание информационной системы «1С «Бухгалтерия»»**

Информационная система развёрнута на пяти компьютерах. Компьютеры имеют подключения к локальной сети и выход в сеть Интернет. Обработка персональных данных осуществляется в программах «Open Office», «Microsoft Office», «1С Бухгалтерия». Операционная система – «Windows 7».

**Описание информационной системы «УРМ АС «Бюджет»»**

Информационная система развёрнута на одном компьютере. Компьютер имеет подключение к локальной сети и выход в сеть Интернет. Обработка персональных данных осуществляется в программах «УРМ АС «Бюджет»», «Open Office», «Microsoft Office». Операционная система – «Windows 7».

**«СБиС ++ «Электронная отчетность и документооборот»»**

Информационная система развёрнута на одном компьютере. Компьютер имеет подключение к локальной сети и выход в сеть Интернет. Обработка персональных данных осуществляется в программах «СБиС ++ «Электронная отчетность и документооборот»», «Microsoft Office». Операционная система – «Windows 7».

**Описание информационной системы «Учет клиентов ЦСО»**

Информационная система развёрнута на десяти компьютерах. Компьютеры имеют подключение к локальной сети и выход в сеть Интернет. Обработка персональных данных осуществляется в программах «Microsoft Office», «Учет клиентов ЦСО». Операционная система – «Windows 7».

**Описание информационной системы «Автоматизированная система «Адресная социальная помощь»**

Информационная система развёрнута на трех компьютерах. Компьютеры имеют подключения к локальной сети и выход в сеть Интернет. Обработка персональных данных осуществляется в программах «Microsoft Office», «Автоматизированная система «Адресная социальная помощь», Операционная система – «Windows 7».

**Необходимый уровень защищенности**

Согласно Актам классификации, информационным системам необходимо обеспечить 4 уровень защищенности.

## Определение угроз безопасности персональных данных

**Классификация нарушителей**

По признаку принадлежности к ИСПДн все нарушители делятся на две группы:

1. Внешние нарушители – физические лица, не имеющие права пребывания в пределах контролируемой территории, где размещается оборудование ИСПДн;
2. Внутренние нарушители – физические лица, имеющие право пребывания в пределах контролируемой территории, где размещается оборудование ИСПДн.

**Внешний нарушитель**

Внешние нарушители имеют возможности:

1. Воздействовать на защищаемую информацию по техническим каналам утечки информации;
2. Осуществлять несанкционированный доступ к каналам связи, выходящим за пределы служебных помещений;
3. Осуществлять несанкционированный доступ через автоматизированные рабочие места, подключенные к сетям связи общего пользования и сетям международного информационного обмена;
4. Осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, алгоритмических или программных закладок;
5. Осуществлять несанкционированный доступ через элементы информационной инфраструктуры ИСПДн, которые в процессе своего жизненного цикла (модернизации, сопровождения, ремонта, утилизации) оказываются за пределами контролируемой зоны;
6. Осуществлять несанкционированный доступ через информационные системы взаимодействующих ведомств, организаций и учреждений при их подключении к ИСПДн.

Предполагается, что выявленные внешние нарушители не могут получать доступ к защищаемой информации и воздействовать на нее по техническим каналам утечки, так как объем информации, хранимой и обрабатываемой в ИСПДн, является недостаточным для возможной мотивации внешних нарушителей к осуществлению указанных действий.

Таким образом, выявленные внешние нарушители могут воздействовать на защищаемую информацию всеми перечисленными выше способами, за исключением действий, направленных на утечку и искажение конфиденциальной информации по техническим каналам.

**Внутренний нарушитель**

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основным является реализация комплекса организационно-технических мер, в том числе по подбору, расстановке и обеспечению высокой профессиональной подготовки кадров, допуску физических лиц внутрь контролируемой зоны и контролю за порядком проведения работ, направленных на предотвращение и пресечение несанкционированного доступа к защищаемой информации.

**Предположения об имеющейся у нарушителя информации об объектах реализации угроз**

В качестве основных уровней знаний нарушителей об ИСПДн можно выделить следующие:

1. Общая информация – информация о назначениях и общих характеристиках ИСПДн;
2. Эксплуатационная информация – информация, полученная из эксплуатационной документации;
3. Чувствительная информация – информация, дополняющая эксплуатационную информацию об ИСПДн (например, сведения из проектной документации ИСПДн).

**В частности, нарушитель может иметь:**

1. Данные об организации работы, структуре и используемых технических, программных и программно-технических средствах ИСПДн;
2. Сведения об информационных ресурсах ИСПДн: порядок и правила создания, хранения и передачи информации, структура и свойства информационных потоков;
3. Данные об уязвимостях, включая данные о недокументированных (недекларированных) возможностях технических, программных и программно-технических средств ИСПДн;
4. Данные о реализованных в СЗИ принципах и алгоритмах;
5. Сведения о возможных каналах реализации угроз;
6. Информацию о способах реализации угроз.

Степень информированности нарушителя зависит от многих факторов, включая реализованные в Учреждения конкретные организационные меры и компетенцию нарушителей.

В связи с изложенным, предполагается, что вероятные нарушители обладают всей информацией, необходимой для подготовки и реализации угроз.

**Предположения об имеющихся у нарушителя средствах реализации угроз**

**Предполагается, что нарушитель имеет:**

1. Аппаратные компоненты ИСПДн и СЗИ;
2. Доступные в свободной продаже технические средства и программное обеспечение;
3. Специально разработанные технические средства и программное обеспечение.
4. Внутренний нарушитель может использовать штатные средства.

Состав имеющихся у нарушителя средств, которые он может использовать для реализации угроз ИБ, а также возможности по их применению зависят от многих факторов, включая реализованные в Учреждения конкретные организационные меры, финансовые возможности и компетенцию нарушителей. Поэтому объективно оценить состав имеющихся у нарушителя средств реализации угроз в общем случае практически невозможно.

Так как специальные средства, используемые для реализации угроз утечки информации по техническим каналам, отсутствуют в свободной продаже, предполагается, что потенциальные нарушители **не имеют**:

1. Средств воздействия через сигнальные цепи (информационные и управляющие интерфейсы СВТ) на ИСПДн;
2. Средств воздействия на источники питания и через цепи питания;
3. Средств воздействия через цепи заземления;
4. Средств активного воздействия на технические средства (средств облучения).

Предполагается, что нарушитель обладает совершенными средствами реализации угроз.

**Исходный уровень защищенности информационной системы персональных данных**

Под исходным уровнем защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн (Y1).

В Таблице 1 представлены характеристики уровня исходной защищенности для ИСПДн Учреждения.

Таблица 1

| Технические и эксплуатационные характеристики ИСПДн | Уровень защищенности |
|---|---|
| По территориальному размещению<br><br>Локальная ИСПДн, развернутая в пределах одного здания | Высокий |
| По наличию соединения с сетями общего пользования:<br><br>ИСПДн, имеющая одноточечный выход в сеть общего пользования; | Средний |
| По встроенным (легальным) операциям с записями баз персональных данных<br><br>Модификация, передача | Низкий |
| По разграничению доступа к персональным данным<br><br>ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн; | Средний |
| По наличию соединений с другими базами ПДн иных ИСПДн<br><br>ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн | Высокий |
| По уровню обобщения (обезличивания) ПДн<br><br>ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн) | Низкий |
| По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки<br><br>ИСПДн, предоставляющая часть ПДн; | Средний |

Таким образом, исходя из вышеперечисленных данных, коэффициент Y1=5

**Перечень действующих угроз на информационную систему и их актуальность**

**Кража ПЭВМ**

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн.

Имеющиеся средства защиты

- Физическая охрана. Круглосуточно дежурит охранник;
- Посетители регистрируются в журнале.
- Система видеонаблюдения.
- Тревожная кнопка, договор с частным охранным предприятием.
- Кабинеты, в которых расположены элементы ИСПДн, запираются.

*Опасность - Высокая*

*Вероятность реализации - Низкая*

Y1 = 5 Y2 = 2

(Y1+Y2)/20 = 0,35 => Возможность реализации - Средняя

*Актуальность - Актуальна*

**Кража носителей информации**

Угроза осуществляется путем НСД внешними и внутренними нарушителями к носителям информации.

Имеющиеся средства защиты

- Физическая охрана. Круглосуточно дежурит охранник;
- Посетители регистрируются в журнале.
- Система видеонаблюдения.
- Тревожная кнопка, договор с частным охранным предприятием.
- Кабинеты, в которых расположены элементы ИСПДн, запираются.
- Инструкция по работе со съемными носителями, регламентирующая правила безопасной работы с съемными носителями конфиденциальной информации.

*Опасность - Высокая*

*Вероятность реализации - Низкая*

Y1 = 5 Y2 = 2

(Y1+Y2)/20 = 0,35 => Возможность реализации - Средняя

*Актуальность - Актуальна*

**Кража ключей и паролей доступа внутренними и внешними нарушителями**

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн.

Имеющиеся средства защиты

- Инструкция пользователя ИСПДн, запрещающая хранение паролей доступа на бумажных или электронных носителях без соответствующей защиты от несанкционированного доступа к ним.

*Опасность - Средняя*

*Вероятность реализации - Низкая*

Y1 = 5 Y2 = 2

(Y1+Y2)/20 = 0,35 => Возможность реализации - Средняя

*Актуальность - Актуальна*

**Кража, модификация, уничтожение информации**

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн и средства защиты, а также происходит работа пользователей.

Имеющиеся средства защиты

- Разрешительная система доступа (организационная мера) к информационным ресурсам.

*Опасность - Высокая*

*Вероятность реализации - Низкая*

Y1 = 5 Y2 = 2

(Y1+Y2)/20 = 0,35 => Возможность реализации - Средняя

*Актуальность - Актуальна*

**Несанкционированное отключение средств защиты**

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены средства защиты всех ИСПДн.

Имеющиеся средства защиты

- Инструкция пользователя ИСПДн;
- Инструкция по антивирусной защите.

*Опасность - Средняя*

*Вероятность реализации - Маловероятно*

Y1 = 5 Y2 = 0

(Y1+Y2)/20 = 0,25 => Возможность реализации - Низкая

*Актуальность - Неактуальна*

**Действия вредоносных программ (вирусов)**

Программно-математическое воздействие - это воздействие с помощью вредоносных программ. Программой с потенциально опасными последствиями или вредоносной программой (вирусом) называют

некоторую самостоятельную программу (набор инструкций), которая способна выполнять любое непустое подмножество следующих функций:

– скрывать признаки своего присутствия в программной среде компьютера; обладать способностью к самодублированию, ассоциированию себя с другими программами и (или) переносу своих фрагментов в иные области оперативной или внешней памяти; разрушать (искажать произвольным образом) код программ в оперативной памяти;

– выполнять без инициирования со стороны пользователя (пользовательской программы в штатном режиме ее выполнения) деструктивные функции (копирования, уничтожения, блокирования и т.п.);

– сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);

– искажать произвольным образом, блокировать и (или) подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

Имеющиеся средства защиты

- Антивирус Касперского.

*Опасность - Средняя*
*Вероятность реализации - Низкая*
Y1 = 5 Y2 = 2
(Y1+Y2)/20 = 0,35 => Возможность реализации - Средняя
*Актуальность – Актуальна*

**Установка ПО не связанного с исполнением служебных обязанностей**

Угроза осуществляется путем несанкционированной установки ПО внутренними нарушителями, что может привести к нарушению конфиденциальности, целостности и доступности всей ИСПДн или ее элементов.

Имеющиеся средства защиты

- Инструкция пользователя ИСПДн, запрещающая пользователям самостоятельную установку стороннего программного обеспечения.

*Опасность - Низкая*
*Вероятность реализации - Средняя*
Y1 = 5 Y2 = 5
(Y1+Y2)/20 = 0,5 => Возможность реализации - Средняя
*Актуальность – Неактуальна*

**Утрата паролей доступа к ИСПДн**

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения парольной политики в части их создания (создают легкие или пустые пароли, не меняют пароли по истечении срока их жизни или компрометации и т.п.) и хранения (записывают пароли на бумажные носители, передают ключи доступа третьим лицам и т.п.) или не осведомлены о них.

Имеющиеся средства защиты

- Инструкция по парольной защите, устанавливающая правила использования и хранения паролей.

*Опасность - Средняя*
*Вероятность реализации - Средняя*
Y1 = 5 Y2 = 5
(Y1+Y2)/20 = 0,5 => Возможность реализации - Средняя
*Актуальность – Актуальна*

**Непреднамеренное отключение средств защиты**

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения принятых правил работы с ИСПДн и средствами защиты или не осведомлены о них.

Имеющиеся средства защиты

- Инструкция пользователя ИСПДн.

*Опасность - Средняя*
*Вероятность реализации - Низкая*
Y1 = 5 Y2 = 2
(Y1+Y2)/20 = 0,25 => Возможность реализации - Средняя
*Актуальность - Актуальна*

**Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке**

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн.

Имеющиеся средства защиты

- Инструкция пользователя ИСПДн, регламентирующая работу с персональными данными.

*Опасность - Высокая*
*Вероятность реализации - Средняя*
Y1 = 5 Y2 = 5
(Y1+Y2)/20 = 0,5 => Возможность реализации - Средняя
*Актуальность – Актуальна*

**Перехват информации за пределами контролируемой зоны**

Угроза осуществляется путем перехвата и анализа трафика проходящего по каналам связи принадлежащим сторонним организациям. Угроза может быть реализована при передаче отчетности, в контролирующие органы, через сеть Интернет.

Имеющиеся средства защиты

- Криптографические средства защиты информации (КриптоПро, ViPNET).

*Опасность - Высокая*
*Вероятность реализации - Маловероятно*
Y1 = 5 Y2 = 0
(Y1+Y2)/20 = 0,25 => Возможность реализации - Низкая
*Актуальность – Актуальна*

**Удаленный запуск приложений**

Угроза заключается в стремлении запустить на хосте ИСПДн различные предварительно внедренные вредоносные программы: программы-закладки, вирусы, «сетевые шпионы», основная цель которых - нарушение конфиденциальности, целостности, доступности информации и полный контроль за работой хоста. Кроме того, возможен несанкционированный запуск прикладных программ пользователей для несанкционированного получения необходимых нарушителю данных, для запуска управляемых прикладной программой процессов и др. Выделяют три подкласса данных угроз:

- распространение файлов, содержащих несанкционированный исполняемый код;
- удаленный запуск приложения путем переполнения буфера приложений-серверов;
- удаленный запуск приложения путем использования возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками, либо используемыми штатными средствами.

Типовые угрозы первого из указанных подклассов основываются на активизации распространяемых файлов при случайном обращении к ним. Примерами таких файлов могут служить: файлы, содержащие исполняемый код в вид документы, содержащие исполняемый код в виде элементов ActiveX, Java-апплетов, интерпретируемых скриптов (например, тексты на JavaScript); файлы, содержащие исполняемые коды программ. Для распространения файлов могут использоваться службы электронной почты, передачи файлов, сетевой файловой системы. При угрозах второго подкласса используются недостатки программ, реализующих сетевые сервисы (в частности, отсутствие контроля за переполнением буфера). Настройкой системных регистров иногда удается переключить процессор после прерывания, вызванного переполнением буфера, на исполнение кода, содержащегося за границей буфера. Примером реализации такой угрозы может служить внедрение широко известного «вируса Морриса». При угрозах третьего подкласса нарушитель использует возможности удаленного управления системой, предоставляемые скрытыми компонентами (например, «троянскими» программами типа Back.Orifice, NetBus), либо штатными средствами управления и администрирования компьютерных сетей (LandeskManagementSuite, Managewise, BackOrifice и т. п.). В результате их использования удается добиться удаленного контроля над станцией в сети.

Имеющиеся средства защиты

- Антивирус Касперского;
- Межсетевой экран Windows.

*Опасность - Средняя*
*Вероятность реализации - Низкая*
Y1 = 5 Y2 =2
(Y1+Y2)/20 = 0,35 => Возможность реализации - Средняя
*Актуальность – Актуальна*

**Сканирование сети**

Сущность процесса реализации угрозы заключается в передачи запросов сетевым службам хостов ИСПДн и анализе ответов от них.

Цель - выявление используемых протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, определение активных сетевых сервисов, подбор идентификаторов и паролей пользователей.

Имеющиеся средства защиты

- Антивирус Касперского;
- Межсетевой экран Windows.

*Опасность - Средняя*

*Вероятность реализации - Низкая*

Y1 = 5 Y2 = 2

(Y1+Y2)/20 = 0,35 => Возможность реализации - Средняя

*Актуальность – Актуальна*