

**Бюджетное учреждение Омской области
"КОМПЛЕКСНЫЙ ЦЕНТР СОЦИАЛЬНОГО
ОБСЛУЖИВАНИЯ НАСЕЛЕНИЯ ОМСКОГО РАЙОНА"**

П Р И К А З

9 января 2023 года

№ 5/1-4

г. Омск

"Об утверждении внутренних нормативно-правовых актов по защите персональных данных" в бюджетном учреждении Омской области "Комплексный центр социального обслуживания населения Омского района"

В целях обеспечения безопасности персональных данных при их обработке в бюджетном учреждении Омской области "Комплексный центр социального обслуживания населения Омского района" и выполнения требований законодательства Российской Федерации в области защиты персональных данных, руководствуясь Уставом,

ПРИКАЗЫВАЮ:

1. Утвердить:

1) Политику Учреждения в отношении обработки персональных данных (приложение № 1);

2) Положение об обработке персональных данных в Учреждении (приложение № 2);

3) Инструкцию о порядке резервирования и восстановления работоспособности технических средств, программного обеспечения и баз данных в Учреждении (приложение № 3);

4) Инструкцию ответственного лица за организацию обработки персональных данных в Учреждении (приложение № 4);

5) Инструкцию по организации антивирусной защиты в Учреждении (приложение № 5);

6) Инструкцию по порядку учета и хранению документов, содержащих персональные данные, в Учреждении (приложение № 6);

7) Инструкцию по обеспечению безопасности эксплуатации средств криптографической защиты информации (СКЗИ) в Учреждении (приложение № 7);

8) Инструкцию по порядку учета и хранению съемных носителей конфиденциальной информации (персональных данных) в Учреждении (приложение № 8);

9) Инструкцию пользователя информационных систем персональных

Приложение № 1
к приказу БУ "КЦСОН
Омского района"
от 09.01.2023 № 5/1-п

ПОЛИТИКА
обработки персональных данных
в бюджетном учреждении Омской области "Комплексный центр социального
обслуживания населения Омского района"

I. ОБЩИЕ ПОЛОЖЕНИЯ

1. Общие положения

1.1. Настоящая Политика обработки персональных данных (далее – Политика обработки ПДн) в бюджетном учреждении Омской области "Комплексный центр социального обслуживания населения Омского района" разработана в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом от 27 июля 2006 года № 149-ФЗ "Об информации, информационных технологиях и о защите информации", Федеральным законом 27 июля 2006 года № 152-ФЗ "О персональных данных", постановлением Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", иными федеральными законами и нормативно-правовыми актами.

1.2. Политика разработана с учетом требований Конституции Российской Федерации, законодательных и иных нормативных правовых актов Российской Федерации в области персональных данных.

1.3. Политика обработки персональных данных разработана с целью обеспечения защиты прав и свобод субъекта персональных данных при обработке его ПДн.

1.4. Положения Политики служат основой для разработки локальных нормативных актов, регламентирующих в БУ "КЦСОН Омского района" вопросы обработки персональных данных работников и других субъектов персональных данных.

В Политике используются следующие основные понятия:

1. **Автоматизированная обработка персональных данных** – обработка персональных данных с помощью средств вычислительной техники;
2. **Блокирование персональных данных** – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);
3. **Информационная система персональных данных** – совокупность содержащихся в базах данных персональных данных, и обеспечивающих их обработку информационных технологий и технических средств;

- ведение текущего бухгалтерского и налогового учёта, формирование, изготовление и своевременная подача бухгалтерской, налоговой и статистической отчетности;
 - выполнение требований законодательства по определению порядка обработки и защиты ПДн граждан, являющихся работниками, клиентами или контрагентами (далее – субъекты персональных данных).
- 2) осуществления прав и законных интересов БУ "КЦСОН Омского района" в рамках осуществления видов деятельности, предусмотренных Уставом и иными локальными нормативными актами центра, или третьих лиц либо достижения общественно значимых целей;
- 3) в иных законных целях.

3. Правовое основание обработки персональных данных

Обработка ПДн осуществляется на основе следующих федеральных законов и нормативно-правовых актов:

- 1) Конституции Российской Федерации;
- 2) Трудового кодекса Российской Федерации;
- 3) Федерального закона от 27 июля 2006 года № 152-ФЗ "О персональных данных";
- 4) Федерального закона "Об информации, информационных технологиях и о защите информации" от 27.07.2006 № 149-ФЗ.
- 5) Положения "Об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации. Утверждено постановлением Правительства Российской Федерации" от 15 сентября 2008 года № 687.
- 6) Постановление от 1 ноября 2012 г. № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";
- 7) 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";
- 8) Приказ Роскомнадзора от 05 сентября 2013 г. № 996 "Об утверждении требований и методов по обезличиванию персональных данных";
- 9) Иные нормативные правовые акты Российской Федерации и нормативные документы уполномоченных органов государственной власти.

4. Перечень действий с персональными данными

При обработке ПДн Оператор будет осуществлять следующие действия с ПДн: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

5. Состав обрабатываемых персональных данных

5.1. Обработке Оператором подлежат ПДн следующих субъектов ПДн:

постановлением Правительства от 01 ноября 2012 года № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", и другими нормативными правовыми актами, если иное не предусмотрено федеральными законами. К таким мерам относятся:

- назначение Оператором ответственного за организацию обработки персональных данных;
- издание Оператором документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;
- применение правовых, организационных и технических мер по обеспечению безопасности персональных данных;
- осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону "О персональных данных" и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике Оператора в отношении обработки персональных данных, локальным актам Оператора;
- определение оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона "О персональных данных", соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных";
- ознакомление сотрудников Оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику Оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных сотрудников.

7.2. Оператор при обработке персональных данных принимает необходимые правовые, организационные и технические меры или обеспечивает 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.

8. Право субъекта персональных данных на доступ к его персональным данным

- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка поручена или будет поручена такому лицу.

8.5. Если субъект персональных данных считает, что оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона "О персональных данных" или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие оператора в орган, уполномоченный по вопросам защиты прав субъектов персональных данных, или в судебном порядке.

8.6. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

Положение

об обработке персональных данных в бюджетном учреждении Омской области "Комплексный центр социального обслуживания населения Омского района" (далее – Учреждение)

Общие положения

Настоящее Положение об обработке персональных данных (далее - Положение) в Учреждении разработано в соответствии с Конституцией Российской Федерации, Федеральным законом "Об информации, информационных технологиях и о защите информации", Федеральным законом "О персональных данных".

Цель разработки Положения – определение порядка обработки персональных данных в Учреждении, обеспечение защиты прав и свобод субъектов 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.

Настоящее Положение вступает в силу с момента его утверждения приказом руководителя Учреждения. Срок действия не ограничен. Положение действует до принятия нового. Все работники Учреждения, имеющие доступ к персональным данным, должны быть ознакомлены с настоящим Положением под роспись.

Режим конфиденциальности персональных данных снимается только в случаях их обезличивания.

Основные понятия и состав персональных данных

Для целей настоящего Положения используются следующие основные понятия:

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;

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

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;

распространение персональных данных – действия, направленные на

третьей стороны, то субъект персональных данных должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Сотрудник 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.

Порядок обработки персональных данных

Субъект персональных данных предоставляет сотруднику Учреждения 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.

В соответствии со ст. 6 ФЗ-152 "О Персональных данных" сотрудники Учреждения при обработке персональных данных должны соблюдать следующие общие требования:

Обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных.

Письменное согласие субъекта персональных данных на обработку своих персональных данных должно включать в себя:

фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

наименование и адрес оператора, получающего согласие субъекта персональных данных;

цель обработки персональных данных;

перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

срок, в течение которого действует согласие, а также порядок его отзыва.

Обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей.

Обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем.

Обработка персональных данных необходима для осуществления прав

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.

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

Уничтожение персональных данных

Уничтожение документов, содержащих персональные данные, в том числе черновиков, бракованных листов и испорченных копий, должно производиться сотрудниками, выполняющими обработку персональных данных, с последующим составлением акта об уничтожении.

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.

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

Разрешение на уничтожение персональных данных дает руководитель Учреждения.

Доступ к персональным данным

Доступ сотрудников к персональным данным осуществляется на основании разрешительной системы доступа.

Копировать и делать выписки персональных данных разрешается исключительно в служебных целях.

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

Правила работы с обезличенными данными

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).

Обезличивание персональных данных в Учреждении при обработке

персональных данных либо осуществление доступа к персональным данным;
актуальность перечня должностей сотрудников Учреждения, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных;

соблюдение прав субъектов персональных данных, чьи персональные данные обрабатываются в информационных системах персональных данных Учреждения;

соблюдение обязанностей сотрудников Учреждения, 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 уведомлению, 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 Учреждения;

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 сотрудниками Учреждения положений действующего законодательства Российской Федерации в области персональных данных;

знания и соблюдение сотрудниками Учреждения положений локальных актов Учреждения в области обработки и обеспечения безопасности персональных данных;

знания и соблюдение сотрудниками Учреждения инструкций, руководств и иных эксплуатационных документов на применяемые средства автоматизации, в том числе программное обеспечение, и средства защиты информации;

соблюдение сотрудниками Учреждения конфиденциальности персональных данных;

актуальность локальных актов Учреждения в области обеспечения безопасности персональных данных, в том числе в Технических паспортах информационных систем персональных данных;

соблюдение сотрудниками Учреждения требований по обеспечению безопасности персональных данных;

наличие локальных актов Учреждения, технической и

неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях.

Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

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.

Положение об обработке персональных данных в бюджетном учреждении Омской области "Комплексный центр социального обслуживания населения Омского района"

разработала Чучалина С.С., юрисконсульт

 С.С. Чучалина 09.01.23
(подпись) (расшифровка) (дата)

СОГЛАСОВАНО:

Ю.Н. Кузменко, заместитель руководителя

 Ю.Н. Кузменко 09.01.2023
(подпись) (расшифровка) (дата)

Г.Ю. Распутина, главный бухгалтер

 Г.Ю. Распутина 09.01.2023
(подпись) (расшифровка) (дата)

Инструкция

о порядке резервирования и восстановления работоспособности технических средств, программного обеспечения и баз данных в бюджетном учреждении Омской области "Комплексный центр социального обслуживания населения Омского района" (далее – Учреждение) .

Данная Инструкция определяет действия, связанные с мерами и средствами поддержания непрерывной работы и восстановления работоспособности информационных систем в Учреждении.

Настоящая Инструкция регламентирует:

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

Действие настоящей Инструкции распространяется на Администратора баз данных, ответственного за резервное копирование информации.

Меры обеспечения надежной работы и восстановления ресурсов при возникновении инцидентов

1.1. Технические меры

1.1.1. 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;
- системы контроля физического доступа.

Системы жизнеобеспечения ИСПДн включают:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

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

1.1.3. 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

управления базами данных (при использовании таковой).

Все файлы, входящие в состав резервной копии, должны архивироваться в один архив с присвоением имени архива в формате время-дата (например 18.00 21.11.2016).

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

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

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.

Порядок проведения восстановления информации

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

Восстановление информации следует проводить из наиболее актуальной резервной копии.

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).

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).

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

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.

Инструкция

ответственного за организацию обработки персональных данных в бюджетном учреждении Омской области "Комплексный центр социального обслуживания населения Омского района" (далее – Учреждение).

Общие положения

Настоящая Инструкция разработана в соответствии со ст. 22.1 Федерального закона от 27.07.2006 г. № 152-ФЗ "О персональных данных" и определяет обязанности, полномочия и ответственность лиц, ответственных за организацию обработки персональных данных в Учреждении.

Ответственный за организацию обработки персональных данных назначается приказом руководителя из числа сотрудников Учреждения.

Ответственный за организацию обработки персональных данных подчиняется руководителю.

Ответственный за организацию обработки персональных данных в своей работе руководствуется настоящей Инструкцией, ФЗ-№ 152 от 27 июля 2006 года "О персональных данных", ФЗ-№ 149 от 27 июня 2006 года "Об информации, информационных технологиях и о защите информации", 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 15 сентября 2008 года № 687 "Об утверждении положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации", Приказом федеральной службы по техническому и экспортному контролю России от 05 февраля 2010 года № 58 "Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных", специальным требованиям и рекомендациям по технической защите конфиденциальной информации (СТР-К) и внутренними нормативно-правовыми актами по защите информации.

Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам обеспечения безопасности персональных данных и не исключает обязательного выполнения их требований.

Обязанности

Осуществлять внутренний контроль за соблюдением сотрудниками Учреждения (структурного подразделения) требований законодательства РФ при обработке персональных данных, внутренних положений, инструкций и других нормативно-правовых документов в области защиты информации.

Инструкция

по организации антивирусной защиты в бюджетном учреждении Омской области "Комплексный центр социального обслуживания населения Омского района" (далее – Учреждение).

Настоящая Инструкция предназначена для организации порядка проведения в Учреждении антивирусного контроля и предотвращения возникновения фактов заражения вредоносным программным обеспечением.

Данная Инструкция распространяется на всех пользователей и администраторов информационных систем персональных данных (далее - ИСПДн) в Учреждении.

Установка и обновление антивирусных средств.

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

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

Требования к проведению мероприятий по антивирусной защите:

- 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).

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

Контроль информации на съёмных носителях производится непосредственно перед её использованием.

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.

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

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

Внеочередной антивирусный контроль всех дисков и файлов

Инструкция

по порядку учета и хранению документов, содержащих персональные данные, в бюджетном учреждении Омской области "Комплексный центр социального обслуживания населения Омского района" (далее – Учреждение).

Общие положения

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

Действие настоящей Инструкции распространяется на сотрудников Учреждения, допущенных к обработке персональных данных.

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

Все находящиеся на хранении и в обращении документы с персональными данными в Учреждении подлежат учёту.

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

Учет и выдачу документов с персональными данными осуществляют сотрудники структурных подразделений, на которых возложены функции хранения документов, содержащих персональные данные. Факт выдачи документов фиксируется в журнале учета.

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 организацию обработки персональных данных о любых фактах нарушения требований настоящей Инструкции.

Бережно относиться к документам, содержащим персональные данные.

Обеспечивать физическую безопасность документов всеми разумными способами.

Извещать ответственного за обработку 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

Инструкция

по обеспечению безопасности эксплуатации средств криптографической защиты информации (СКЗИ) в бюджетном учреждении Омской области "Комплексный центр социального обслуживания населения Омского района" (далее – Учреждение).

Общие положения

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 Учреждении.

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

Обязанности Пользователя

Пользователь обязан соблюдать требования по обеспечению безопасности функционирования СКЗИ.

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

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

Пользователь обязан сдать НКИ по окончании срока действия сертификата ключа, а также в случае компрометации ключа.

Пользователь обязан немедленно уведомлять ответственного за организацию обработки персональных данных о компрометации криптографических ключей.

Пользователь обязан немедленно уведомлять ответственного за организацию обработки персональных данных о фактах утраты или недостачи СКЗИ, НКИ.

Порядок обращения со средствами криптографической защиты информации

Монтаж и установка СКЗИ осуществляются только ответственным за обеспечение информационной безопасности, либо организацией, имеющей необходимые лицензии. Все СКЗИ и НКИ должны учитываться в журнале.

Действия при компрометации действующих ключей и восстановлении конфиденциальной связи

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;

Увольнение (переназначение) сотрудников, имевших доступ к ключевой информации;

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 учёта 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).

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.

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

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

Ответственность Пользователя

Владелец ключа несет персональную ответственность за конфиденциальность личных ключевых носителей.

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

Инструкция

по порядку учета и хранению съемных носителей конфиденциальной информации (персональных данных) в бюджетном учреждении Омской области "Комплексный центр социального обслуживания населения Омского района" (далее – Учреждение).

Общие положения

Настоящая Инструкция разработана с целью обеспечения безопасности персональных данных при их хранении на съемных носителях.

Действие настоящей Инструкции распространяется на сотрудников Учреждения, допущенных к обработке персональных данных.

Основные термины, сокращения и определения

Администратор информационной системы персональных данных - технический специалист, обеспечивает ввод в эксплуатацию, поддержку и последующий вывод из эксплуатации ПО и оборудования вычислительной техники.

АРМ – автоматизированное рабочее место пользователя (ПК с прикладным ПО) для выполнения определенной производственной задачи.

ИБ – информационная безопасность - комплекс организационно-технических мероприятий, обеспечивающих конфиденциальность, целостность и доступность информации.

ИС – информационная система – система, обеспечивающая хранение, обработку, преобразование и передачу информации с использованием компьютерной и другой техники.

Носитель информации – любой материальный объект, используемый для хранения и передачи электронной информации. ПК – персональный компьютер.

ПО– программное обеспечение вычислительной техники.

ПО вредоносное – ПО или изменения в ПО, приводящие к нарушению конфиденциальности, целостности и доступности критичной информации.

Пользователь – работник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработке персональных данных и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

Порядок использования носителей информации

Под использованием носителей информации в ИС понимается их подключение к инфраструктуре ИС с целью обработки, приема/передачи информации между ИС и носителями информации.

осуществляется в порядке, установленном для документов данного типа.

В случае утраты или уничтожения съемных носителей конфиденциальной информации (персональных данных) либо разглашении содержащихся в них сведений немедленно ставится в известность руководитель Учреждения. На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы учета съемных носителей конфиденциальной информации (персональных данных).

Съемные носители конфиденциальной информации (персональных данных), пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с конфиденциальной информацией осуществляется "уполномоченной комиссией". По результатам уничтожения носителей составляется акт.

В случае увольнения или перевода работника в другое структурное подразделение, предоставленные носители конфиденциальной информации изымаются.

Запрещается

Использовать носители конфиденциальной информации в личных целях.

Передавать носители конфиденциальной информации другим лицам (за исключением администраторов ИС).

Хранить съемные носители с конфиденциальной информацией (персональными данными) вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

Выносить съемные носители с конфиденциальной информацией (персональными данными) из служебных помещений для работы с ними на дому и т. д.

Ответственность

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

Инструкция

пользователя информационных систем персональных данных по обеспечению безопасности персональных данных в бюджетном учреждении Омской области "Комплексный центр социального обслуживания населения Омского района" (далее – Учреждение).

Общие положения

Пользователь информационной системы персональных данных (далее - Пользователь) осуществляет обработку персональных данных в информационных системах персональных данных в Учреждении.

Пользователем является каждый работник Учреждения, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки персональных данных и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

Пользователь несет персональную ответственность за свои действия.

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 документами Учреждения по защите информации.

Обязанности пользователя

Знать и выполнять требования настоящей Инструкции и других внутренних нормативно-правовых документов, по защите персональных данных.

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

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.

Соблюдать требования парольной политики (Раздел 3).

Соблюдать правила при работе в сетях общего доступа и международного обмена - Интернет (Раздел 4).

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).

Обо всех выявленных нарушениях, связанных с информационной

Администратором информационной системы персональных данных при первом входе в систему.

Полная плановая смена паролей в информационной системе персональных данных проводится не реже одного раза в 3 месяца.

Правила формирования пароля:

Пароль не может содержать имя учетной записи пользователя или какую либо его часть.

Пароль должен состоять не менее чем из 8 символов.

В пароле должны присутствовать символы трех категорий из числа следующих четырех:

прописные буквы английского алфавита от А до Z;

строчные буквы английского алфавита от а до z; десятичные цифры (от 0 до 9);

символы, не принадлежащие алфавитно-цифровому набору (например, !, \$, #, %).

Запрещается использовать в качестве пароля имя входа в систему, простые пароли типа "123", "111", "qwerty" и им подобные, а также имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе;

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

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

Запрещается выбирать пароли, которые уже использовались ранее.

Правила ввода пароля:

Ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан;

Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

Правила хранения пароля:

Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;

Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем;

Лица, использующие паролирование, обязаны:

Четко знать и строго выполнять требования настоящей Инструкции и других руководящих документов по паролированию;

Своевременно сообщать Администратору информационной системы персональных данных об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия

Инструкция

администратора безопасности информационных систем персональных данных бюджетного учреждения Омской области "Комплексный центр социального обслуживания населения Омского района" (далее – Учреждение)

Общие положения

Настоящая Инструкция определяет обязанности, полномочия и ответственность администратора безопасности данных информационных систем персональных данных (далее – Администратор ИСПДн) по обеспечению безопасности персональных данных в Учреждении.

Администратор ИСПДн назначается приказом руководителя Учреждения.

Администратор ИСПДн подчиняется руководителю. Администратор ИСПДн в своей работе руководствуется настоящей Инструкцией, Положением о защите персональных данных, руководящими и нормативными документами ФСТЭК России и внутренними нормативно-правовыми актами по защите персональных данных.

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

Обязанности по обеспечению безопасности информации

Администратор ИСПДн обязан:

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

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

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;

Регламент

порядка действий сотрудников бюджетного учреждения Омской области
"Комплексный центр социального обслуживания населения Омского района"
(далее – Учреждение).

Настоящий Регламент разработан на основании и во исполнение Федерального закона РФ "О персональных данных" от 27.07.2006 г. № 152-ФЗ.

Целью настоящего Регламента является:

обеспечение прав субъектов персональных данных на доступ к их персональным данным, которые обрабатываются в Учреждении;

обеспечение прав уполномоченного органа по защите прав субъектов персональных данных на получение информации, необходимой ему для реализации полномочий по защите прав субъектов персональных данных;

упорядочение действий сотрудников Учреждения и при обращении либо при получении запроса субъекта персональных данных или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных.

Настоящий Регламент распространяется на сотрудников Учреждения, которые в рамках исполнения своих должностных обязанностей осуществляют прием и регистрацию обращений (запросов) субъектов персональных данных, а также уполномоченного органа по защите прав субъектов персональных данных, осуществляют рассмотрение обращений (запросов), подготовку и направление ответов на них.

Настоящий Регламент подлежит применению исключительно в случаях обращений либо при получении запросов субъектов персональных данных или их законных представителей, а также уполномоченного органа по защите прав субъектов персональных данных в рамках Федерального закона РФ "О персональных данных" от 27.07.2006 г. № 152-ФЗ.

Общие положения

Настоящий Регламент использует следующие сокращения:

ПДн – персональные данные;

ИСПДн – информационная система персональных данных.

Субъект ПДн – это физическое лицо, определенное или определяемое на основании любой относящейся к нему информации.

Законный представитель субъекта ПДн – это гражданин, который в силу закона выступает во всех учреждениях и организациях от имени и в защиту личных и имущественных прав и законных интересов недееспособных, ограниченно дееспособных граждан, либо дееспособных, но

предоставить возможность ознакомления с ПДн без взимания платы за это;

внести в ПДн необходимые изменения, уничтожить или блокировать соответствующие ПДн при предоставлении субъектом ПДн сведений, подтверждающих, что ПДн, которые относятся к соответствующему субъекту и обработку которых осуществляет Учреждение, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

прекратить обработку ПДн и уничтожить их в случае отзыва субъектом ПДн согласия на обработку своих ПДн;

о внесенных изменениях и предпринятых мерах уведомить субъекта ПДн и третьих лиц, которым ПДн этого субъекта были переданы;

уведомить субъекта ПДн об уничтожении ПДн;

В соответствии с п. 3 ч. 5 ст. 14 Федерального закона РФ "О персональных данных" от 27.07.2006 г. № 152-ФЗ право субъекта ПДн на доступ к своим ПДн ограничивается в случае, если предоставление ПДн нарушает конституционные права и свободы других лиц.

Действия сотрудников Учреждения при получении запроса субъекта ПДн

В соответствии с ч. 3 ст. 14 Федерального закона РФ "О персональных данных" от 27.07.2006 г. № 152-ФЗ запрос должен содержать номер основного документа, удостоверяющего личность субъекта ПДн или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта ПДн или его законного представителя.

В целях регистрации запросов субъектов ПДн и ответов на такие запросы в Учреждение осуществляется ведение журнала регистрации запросов субъектов ПДн.

Работник Учреждения по организационным вопросам и делопроизводству осуществляет прием и регистрацию запросов субъектов ПДн, а также рассмотрение, подготовку, регистрацию и направление ответов на такие запросы.

При получении запроса (обращения) физического лица, сотрудник Учреждения, ответственный за прием и регистрацию входящей корреспонденции в Учреждении, непосредственно в день получения устанавливает:

Содержит ли запрос фамилию, имя, отчество (последнее при его наличии) гражданина или его законного представителя, номер основного документа, удостоверяющего личность гражданина или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе;

Содержит ли почтовый адрес, по которому должны быть направлены ответ;

Имеется ли собственноручная подпись, а если запрос направлен в

Действия сотрудников Учреждения при получении запроса уполномоченного органа по защите прав субъектов персональных данных

Прием и регистрация запросов уполномоченного органа по защите прав субъектов ПДн осуществляется в порядке, установленном для приема и регистрации входящей корреспонденции.

При получении запроса уполномоченного органа по защите прав субъектов ПДн сотрудники Учреждения, ответственные за прием и регистрацию входящей корреспонденции, в тот же день осуществляют регистрацию такого запроса и передают его сотрудникам, указанным в п. 2.3

Учреждение, в лице сотрудников, указанных в п. 2.3. настоящего Регламента, сообщает в уполномоченный орган по защите прав субъектов ПДн по его запросу информацию, необходимую для осуществления деятельности указанного органа, а также направляет истребуемые им документы в течение семи рабочих дней с даты получения такого запроса.

В случае выявления уполномоченным органом по защите прав субъектов ПДн фактов недостоверности ПДн или неправомерных действий с ними, уточнение, блокирование или уничтожение таких ПДн осуществляется в порядке и сроки, предусмотренные п. 5 настоящего Регламента для соответствующих действий (операций) в отношении ПДн.

Действия сотрудников Учреждения при получении требования субъекта ПДн об уточнении своих ПДн, их блокировании или уничтожении; в случае выявления при обращении или по запросу субъекта ПДн фактов недостоверности ПДн или неправомерных действий с ними; в случае отзыва субъектом ПДн согласия на их обработку

При получении требований субъектов ПДн об уточнении своих ПДн, их блокировании, уничтожении прием и регистрация таких требований осуществляется в порядке, предусмотренном п. 2 настоящего Регламента.

Требования субъектов ПДн в тот же день передаются сотрудникам Учреждения, указанным в п. 2.3.

Полномочные сотрудники Учреждения вносят в ПДн субъекта необходимые изменения, уничтожают или блокируют соответствующие ПДн при предоставлении субъектом ПДн сведений, подтверждающих, что ПДн, которые относятся к соответствующему субъекту и обработку которых осуществляет Учреждение, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

О внесенных изменениях и предпринятых мерах Учреждение обязано уведомить субъекта ПДн и третьих лиц, которым ПДн этого субъекта были переданы.

В случае если факт недостоверности ПДн или неправомерных действий с ними будет выявлен при обращении или по запросу субъекта ПДн

Приложение № 1
к Регламенту порядка
действий сотрудников
БУ "КЦСОН Омского
района"
от 09.01.2023 № 5/1-н

Форма 1 "Запрос субъекта ПДн"

Руководителю БУ "КЦСОН Омского района"

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:

Какова цель обработки моих персональных данных в бюджетном учреждении Омской области "Комплексный центр социального обслуживания населения Омского района" (далее – Учреждение).

Каковы способы обработки моих персональных данных, применяемые в Учреждении, как оператором персональных данных;

Какие лица имеют доступ к моим персональным данным и каким лицам может быть предоставлен такой доступ;

Каков перечень обрабатываемых в Учреждении принадлежащих мне персональных данных и каков источник их получения;

Каковы сроки обработки моих персональных данных и каковы сроки их хранения;

Какие юридические последствия для меня, как для субъекта персональных данных, может повлечь за собой обработка моих персональных данных.

Ф.И.О.

(Подпись)

(Дата)

Приложение № 2
к Регламенту порядка
действий сотрудников
БУ "КЦСОН Омского
района"
от 09.01.2023 № 5/1-н

Форма 2 "Ответ на запрос субъекта ПДн"

Исх N	От
-------	----

Фамилия Имя Отчество
Адрес

Уважаемый _____!

Руководствуясь положениями ст. № 14, 20 Федерального закона РФ "О персональных данных" от 27.07.2006 г. № 152-ФЗ сообщаем Вам, что бюджетное учреждение Омской области "Комплексный центр социального обслуживания населения Омского района" (далее – Учреждение) обрабатывает Ваши персональные данные.

Цель обработки Ваших персональных –

(указать цель, заранее определенную до начала обработки)

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

Лица, имеющие доступ к Вашим персональным данным:

Должность 1;

Должность 2;

Должность 3.

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.

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

Срок обработки Ваших персональных данных – (указать срок)

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

Инструкция
осуществления внутреннего контроля соответствия обработки персональных
данных требованиям к защите персональных данных в бюджетном
учреждении Омской области "Комплексный центр социального
обслуживания населения Омского района" (далее – Учреждение)

Общие положения

Настоящая Инструкция осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Учреждении разработана с учетом Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных" и принятыми в соответствии с ним внутренними нормативными правовыми актами.

Настоящая Инструкция определяет порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

Тематика внутреннего контроля:

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 со 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.

Соблюдение правил хранения и работы с бумажными носителями персональных данных.

Порядок проведения внутренних проверок:

В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям Учреждение организует проведение периодических проверок условий обработки персональных данных.

Проверки осуществляются комиссией по внутреннему контролю,

ИНСТРУКЦИЯ
по работе с ресурсами сети Интернет в
бюджетном учреждении Омской области "Комплексный центр социального
обслуживания населения Омского района"

1. Общие положения

1. Настоящая инструкция по работе с ресурсами сети Интернет в бюджетном учреждении Омской области "Комплексный центр социального обслуживания населения Омского района" (далее – Инструкция) предназначена для организации работы в сети Интернет работников бюджетного учреждения Омской области "Комплексный центр социального обслуживания населения Омского района" (далее – пользователи сети Интернет) и определяет порядок подключения персональных компьютеров к сети Интернет.

2. Подключение к сети Интернет пользователей сети Интернет осуществляется администратором баз данных обеспечивающей службы (далее – администратор безопасности) на основании служебной записки от руководителя структурного с указанием фамилии, имени, отчества и должности сотрудников подразделения.

3. Доступ пользователей сети Интернет к сети Интернет предоставляется администратором безопасности по присвоенным им идентификаторам (имя учетной записи пользователя) и паролям.

4. Администратор безопасности, используя функциональные возможности прокси-сервера, ограничивает доступ к ресурсам сети Интернет, содержание которых не имеет отношения к исполнению служебных обязанностей, а также к ресурсам, содержащим информацию, оскорбляющую честь и достоинство других лиц, материалам, способствующим разжиганию межнациональной розни, подстрекающим к насилию, призывающим к совершению противоправных действий и т.п.

5. Вся информация о ресурсах, посещаемых пользователем сети Интернет, должна автоматически протоколироваться посредством программного обеспечения прокси-сервера.

2. Запреты и ограничения при работе с ресурсами сети Интернет

6. При работе с ресурсами сети Интернет пользователям сети Интернет запрещается:

- 1) посещение и использование в личных целях сайтов с объявлениями, форумами и конференциями, а также не корпоративной электронной почты;
- 2) публикация в сети Интернет своего служебного адреса электронной почты;
- 3) единовременное скачивание информации в объеме, превышающем

компьютеров пользователя сети Интернет обязаны поставить в известность администратора безопасности.

Перечень

должностей работников, допущенных к работе с персональными данными, в бюджетном учреждении Омской области "Комплексный центр социального обслуживания населения Омского района" (далее – Учреждение).

Для обеспечения безопасности персональных данных при их обработке, хранении и передаче утверждаю следующий перечень должностей, допущенных к работе с персональными данными:

1. Руководитель Учреждения
2. Заместители руководителя
3. Заведующие структурных подразделений
4. Главный бухгалтер
5. Бухгалтер
6. Администратор баз данных
7. Социальный работник
8. Специалист по реабилитационной работе
9. Специалист по социальной работе
10. Массажист
11. Парикмахер
12. Аналитик
13. Заведующий хозяйством
14. Экономист
15. Психолог
16. Специалист по управлению персоналом
17. Делопроизводитель
18. Юрисконсульт

Перечень

обрабатываемых персональных данных в бюджетном учреждении Омской области "Комплексный центр социального обслуживания населения Омского района" (далее – Учреждение).

1. Персональные данные работников

- ФИО;
- дата рождения;
- паспортные данные;
- адрес места жительства;
- сведения о заработной плате;
- сведения о семейном положении;
- место работы;
- сведения о стаже работы;
- сведения о здоровье;
- ИНН;
- СНИЛС

2. Персональные данные лиц, получающих услуги в Учреждении

- ФИО;
- дата рождения;
- паспортные данные;
- адрес места жительства;
- сведения о заработной плате;
- сведения о семейном положении;
- место работы;
- сведения о стаже работы;
- сведения о здоровье;
- ИНН;
- СНИЛС;
- информация об образовании;
- награды;
- социальные льготы;
- документы, подтверждающие льгот;
- Документы, подтверждающие инвалидность.

ИНСТРУКЦИЯ

по применению программных средств обработки информации в бюджетном учреждении Омской области "Комплексный центр социального обслуживания населения Омского района" (далее - Учреждение)

1. Общие положения

1 Настоящая инструкция по применению программных средств обработки информации (далее – Инструкция) определяет порядок работы с программным обеспечением в Учреждении.

2 Персональные компьютеры, программное обеспечение, коммуникационное оборудование локальной вычислительной сети предоставляются работникам Учреждения для осуществления ими своих служебных обязанностей.

3 Пользователь автоматизированного рабочего места – работник Учреждения, за которым закреплена ответственность за предоставленное ему автоматизированное рабочее место (далее – АРМ).

4 Администратор баз данных ответственный за правильность работы программного обеспечения и его функционирования в части исполнения его должностных обязанностей.

5 Системный администратор–отвечающий за обслуживание персональных компьютеров и коммуникационного оборудования локальной вычислительной сети.

6 Целью настоящей Инструкции является регулирование работы администратора, системного администратора и пользователей АРМ, поддержания необходимого уровня защиты информации, ее сохранности, повышение эффективности работы и уменьшение риска умышленного или неумышленного воздействия на информационную систему.

7 Работа пользователя АРМ разрешена только на закрепленном за ними персональном компьютере и только с разрешенным программным обеспечением, устанавливаемым администратором в Учреждении.

8 Администратором для каждого рабочего места составляется перечень разрешенного программного обеспечения, устанавливаемого на рабочие места в Учреждении.

2. Обязанности пользователя АРМ

Пользователь АРМ обязан:

1) обеспечивать беспрепятственный доступ администратора и системного администратора к своему АРМ;

Перечень

разрешенного программного обеспечения, устанавливаемого на рабочие места в бюджетном учреждении Омской области "Комплексный центр социального обслуживания населения Омского района" (далее – Учреждение).

- Microsoft Windows
- Microsoft Office
- Продукты 1С
- СБИС ++
- Браузеры Firefox, Chrome, Yandex
- Архиватор 7zip
- Adobe Reader
- ДубльГИС
- Правовая система Гарант
- Kaspersky Endpoint Security Russian Edition
- КриптоПро CSP v 4.0
- VipNet CSP