

ПРИКАЗ №169

от 19.10.2023 г.

г. Саратов

**Об организации работы по
защите персональных данных**

Во исполнение Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» (с изменениями и дополнениями) и в целях организации работ с персональными данными.

ПРИКАЗЫВАЮ:

1. Функции ответственного за организацию обработки персональных данных в ГАУ СО «ФСЦ «Урожай» возложить на специалиста по защите информации Захаровского А.О.
2. Утвердить список должностей ГАУ СО «ФСЦ «Урожай», имеющих право обрабатывать персональные данные (согласно приложению № 1).
3. Утвердить Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, Положения об обработке и защите персональных данных сотрудников и занимающихся (согласно приложениям № 2, № 3, № 4).
4. Утвердить Инструкцию ответственного за организацию обработки персональных данных в учреждении (согласно приложению № 5).
5. Утвердить Инструкцию оператора по обработке персональных данных на автоматизированных рабочих местах (согласно приложению № 6).
6. Приказ довести до должностных лиц учреждения.
7. Приказ №90 от 05.08.2022 года «Об организации работы по защите персональных данных» считать утратившим силу.
8. Контроль за исполнением настоящего приказа оставляю за собой.

Директор

В.Е. Новиков

ПОЛОЖЕНИЕ

об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных

1. Общие положения

1. Настоящее Положение устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, представляющих собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации (далее - информационные системы).

2. Под техническими средствами, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.) средства защиты информации, применяемые в информационных системах.

Цель

Настоящее Положение является развитием комплекса мер, направленных на обеспечение защиты персональных данных, хранящихся у Оператора, посредством планомерных действий по совершенствованию организации труда.

Основания

Основанием для разработки данного Положения являются:

- Конституция РФ от 12.12.1993 г., ст. 24;
- Трудовой Кодекс РФ № 197-ФЗ от 01.02.2002 г., ст. 85-90;
- Кодекс РФ об административных правонарушениях № 195-ФЗ от 30.12.2001 г.;
- Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
- Указ Президента РФ № 188 от 06.09.1997 г. «Об утверждении перечня сведений конфиденциального характера».

2. Понятие и состав персональных данных

1. Под персональными данными Работников понимается любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация. Персональные данные всегда являются конфиденциальной, строго охраняемой информацией.

К персональным данным относятся:

- все биографические сведения Работника;
- образование;
- специальность;
- занимаемая должность;
- наличие судимостей;
- адрес местожительства;
- домашний и сотовый телефон;
- состав семьи;
- место работы или учебы членов семьи и родственников;
- характер взаимоотношений в семье;

- размер заработной платы;
- содержание трудового договора;
- состав декларируемых сведений о наличии материальных ценностей;
- содержание декларации, подаваемой в налоговую инспекцию;
- подлинники и копии приказов по личному составу;
- личные дела, личные карточки (форма Т) и трудовые книжки Работников;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке Работников, их аттестации, служебным расследованиям;
- копии отчетов, направляемые в органы статистики;
- анкета;
- копии документов об образовании;
- результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей;
- фотографии и иные сведения, относящиеся к персональным данным работника.

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

Собственником информационных ресурсов (персональных данных) – является субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения этими ресурсами. Это любой гражданин, к личности которого относятся соответствующие персональные данные, и который вступил (стал Работником) или изъявил желание вступить в трудовые отношения с Оператором. Субъект персональных данных самостоятельно решает вопрос передачи Оператору своих персональных данных.

Держателем персональных данных является Оператор, которому Работник добровольно передает во владение свои персональные данные. Оператор выполняет функцию владения этими данными и обладает полномочиями распоряжения ими в пределах, установленных законодательством.

Права и обязанности Оператора в трудовых отношениях осуществляются физическим лицом, уполномоченным Оператором. Указанные права и обязанности он может делегировать нижестоящим руководителям – своим заместителям, руководителям структурных подразделений, работа которых требует знания персональных данных работников или связана с обработкой этих данных.

Потребителями (операторами) персональных данных являются юридические и физические лица, обращающиеся к собственнику или держателю персональных данных за получением необходимых сведений и пользующиеся ими без права передачи и разглашения.

2. Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Для обеспечения безопасности персональных данных при их обработке в информационных системах осуществляется защита речевой информации и информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе.

3. Методы и способы защиты информации в информационных системах устанавливаются Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

Достаточность принятых мер по обеспечению безопасности персональных данных при их обработке в информационных системах оценивается при проведении государственного контроля и надзора.

4. Работы по обеспечению безопасности персональных данных при их обработке в информационных системах являются неотъемлемой частью работ по созданию информационных систем.

5. Средства защиты информации, применяемые в информационных системах, должны в установленном порядке проходить процедуру оценки соответствия.

6. Информационные системы классифицируются в структурных подразделениях, осуществляющих обработку персональных данных, а также определяющих цели и содержание обработки персональных данных, в зависимости от объема обрабатываемых ими персональных данных и угроз безопасности жизненно важным интересам личности, общества и государства.

Порядок проведения классификации информационных систем определен Приказом от 13 февраля 2008 года №55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных» совместно с Федеральной службой по техническому и экспортному контролю, * Федеральной службой безопасности Российской Федерации и Министерством информационных технологий и связи Российской Федерации. утратил силу

7. Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения технических средств.

8. Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

9. Возможные каналы утечки информации при обработке персональных, данных в информационных системах определяются Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

10. Безопасность персональных данных при их обработке в информационной системе обеспечивает оператор или лицо, которому на основании договора оператор поручает обработку персональных данных (далее — уполномоченное лицо). Существенным условием договора является обязанность уполномоченного лица обеспечить конфиденциальность персональных данных и их безопасность при обработке в информационной системе.

11. При обработке персональных данных в информационной системе должно быть обеспечено:

а) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передача их лицам, не имеющим права доступа к такой информации;

б) своевременное обнаружение факторов несанкционированного доступа к такой информации;

в) недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

г) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

д) постоянный контроль обеспечения уровня защищенности персональных данных.

12. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включает в себя:

а) определение угроз безопасности персональных данных при их обработке, формирование на их основе частной модели угроз;

б) разработку на основе частной модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

в) проверку готовности средств защиты информации к использованию с составлением заключения о возможности их эксплуатации;

г) установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационно-технической документацией;

д) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

е) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

ж) учет лиц, допущенных к работе с персональными данными в информационной системе;

з) контроль соблюдения условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

и) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использование средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

к) описание системы защиты персональных данных.

13. Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационной системе оператором или уполномоченным лицом может назначаться структурное подразделение или должностное лицо (работник), ответственные за обеспечение безопасности персональных данных.

14. Лица, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании списка, утвержденного оператором или уполномоченным лицом.

15. Запросы пользователей информационной системы на получение персональных данных, включая лиц, указанных в пункте 14 настоящего Положения, а также факты предоставления персональных данных по этим запросам регистрируются автоматизированными средствами информационной системы в электронном журнале обращений. Содержание электронного журнала обращений периодически проверяется соответствующими должностными лицами (работниками) оператора или уполномоченного лица.

16. При обнаружении нарушений порядка предоставления персональных данных оператор или уполномоченное лицо незамедлительно приостанавливает предоставление персональных данных оператору информационной системы до выявления причин нарушений и устранения этих причин.

17. Реализация требований по обеспечению безопасности информации в средствах защиты информации возлагается на их разработчиков.

18. Результаты оценки соответствия и (или) тематических исследований средств защиты информации, предназначенных для обеспечения безопасности персональных данных при их обработке в информационных системах оцениваются в ходе экспертизы, осуществляемой Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

19. К средствам защиты информации, предназначенным для обеспечения безопасности персональных данных при их обработке в информационных системах, прилагаются правила пользования этими средствами, согласованные с Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

Изменение условий применения средств защиты информации, предусмотренных указанными правилами, согласовывается с этими федеральными органами исполнительной власти в пределах их полномочий.

20. Средства защиты информации, предназначенные для обеспечения безопасности персональных данных при их обработке в информационных системах, подлежат учету с использованием индексов или условных наименований и регистрационных номеров. Перечень индексов, условных наименований и регистрационных номеров определяется Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

ПОЛОЖЕНИЕ **об обработке и защите персональных данных сотрудников**

1. Общие положения

Настоящее Положение устанавливает порядок приема, учета, сбора, поиска, обработки, накопления и хранения документов, содержащих сведения, отнесенные к персональным данным сотрудников ГАУ СО «ФСЦ «Урожай» (далее – «Оператор»). Под сотрудниками подразумеваются лица, имеющие трудовые отношения с ГАУ СО «ФСЦ «Урожай» (далее – «сотрудники»).

Цель

Обеспечение уважения прав и основных свобод каждого сотрудника при обработке его персональных данных, в том числе защиты прав, неприкосновенность частной жизни, личную и семейную тайну.

Настоящее Положение является развитием комплекса мер, направленных на обеспечение защиты персональных данных, хранящихся у Оператора, посредством планомерных действий по совершенствованию организации труда.

Основания

Основанием для разработки данного Положения являются:

- Конституция РФ;
- Федеральный закон от 19.12.2005 № 16-ФЗ «О ратификации конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;
- Трудовой Кодекс РФ № 197-ФЗ от 01.02.2002 г., ст.ст. 85-90;
- Кодекс РФ об административных правонарушениях № 195-ФЗ от 30.12.2001 г.;
- Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
- Указ Президента РФ № 188 от 06.09.1997 г. «Об утверждении перечня сведений конфиденциального характера»;
- Постановление Правительства РФ от 17.11.2007 г. №781 «об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;
- «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных», утверждены заместителем директора ФСТЭК РФ 15.02.2008 г.;
- «Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» утверждены заместителем директора ФСТЭК РФ 15.02.2008 г.;
- Положение о методах и способах защиты информации в информационных системах персональных данных (Приложение к Приказу ФСТЭК РФ от 5 февраля 2010 г. № 58);

Порядок ввода в действие Положения о защите персональных данных и изменений к нему

Положение о защите персональных данных утверждается приказом директор ГАУ СО «ФСЦ «Урожай». Все сотрудники организации должны быть ознакомлены под расписку с данным Положением.

2. Понятие и состав персональных данных

Под персональными данными сотрудников понимается любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация. Персональные данные всегда являются конфиденциальной, строго охраняемой информацией.

К персональным данным относятся:

- все биографические сведения сотрудника;
- образование;
- специальность;
- занимаемая должность;
- наличие судимостей;
- адрес местожительства;
- домашний и сотовый телефон;
- состав семьи;
- место работы или учебы членов семьи и родственников;
- характер взаимоотношений в семье;
- размер заработной платы;
- содержание трудового договора;
- состав декларируемых сведений о наличии материальных ценностей;
- содержание декларации, подаваемой в налоговую инспекцию;
- подлинники и копии приказов по личному составу;
- личные дела, личные карточки (форма Т) и трудовые книжки сотрудников;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
 - копии отчетов, направляемые в органы статистики;
 - анкета;
 - копии документов об образовании;
 - результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей;
 - фотографии и иные сведения, относящиеся к персональным данным Сотрудника.

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

Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.

Собственником информационных ресурсов (персональных данных) – является субъект, в полном объеме реализующий полномочия, владения, пользования, распоряжения этими ресурсами. Это любой гражданин, к личности которого относятся соответствующие персональные данные, и который вступил (стал сотрудником) или изъявил желание вступить в трудовые отношения с Оператором. Субъект персональных данных самостоятельно решает вопрос передачи Оператору своих персональных данных.

Держателем персональных данных является Оператор, которому Сотрудник добровольно передает во владение свои персональные данные. Оператор выполняет функцию владения этими данными и обладает полномочиями распоряжения ими в пределах, установленных законодательством.

Права и обязанности Оператора в трудовых отношениях осуществляются физическим лицом, уполномоченным Оператором. Указанные права и обязанности он может делегировать нижестоящим руководителям – своим заместителям, руководителям структурных подразделений, работа которых требует знания персональных данных работников или связана с обработкой этих данных.

Потребителями (операторами) персональных данных являются юридические и физические лица, обращающиеся к собственнику или держателю персональных данных за получением необходимых сведений и пользующиеся ими без права передачи и разглашения.

3. Принципы обработки персональных данных

Обработка персональных данных включает в себя их получение, хранение, комбинирование, передачу, а так же актуализацию, блокирование, защиту, уничтожение либо другое использование персональных данных сотрудника.

Обработка персональных данных сотрудника может осуществляться с согласия субъекта персональных данных. Согласие субъекта персональных данных не требуется, если такая обработка требуется в целях обеспечения соблюдения законов и иных нормативных актов, в целях исполнения договора, одной из сторон которого является субъект персональных данных, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности сотрудников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

Все персональные данные сотрудника получаются у него самого. Если персональные данные сотрудника возможно получить только у третьей стороны, то сотрудник должен быть уведомлен об этом заранее, и от него должно быть получено письменное согласие.

Не допускается получение и обработка персональных данных сотрудника о его политических, религиозных и иных убеждениях и частной жизни, а также о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных законодательством РФ.

При принятии решений относительно сотрудника на основании его персональных данных не допускается использование данных, полученных исключительно в результате их автоматизированной обработки или электронного получения.

В случаях непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции РФ возможно получение и обработка данных о частной жизни сотрудника только с его письменного согласия.

Пакет анкетно-биографических и характеризующих материалов (далее – пакет) сотрудника формируется после издания приказа о его приеме на работу. Пакет обязательно содержит личную карточку формы Т-2, а также может содержать документы, содержащие персональные данные сотрудника, в порядке, отражающем процесс приема на работу. Все документы хранятся в папках в алфавитном порядке фамилий сотрудников. Пакет пополняется на протяжении всей трудовой деятельности сотрудника в данной организации. Изменения, вносимые в карточку Т-2, должны быть подтверждены соответствующими документами (например, копия свидетельства о браке).

Специалист по кадрам ответственный за документационное обеспечение кадровой деятельности, принимает от принимаемого на работу сотрудника документы, проверяет полноту их заполнения и правильность указываемых сведений в соответствии с предъявленными документами.

Под блокированием персональных данных понимается временное прекращение операций по их обработке по требованию субъекта персональных данных при выявлении им недостоверности обрабатываемых сведений или неправомерных действий в отношении его данных.

При обработке персональных данных сотрудников Оператор в лице директор ГАУ СО «ФСЦ «Урожай» вправе определять способы обработки, документирования, хранения и защиты персональных данных сотрудников ГАУ СО «ФСЦ «Урожай» на базе современных информационных технологий.

Сотрудник обязан:

- передавать Оператору или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом РФ;

- своевременно сообщать Оператору об изменении своих персональных данных.

Работник имеет право на:

- полную информацию о своих персональных данных и обработке этих данных;
- свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные Работника, за исключением случаев, предусмотренных законодательством РФ;

- определение своих представителей для защиты своих персональных данных;

- доступ к относящимся к нему медицинским данным с помощью медицинского специалиста по своему выбору;

- требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований. При отказе Оператора

исключить или исправить персональные данные Работника он имеет право заявить в письменной форме Оператору о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера Работник имеет право дополнить заявлениям, выражающим его собственную точку зрения;

- требование об извещении Оператором всех лиц, которым ранее были сообщены неверные или неполные персональные данные Работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;

- обжалование в суд любых неправомерных действий или бездействия Оператора при обработке и защите его персональных данных.

4. Доступ к персональным данным

Персональные данные добровольно передаются Работником непосредственно держателю этих данных и потребителям внутри ГАУ СО «ФСЦ «Урожай» исключительно для обработки и использования в работе.

Внешний доступ. К числу массовых потребителей персональных данных вне ГАУ СО «ФСЦ «Урожай» можно отнести государственные и негосударственные функциональные структуры:

а. Надзорно-контрольные органы:

- органы, осуществляющие оперативно-розыскную деятельность;
- прокуратура;
- кредитные организации (банки) - с согласия сотрудника;
- управление ГО и ЧС;
- органы статистики;
- негосударственные пенсионные фонды;
- благотворительные фонды (только с письменного заявления);
- страховые агентства;
- военкоматы;
- органы социального страхования;
- пенсионные фонды;
- налоговые органы;
- подразделения муниципальных органов управления;

б. Другие организации и предприятия.

- с письменного разрешения сотрудника, нотариально заверенного, или привезенного собственноручно (гл. 14 ТК РФ).

с. Родственники, члены семьи.

- с письменного разрешения сотрудника, нотариально заверенного, или привезенного собственноручно (гл. 14 ТК РФ).

Внутренний доступ. Внутри ГАУ СО «ФСЦ «Урожай» к разряду потребителей персональных данных относятся Работники функциональных структурных подразделений, которым эти данные необходимы для выполнения должностных обязанностей:

- заместители директора;
- работники бухгалтерии;
- начальник организационно-кадрового отдела;
- старший инструктор-методист;
- инструктора-методисты, инструктора по спорту.

В отделе кадров хранятся личные карточки Работников, работающих в настоящее время. Для этого используются специально оборудованные шкафы или сейфы, которые запираются. Личные карточки формы Т-2 располагаются в контейнерах. После увольнения документы по личному составу передаются на хранение в архив ГАУ СО «ФСЦ «Урожай».

5. Передача персональных данных

При передаче персональных данных Работника Оператор должен соблюдать следующие требования:

Передача внешнему потребителю:

- передача персональных данных от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных;

- при передаче персональных данных Работника потребителям (в том числе и в коммерческих целях) за пределы ГАУ СО «ФСЦ «Урожай» Оператор не должен сообщать эти данные третьей стороне без письменного согласия Работника, за исключением случаев когда это необходимо в целях предупреждения угрозы жизни и здоровью Работника или в случаях, установленных Федеральным законом;

- ответы на правомерные письменные запросы других фирм, учреждений и организаций даются с разрешения директора, его заместителей и только в письменной форме и в том объеме, который позволяет не разглашать излишний объем персональных сведений;

- не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.

Передача внутреннему потребителю. Оператор вправе разрешать доступ к персональным данным Работников. Потребители персональных данных должны подписать обязательство о неразглашении персональных данных Работников.

6. Защита персональных данных

Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

Защита персональных данных представляет собой жестко регламентированный технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности предприятия.

6.1. Внутренняя защита

Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документами и базами данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий руководителями и специалистами предприятия.

Для защиты персональных данных Работников соблюдается ряд мер:

6.1.1. Защита данных на бумажных носителях (несгораемые сейфы).

6.1.2. Защита информации на электронных носителях

- коды;
- пароли;
- доступы;
- строгое избирательное и обоснованное распределение документов и информации между Работниками;
- рациональное размещение рабочих мест Работников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание Работниками требований нормативно - методических документов по защите информации и сохранении тайны;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- определение и регламентация состава Работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;
- организация порядка уничтожения информации;

- своевременное выявление нарушения требований разрешительной системы доступа Работниками подразделения;
- воспитательная и разъяснительная работа с Работниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- не допускается выдача личных дел Работников на рабочие места руководителей. Личные дела могут выдаваться на рабочие места только директору, и в исключительных случаях, по письменному разрешению директора, необходимые данные и документы из личного дела руководителю структурного подразделения;
- персональные компьютеры, в которых содержатся персональные данные, защищены паролями доступа.
- персональные данные на бумажных носителях хранятся в шкафах, в помещениях, закрываемых на замок; доступ к ним ограничен.

6.2. Внешняя защита

Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лиц, пытающихся совершить несанкционированный доступ и овладение информацией.

Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности предприятия, посетители, Работники других организационных структур.

Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в ГАУ СО «ФСЦ «Урожай».

Для защиты персональных данных Работников соблюдается ряд мер:

- порядок приема, учета и контроля деятельности ГАУ СО «ФСЦ «Урожай»;
- ограничение доступа к АРМ пользователей;
- доступ к информационным базам от внешних угроз защищен комплексом программно-технических средств.

7. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

Персональная ответственность - одно из главных требований к организации функционирования системы защиты персональной информации и является обязательным условием обеспечения эффективности этой системы.

Руководитель, разрешающий доступ Работника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

Каждый Работник предприятия, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) влечет дисциплинарную, административную, гражданско-правовую или уголовную ответственность граждан и юридических лиц.

ПОЛОЖЕНИЕ **об обработке и защите персональных данных занимающихся**

1. Общие положения

Настоящее Положение устанавливает порядок приема, учета, сбора, поиска, обработки, накопления и хранения документов, содержащих сведения, отнесенные к персональным данным занимающихся ГАУ СО «ФСЦ «Урожай» (далее – «Оператор»).

Цель

Обеспечение уважения прав и основных свобод каждого сотрудника, и занимающегося при обработке его персональных данных, в том числе защиты прав, неприкосновенность частной жизни, личную и семейную тайну.

Настоящее Положение является развитием комплекса мер, направленных на обеспечение защиты персональных данных, хранящихся у Оператора, посредством планомерных действий по совершенствованию организации труда.

Основания

Основанием для разработки данного Положения являются:

- Конституция РФ;
- Федеральный закон от 19.12.2005 № 16-ФЗ «О ратификации конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;
- Трудовой Кодекс РФ № 197-ФЗ от 01.02.2002 г., ст.ст. 85-90;
- Кодекс РФ об административных правонарушениях № 195-ФЗ от 30.12.2001 г.;
- Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
- Указ Президента РФ № 188 от 06.09.1997 г. «Об утверждении перечня сведений конфиденциального характера».
- Постановление Правительства РФ от 17.11.2007 г. №781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;
- «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных», утверждены заместителем директора ФСТЭК РФ 15.02.2008 г.;
- «Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» утверждены заместителем директора ФСТЭК РФ 15.02.2008 г.;
- Положение о методах и способах защиты информации в информационных системах персональных данных (Приложение к Приказу ФСТЭК РФ от 5 февраля 2010 г. № 58);

2. Понятие и состав персональных данных

1.1. Персональные данные занимающегося - сведения о фактах, событиях и обстоятельствах жизни занимающегося, позволяющие идентифицировать его личность, необходимые администрации учреждения (далее - администрация) в связи с отношениями и воспитанием занимающегося и касающиеся занимающегося.

К персональным данным занимающегося относятся:

- сведения, содержащиеся в свидетельстве о рождении, паспорте или ином документе, удостоверяющем личность;
- информация, содержащаяся в личном деле занимающегося;
- информация, содержащаяся в личном деле занимающегося, лишенного родительского попечения;
- сведения, содержащиеся в документах воинского учета (при их наличии);
- информация об успеваемости;
- информация о состоянии здоровья;
- документ о месте проживания;

- иные сведения, необходимые для определения отношений обучения и воспитания.

1.2. Администрация может получить от самого занимающегося данные о:

- фамилии, имени, отчестве, дате рождения, месте жительства занимающегося;

- № школы, класс, где проходит обучение;

- фамилии, имени, отчестве родителей (законных представителей) занимающегося, место работы.

1.3. Иные персональные данные занимающегося, необходимые в связи с отношениями тренировочного процесса и воспитания, администрация может получить только с письменного согласия одного из родителей (законного представителя). К таким данным относятся документы, содержащие сведения, необходимые для предоставления занимающемуся гарантий и компенсаций, установленных действующим законодательством:

- документы о составе семьи;

- документы о состоянии здоровья (сведения об инвалидности, о наличии хронических заболеваний и т. п.);

- документы, подтверждающие право на дополнительные гарантии и компенсации по определенным основаниям, предусмотренным законодательством (родители-инвалиды, неполная семья, ребенок-сирота и т. п.).

1.4. В случаях, когда администрация может получить необходимые персональные данные занимающегося только у третьего лица, она должна уведомить об этом одного из родителей (законного представителя) заранее и получить от него письменное согласие.

1.5. Администрация обязана сообщить одному из родителей (законному представителю) о целях, способах и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа одного из родителей (законного представителя) дать письменное согласие на их получение.

1.6. Персональные данные занимающегося являются конфиденциальной информацией и не могут быть использованы администрацией или любым иным лицом в личных целях.

1.7. При определении объема и содержания персональных данных занимающегося администрация руководствуется Конституцией Российской Федерации, федеральными законами и настоящим Положением.

2. Хранение, обработка и передача персональных данных занимающегося

2.1. Обработка персональных данных занимающегося осуществляется для обеспечения соблюдения законов и иных нормативных правовых актов в целях воспитания занимающегося, обеспечения его личной безопасности, контроля качества формирования, пользования льготами, предусмотренными законодательством Российской Федерации и локальными актами администрации.

2.2. Право доступа к персональным данным занимающегося имеют:

- работники министерства молодежной политики, спорта и туризма Саратовской области (при наличии соответствующих полномочий, установленных приказом министерства молодежной политики, спорта и туризма Саратовской области);

- директор учреждения;

- заместитель директора по спортивно-массовой работе;

- главный бухгалтер;

- начальники отдела физкультурно-массовой работы и отдела методической работы;

- инструктор по спорту (только к персональным данным занимающихся своей группы);

- инструктор-методист ФСО.

2.3. Директор учреждения осуществляет прием занимающегося в учреждение. Директор учреждения может передавать персональные данные занимающегося третьим лицам, только если это необходимо в целях предупреждения угрозы жизни и здоровья занимающегося, а также в случаях, установленных федеральными законами.

2.4. Инструктор по спорту:

- оформляет списки групп занимающихся и вносит в них необходимые данные;

- предоставляет свободный доступ родителям (законным представителям) к персональным данным занимающегося на основании письменного заявления. К заявлению прилагается:

- родителем: копия документа, удостоверяющего личность;
- законным представителем: копия удостоверения опекуна (попечителя).

2.5. Не имеет права получать информацию о занимающемся родителе, лишенный или ограниченный в родительских правах на основании вступившего в законную силу постановления суда.

2.6. Главный бухгалтер имеет право доступа к персональным данным занимающегося в случае, когда исполнение им своих должностных обязанностей или трудовых обязанностей работников бухгалтерии по отношению к занимающемуся (предоставление льгот, установленных законодательством) зависит от знания персональных данных занимающегося.

2.7. При передаче персональных данных занимающегося директор, заместитель директора по спортивно-массовой работе, главный бухгалтер, начальники отдела физкультурно-массовой работы и отдела методической работы, инструктора по спорту, инструктора-методисты ФСО обязаны:

- предупредить лиц, получающих данную информацию, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены;
- потребовать от этих лиц письменное подтверждение соблюдения этого условия.

2.8. Иные права, обязанности, действия работников, в трудовые обязанности которых входит обработка персональных данных занимающегося, определяются трудовыми договорами и должностными инструкциями.

2.9. Все сведения о передаче персональных данных занимающихся регистрируются в Журнале учета передачи персональных данных занимающихся учреждения в целях контроля правомерности использования данной информации лицами, ее получившими.

3. Обязанности работников администрации, имеющих доступ к персональным данным занимающегося

3.1. Работники администрации, имеющие доступ к персональным данным занимающегося, обязаны:

- не сообщать персональные данные занимающегося третьей стороне без письменного согласия одного из родителей (законного представителя), кроме случаев, когда в соответствии с федеральными законами такого согласия не требуется;
- использовать персональные данные занимающегося, полученные только от него лично или с письменного согласия одного из родителей (законного представителя);
- обеспечить защиту персональных данных занимающегося от их неправомерного использования или утраты, в порядке, установленном законодательством Российской Федерации;
- соблюдать требование конфиденциальности персональных данных занимающегося;
- исключать или исправлять по письменному требованию одного из родителей (законного представителя) занимающегося его недостоверные или неполные персональные данные, а также данные, обработанные с нарушением требований законодательства;
- ограничивать персональные данные занимающегося при передаче уполномоченным работникам правоохранительных органов или работникам министерства только той информацией, которая необходима для выполнения указанными лицами их функций;
- запрашивать информацию о состоянии здоровья занимающегося только у родителей (законных представителей);
- обеспечить занимающемуся или одному из его родителей (законному представителю) свободный доступ к персональным данным занимающегося, включая право на получение копий любой записи, содержащей его персональные данные;
- предоставить по требованию одного из родителей (законного представителя) занимающегося полную информацию о его персональных данных, обрабатываемых оператором.

3.2. Лица, имеющие доступ к персональным данным занимающегося, не вправе:

- получать и обрабатывать персональные данные занимающегося о его религиозных и иных убеждениях, семейной и личной жизни;
- предоставлять персональные данные занимающегося в коммерческих целях.

4. Права и обязанности занимающегося, родителя (законного представителя)

4.1. В целях обеспечения защиты персональных данных, хранящихся у администрации, занимающийся, родитель (законный представитель) имеют право на:

- требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований законодательства.

- требование об извещении администрацией всех лиц, которым ранее были сообщены неверные или неполные персональные данные занимающегося, обо всех произведенных в них исключениях, исправлениях или дополнениях;

- обжалование в суд любых неправомерных действий или бездействия администрации при обработке и защите персональных данных занимающегося;

4.2. Родитель (законный представитель) обязан сообщать администрации сведения, которые могут повлиять на принимаемые администрацией решения в отношении занимающегося.

4.3. Персональные данные занимающихся должны храниться в шкафах (в помещениях, закрываемых на замок) на бумажных носителях и на электронных носителях с ограниченным доступом:

5. Ответственность администрации и ее сотрудников

5.1. Защита прав занимающегося, установленных законодательством Российской Федерации и настоящим Положением, осуществляется судом в целях пресечения неправомерного использования персональных данных занимающегося, восстановления нарушенных прав и возмещения причиненного ущерба, в том числе морального вреда.

5.2. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных занимающегося, привлекаются к дисциплинарной и материальной ответственности, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

ИНСТРУКЦИЯ **ответственного за организацию обработки персональных данных**

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Ответственный за организацию обработки персональных данных организует выполнение мероприятий по защите информации на автоматизированных рабочих местах, обрабатывающих персональные данные согласно Приложению № 1 к приказу ГАУ СО «ФСЦ «Урожай» (далее - Учреждение), обеспечивает сохранность защищаемой информации, настройку системы защиты информации от несанкционированного доступа (СЗИ НСД) (при ее наличии) в соответствии с разрешительной системой доступа пользователей к информационным ресурсам автоматизированных рабочих мест.

1.2. Администратор безопасности назначается приказом директора учреждения (далее – директор). Освобождение от исполнения обязанностей администратора безопасности согласовывается с директором.

1.3. В практической деятельности о информации руководствуется требованиями федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 17 ноября 2007 года № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», постановления Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», совместного приказа ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 года № 55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных», нормативными правовыми документами, разработанными ФСТЭК России, комплектом документации СЗИ НСД (при ее наличии) и настоящей должностной Инструкцией.

2. ОСНОВНЫЕ ФУНКЦИИ

2.1. Основными функциями администратора безопасности являются:

2.1.1. Организация работ по предотвращению неправомерного доступа лиц к защищаемой информации.

2.1.2. Выявление возможных каналов утечки защищаемой информации за счет несанкционированного доступа к информации в процессе деятельности и внесение предложений по их закрытию.

2.1.3. Установка, настройка и поддержание в исправном состоянии технических и программных средств автоматизированных рабочих мест в Учреждении. Настройка и эксплуатация технических и программных средств защиты информации от несанкционированного доступа.

2.1.4. Регистрация пользователей в системе, присвоение или изменение полномочий доступа пользователей к ресурсам автоматизированных рабочих мест в соответствии с разрешительной системой доступа к информационным ресурсам.

2.1.5. Контроль соответствия действий пользователей с заданиями на работы.

2.1.6. Резервное копирование системной информации автоматизированных рабочих мест, ведение двух копий программных средств СЗИ НСД (при ее наличии) и их периодическое обновление и контроль работоспособности.

2.1.7. Обновление программного обеспечения автоматизированных рабочих мест, проверка целостности данных.

2.1.8. Проверка системы автоматизированных рабочих мест на отсутствие вирусов.

3. ПРАВА И ОБЯЗАННОСТИ

3.1. Администратор безопасности обязан:

3.1.1. Четко 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.

3.1.2. Знать перечень автоматизированных рабочих мест, предназначенных для обработки персональных данных, и перечень задач, решаемых с их использованием.

3.1.3. Организовывать разработку и обеспечивать выполнение мер по защите информации при ее обработке на автоматизированных рабочих местах.

3.1.4. Осуществлять настройку системы защиты информации от несанкционированного доступа в соответствии с установленным классом защищенности и разрешительной системой доступа пользователей к информационным ресурсам автоматизированных рабочих мест.

3.1.5. В случаях неисправности или нарушения целостности СЗИ НСД, выявления попыток несанкционированного доступа к защищаемой информации немедленно прекратить работу, ограничить доступ в помещение и поставить в известность ответственного по защите информации.

3.1.6. В случае выявления некачественных действий пользователей, не несущих в себе угроз для безопасности информации, поставить в известность об этом ответственного по защите информации, временно заблокировать возможность работы этого пользователя и организовать дополнительные занятия с ним.

3.1.7. Присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию автоматизированных рабочих мест.

3.1.8. Контролировать соответствие состава автоматизированных рабочих мест реальным конфигурациям и вести учет изменений аппаратно-программной конфигурации (архив заявок, на основании которых были произведены данные изменения на автоматизированных рабочих местах).

3.1.9. Хранить, осуществлять прием и выдачу персональных идентификаторов пользователей (при их наличии), осуществлять контроль правильности использования персональных идентификаторов оператору автоматизированного рабочего места.

3.1.10. Проводить работу по выявлению возможных каналов вмешательства в процесс функционирования автоматизированных рабочих мест и осуществления НСД к информации и техническим средствам автоматизированных рабочих мест. При выявлении таковых сообщать о них ответственному по защите информации.

3.1.11. Проводить инструктаж пользователей автоматизированных рабочих мест по правилам работы с используемой СЗИ НСД.

3.1.12. При увольнении или переводе пользователей в другие подразделения оперативно изменять учетные реквизиты защиты: пароли, идентификаторы (если это необходимо).

3.1.13. При изменении программной среды или пользователей проводить тестирование всех функций СЗИ НСД, имитируя попытки НСД.

3.1.14. В случае необходимости обновлять эксплуатируемое либо устанавливать новое программное обеспечение.

3.1.15. Проверять все новые данные на отсутствие вирусов. Регулярно обновлять базы данных антивирусных средств.

3.1.16. Не реже одного раза в год проводить тестирование всех функций СЗИ НСД (при ее наличии) с помощью специальных программных средств.

3.2. Администратор безопасности информации имеет право:

3.2.1. Требовать от пользователей автоматизированных рабочих мест соблюдения установленных технологий обработки информации и выполнения инструкций по обеспечению безопасности информации.

3.2.2. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов автоматизированных рабочих мест.

3.2.3. Обращаться к ответственному по защите информации с требованием прекращения работы пользователя на автоматизированном рабочем месте при несоблюдении установленной технологии обработки информации и невыполнении требований по безопасности информации.

3.2.4. Выступать с предложениями по совершенствованию мер защиты информации.

3.2.5. Обращаться к ответственному по защите информации для оказания необходимой технической и методологической помощи в своей работе.

4. ОТВЕТСТВЕННОСТЬ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

4.1. На администратора безопасности информации возлагается персональная ответственность за качество проводимых им работ по обеспечению защиты информации, обрабатываемой на автоматизированных рабочих местах.

4.2. Администратор безопасности информации отвечает за соответствие настройки СЗИ НСД (при ее наличии) требованиям установленных для автоматизированных рабочих мест классов защищенности.

4.3. Администратор безопасности информации несет ответственность по действующему законодательству Российской Федерации за разглашение сведений ограниченного распространения, ставших известными ему по роду работы.

5. ПОРЯДОК АДМИНИСТРИРОВАНИЯ РАБОТЫ НА АВТОМАТИЗИРОВАННЫХ РАБОЧИХ МЕСТАХ

5.1. Работа с СЗИ НСД должна осуществляться в соответствии с комплектом документации СЗИ НСД.

5.2. Проанализировать записи журналов входа пользователей и их работы на автоматизированных рабочих местах. Обращать особое внимание на попытки осуществления "скрытого" несанкционированного переноса (копирования) защищаемой информации на любые носители (разделы, каталоги). Характерными признаками осуществления таких действий является работа с защищаемой информацией и создание (редактирование) файлов на других носителях (разделах, каталогах в пределах одного сеанса работы).

5.3. Проанализировать записи журнала попыток несанкционированного входа на автоматизированных рабочих местах.

5.4. Проанализировать полномочия каждого пользователя автоматизированных рабочих мест, соответствие их значений ранее установленным.

5.5. Проанализировать и убедиться в неизменности программной среды автоматизированных рабочих мест. На ПЭВМ автоматизированных рабочих мест должны отсутствовать средства разработки и отладки программ.

ИНСТРУКЦИЯ

оператора по обработке персональных данных на автоматизированном рабочем месте

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая инструкция разработана в соответствии с требованиями «Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденного Постановлением Правительства РФ от 17.11.2007 г. № 781 и «Основных мероприятий по организации и техническому обеспечению безопасности персональных данных», утвержденных ФСТЭК России 15.02.2008 г.

Операторами автоматизированных рабочих мест являются сотрудники, допущенные приказом директора ГАУ СО «ФСЦ «Урожай» (далее – директор) к обработке персональных данных на автоматизированных рабочих местах.

2. ФУНКЦИИ

2.1. Основными функциями пользователя являются:

2.1. Выполнение мероприятий, направленных на предотвращение неправомерного доступа лиц к защищаемой информации.

2.2. Обеспечение установленного режима обработки персональных данных на автоматизированных рабочих местах.

2.3. Комиссионное удаление защищаемой информации с жестких дисков ПЭВМ, совместно с руководителем подразделения, ответственным за безопасность информации подразделения (администратором безопасности).

2.4. Вывод (запись) данных, полученных на основе защищаемой информации, либо данных, содержащих защищаемую информацию, на печать или съемные машинные носители информации (МНИ).

2.5. Проверка новых данных на отсутствие вирусов.

2.6. Ведение учета работы пользователя АС в соответствующем журнале учета.

2.7. Ведение учета съемных носителей информации с персональными данными в соответствующих журналах учета.

3. ФУНКЦИОНАЛЬНЫЕ ОБЯЗАННОСТИ

3.1. Каждый сотрудник, участвующий в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным АРМ, несет персональную ответственность за свои действия и обязан:

3.1.1. Строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами АРМ.

3.1.2. Знать и строго выполнять правила работы со средствами защиты информации, установленными на АРМ.

3.1.3. В случае неисправности средств защиты информации от несанкционированного доступа, выявление попыток несанкционированного доступа к защищаемой информации, либо обнаружения следов вскрытия технических средств, входящих в состав автоматизированного рабочего места, немедленно прекратить работу, ограничить доступ в помещение, поставить в известность администратора безопасности информации и ответственного за защиту информации.

3.1.4. Регулярно производить смену личного пароля доступа (не реже 1 раза в 3 месяца).

3.1.5. Передавать для хранения установленным порядком свои реквизиты разграничения доступа только начальнику своего подразделения. Запрещается сообщать кому-либо свой пароль доступа.

3.1.6. Выполнять требования по антивирусной защите в части касающейся действий пользователей. Проверять все новые данные, вводимые со съемных МНИ на отсутствие вирусов.

3.1.7. Немедленно вызывать администратора безопасности (ответственного за безопасность) информации и ставить в известность начальника своего подразделения в случае

утери личных реквизитов доступа или при подозрении компрометации личных паролей, а также при обнаружении:

- нарушений целостности пломб (наклеек) на аппаратных средствах АРМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (НСД) к ресурсам АРМ;

- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АРМ;

- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов или периферийных устройств (дисководов, принтера и т.п.) АРМ, а также перебоев в системе электроснабжения;

- некорректного функционирования установленных на АРМ технических средств защиты;

- непредусмотренных техническим паспортом АРМ отводов кабелей и подключенных устройств.

3.2. Оператору категорически ЗАПРЕЩАЕТСЯ:

3.2.1. Использовать компоненты программного и аппаратного обеспечения АРМ в неслужебных целях.

3.2.2. Самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств АРМ или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные техническим паспортом АРМ.

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

3.2.4. Записывать и хранить защищаемую информацию на неучтенных носителях информации (гибких магнитных дисках, компакт-дисках, флэш-накопителях, внешних ЖМД и т.п.).

3.2.5. Оставлять включенным без присмотра АРМ, не активизировав средства защиты информации от НСД. Передавать включенную ПЭВМ другому исполнителю без перезагрузки.

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

3.2.7. Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок - ставить в известность администратора безопасности информации и начальника отдела, эксплуатирующего АРМ.

4. ПОРЯДОК ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЯ ПРИ РАБОТЕ

4.1. Общие положения и требования:

4.1.1. Обработка персональных данных разрешается на основании распоряжения руководителя подразделения.

4.1.2. На период обработки защищаемой информации в помещении, в котором расположены автоматизированные рабочие места, могут находиться только лица, допущенные к обрабатываемой информации.

4.1.3. В начале и по окончании работы проверить сохранность печатей системного блока ПК.

4.1.4. Ввод информации со съемных МНИ осуществляется только после их проверки антивирусными средствами, которые должны периодически обновляться,

4.1.5. Файлы с защищаемой информацией должны храниться только в установленных для этого каталогах (разделах). Запрещается перенос (копирование) файлов в каталоги (разделы) с открытой информацией.

4.1.6. По окончании обработки защищаемой информации или при передаче управления другому допущенному оператору необходимо уничтожить остаточную и не нужную информацию на жестком магнитном диске ПК или съемных МНИ.

4.1.7. При утере пароля или электронного идентификатора **НЕМЕДЛЕННО** прекратить работу, поставить в известность администратора безопасности информации и ответственного за защиту информации.