Приложение №1
к приказу руководителя
управления социальной защиты
населения администрации
Свердловского района в городе
Красноярске
от 30.11.2010 № 187-ОД

ПОЛОЖЕНИЕ
по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах управления социальной защиты населения администрации Свердловского района в городе Красноярске

I. Общие положения

Положение по организации и техническому обеспечению безопасности персональных данных при их обработке в информационных системах управления социальной защиты населения администрации Свердловского района в городе Красноярске (далее Положение) разработано в соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 17.11.2007
№ 781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», Приказом Федеральной службы по техническому и экспортному контролю России от 05.02.2010 № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных», правовыми актами администраций города Красноярска, Положением об управлении социальной защиты населения администрации Свердловского района в городе Красноярске.

Положение определяет порядок обработки организации мероприятий, направленных на обеспечение безопасности персональных данных при их обработке в информационных системах и защиты персональных данных от несанкционированного, в том числе случайного неправомерного доступа к персональным данным, результатом которого может стать уничтожение, изменение, копирование, распространение персональных данных, а так же иных несанкционированных действий.

Термины и сокращения, используемые в Положении.

Автоматизированное рабочее место (АРМ) – комплекс технических и программных средств, предназначенных для решения определённого круга задач.

Безопасность персональных данных – состояние защищенности персональных данных, при котором обеспечиваются их конфиденциальность, доступность и целостность при их обработке в информационных системах персональных данных.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа или воздействия на информационные ресурсы, заведомо приводящая к уничтожению, блокированию, модификации, копированию информации либо к нарушению работы автоматизированной системы.

Защита персональных данных – осуществление комплекса мероприятий по предотвращению несанкционированного распространения (утечки, хищения, копирования), утраты, уничтожения, искажения, подделки, блокирования информации.

Информационная система персональных данных (ИСПДн) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационный ресурс – сведения (сообщения, данные), входящие в состав отдельных документов, массивов документов, баз данных, представленные в электронно-цифровой форме.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

Контролируемая зона – это пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств.

Несанкционированный доступ – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Оператор – Управление социальной защиты населения администрации Свердловского района в городе Красноярске, организующее и осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

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

Персональные данные (ПДн) – 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.

Пользователь информационной системы персональных данных (Пользователь ИСПДн) – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Средства вычислительной техники (СВТ) – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Управление – Управление социальной защиты населения администрации Свердловского района в городе Красноярске.

II. Порядок обработки персональных данных

2.1. Обработка персональных данных осуществляется после получения согласия субъекта персональных данных, за исключением случаев, предусмотренных частью 2 статьи 6 Федерального закона «О персональных данных».

2.2. Обработка персональных данных осуществляется только в пределах контролируемой зоны.

2.3. Электронные носители информации, содержащие персональные данные, регистрируются в журнале учета электронных носителей персональных данных.

2.4. В Управлении приказом руководителя Управления назначаются сотрудники, ответственные за защиту персональных данных, администратор информационной безопасности и утверждается перечень лиц, допущенных к обработке персональных данных, с указанием полномочий доступа к ресурсам управления.

2.5. Сотрудники Управления перед допуском к обработке персональных данных в обязательном порядке подписывают Обязательство о неразглашение информации, содержащей персональные данные.

2.6. Обработка персональных данных в ИСПДн осуществляется специалистами Управления в соответствии с инструкциями по работе в ИСПДн.

2.7. Ответственный за защиту персональных данных в соответствии с утверждаемым ежегодно планом внутренних проверок режима защиты персональных данных проводит мероприятия по проверкам соблюдения режима защиты персональных данных, результат проверки фиксируется в журнале внутренних проверок.

2.8. Предоставление доступа к ПДн сотрудникам МУ «Комплексный Центр социального обслуживания населения» Свердловского района г. Красноярска (Центр) осуществляется на основании соглашения о взаимодейст-

вии. Обязанность обеспечения конфиденциальности и безопасности персональных данных при их обработке возлагается на специалистов Центра.

2.9. Сотрудники Управления, допущенные к обработке персональных данных, в обязательном порядке под роспись знакомятся с Положением.

III. Объекты защиты ИСПДн

3.1. Объектами защиты являются – информация, обрабатываемая в ИСПДн, и технические средства ее обработки и защиты, безопасность которых должна обеспечиваться системой защиты персональных данных в ИСПДн Управления. Объекты защиты каждой ИСПДн включают:

- персональные данные субъектов ПДн;
- технологическая информация;
- программно-технические средства обработки;
- средства защиты ПДн;
- каналы информационного обмена и телекоммуникации;
- объекты и помещения, в которых размещены компоненты ИСПДн.

3.2. Персональные данные субъектов ПДн

3.2.1. ИСПДн «Адресная социальная помощь».

Перечень персональных данных субъектов ПДн:

- фамилия, имя, отчество;
- дата рождения;
- место рождения;
- гражданство;
- контактный телефон;
- адрес регистрации места жительства и фактического проживания;
- паспортные данные;
- идентификационный номер плательщика;
- страховое свидетельство обязательного пенсионного страхования;
- полис обязательного медицинского страхования;
- свидетельство о рождении;
- справка об инвалидности;
- доходы;
- информация о видах деятельности (вид и срок деятельности);
- семейное положение и состав семьи (муж/жена, дети);
- сведения об образовании;
- данные об удостоверениях, наградах, медалях, поощрениях, почетных званиях;
- сведения об опекунах;
- дата и место участия в боевых действиях;
- данные о банковских лицевых счетах;
- данные о жилье (характеристики жилья, квартплата);

– номер финансово-лицевого счета

3.2.2. ИСПДн «1С: Зарплата и Кадры».

Перечень персональных данных субъектов ПДн:

– фамилия, имя, отчество;
– дата рождения;
– место рождения;
– гражданство;
– адрес регистрации места жительства или временного проживания;
– паспортные данные;
– идентификационный номер плательщика;
– страховое свидетельство обязательного пенсионного страхования;
– стаж;
– оклад;
– зарплатный счет.

3.3. Технологическая информация, подлежащая защите, включает:

– управляющую информацию (конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.);

– технологическую информацию средств доступа к системам управления (аутентификационная информация, ключи и атрибуты доступа и др.);

– информацию на съемных носителях информации (бумажные, магнитные, оптические и пр.), содержащие защищаемую технологическую информацию системы управления ресурсами или средств доступа к этим системам управления;

– информацию о средствах защиты ПДн, их составе и структуре, принципах и технических решениях защиты;

– информационные ресурсы (базы данных, файлы и другие), содержащие информацию о информационно-телекоммуникационных системах, о служебном, телефонном, факсимильном, диспетчерском трафике, о событиях, произошедших с управляемыми объектами, о планах обеспечения бесперебойной работы и процедурах перехода к управлению в аварийных режимах;

– служебные данные (метаданные), появляющиеся при работе программного обеспечения, сообщения и протоколы межсетевого взаимодействия, в результате обработки информации.

3.4. Программно-технические средства включают в себя:

– общесистемное и специальное программное обеспечение (операционные системы, СУБД, клиент-серверные приложения и другие);

– резервные копии общесистемного программного обеспечения;

– инструментальные средства и утилиты систем управления ресурсами ИСПДн;

– аппаратные средства обработки ПДн (рабочие станции и сервера);

– сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.).

3.5. Средства защиты ПДн состоят из аппаратно-программных средств включают в себя:
- средства управления и разграничения доступа пользователей;
- средства обеспечения регистрации и учета действий с информацией;
- средства, обеспечивающие целостность данных;
- средства антивирусной защиты;
- средства межсетевого экранирования;
- средства анализа защищенности;
- средства обнаружения вторжений;
- средства криптографической защиты ПДн, при их передачи по каналам связи сетей общего и (или) международного обмена.

3.6. Каналы информационного обмена и телекоммуникации являются объектами защиты, если по ним передаются обрабатываемая и технологическая информация.

3.7. Объекты и помещения являются объектами защиты, если в них происходит обработка обрабатываемой и технологической информации, установлены технические средства обработки и защиты.

IV. Порядок реализации доступа к информационным ресурсам и информационным системам, содержащим информацию о персональных данных.

4.1. Разграничение прав пользователей, а так же их уровень прав доступа к обрабатываемым персональным данным, осуществляется исходя из характера и режима обработки персональных данных в ИСПДн. Руководители и специалисты управления должны иметь доступ только к той ИСПДн, которая необходима им для выполнения служебных обязанностей.

4.2. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику Управления, допущенному к работе с конкретным информационным ресурсом или ИСПДн Управления, должна быть сопоставлена учетная запись пользователя, под которым он будет регистрироваться и работать в системе. Использование несколькими сотрудниками одного и того же имени пользователя (“группового имени”) запрещено.

4.3. Процедура регистрации (создания учетной записи) пользователя для сотрудника Управления и предоставления ему (или изменения его) прав доступа к информационным ресурсам и ИСПДн инициируется заявкой начальника отдела согласно приложению 1 к Положению.

4.3.1. В заявке указывается:
- содержание запрашиваемых изменений (регистрация нового пользователя, удаление учетной записи пользователя, расширение или сужение

полномочий и прав доступа к ресурсам ИСПДн ранее зарегистрированного пользователя);

– должность (с полным наименованием отдела), фамилия, имя и отчество сотрудника;

– имя пользователя (учетной записи) данного сотрудника;

– полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользователем задач и полномочий в конкретных ИСПДн).

4.3.2. Заявку визирует руководитель Управления , утверждая тем самым производственную необходимость допуска (изменения прав доступа) данного сотрудника к необходимым для решения им указанных задач.

4.3.3. Затем начальник информационно-аналитического отдела рассматривает представленную заявку и подписывает задание администратору информационной безопасности, администратору ИСПДн на внесение необходимых изменений в списки пользователей.

4.3.4. На основании заявки администратор информационной безопасности сети в соответствии с формулярами указанных задач, и документацией на средства защиты сетевых операционных систем производит необходимые операции по созданию (удалению) учетной записи пользователя, присвоению ему начального значения пароля и заявленных прав доступа к сетевым ресурсам, включению его в соответствующие задачам группы пользователей и другие необходимые действия. Для всех пользователей должен быть установлен режим принудительного запроса смены пароля не реже одного раза в месяц.

4.3.5. Администратор ИСПДн производит необходимые операции по созданию (удалению) учетной записи пользователя в ИСПДн, присвоению ему начального значения пароля и заявленных прав в соответствии с заявкой. Для всех пользователей должен быть установлен режим принудительного запроса смены пароля не реже одного раза в месяц.

4.3.6. После внесения изменений в списки пользователей администратор информационной безопасности должен обеспечить соответствующие категориям защиты указанных рабочих станций настройки средств защиты. По окончании внесения изменений в списки пользователей в заявке делается отметка о выполнении задания за подписями исполнителей – администратора информационной безопасности и администратора ИСПДн.

4.3.7. Сотруднику, зарегистрированному в качестве нового пользователя системы, под роспись сообщается имя пользователя и пароль, который он обязан сменить при первом же входе в систему (при первом подключении к ИСПДн).

4.3.8. Исполненная заявка хранится у начальника информационно-аналитического отдела.

V. Порядок резервирования и восстановления работоспособности средств вычислительной техники и средств защиты информации, баз данных ИСПДн.

5.1. Порядок резервирования и восстановления работоспособности СВТ и средств защиты информации (далее – Порядок) определяет действия, связанные с функционированием ИСПДн Управления, меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

5.2. Действие настоящего Порядка распространяется на всех пользователей, имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций.

5.3. Ответственным сотрудником за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, назначается администратор безопасности Управления.

5.4. Ответственным за контроль обеспечения мероприятий по предотвращению инцидентов безопасности, приводящих к потере защищаемой информации, назначается ответственный за обеспечение защиты персональных данных.

5.5. Под Инцидентом понимается происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а так же потерей защищаемой информации.

5.6. В сроки, не превышающие одного рабочего дня, ответственный за реагирование сотрудник Управления, предпринимают меры по восстановлению работоспособности. Предпринимаемые меры согласуются с вышестоящим руководством.

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

5.8. Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИСПДн в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

5.9. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания.

5.10. Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии RAID (резервированный массив независимых жестких дисков).

5.11. Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердый носитель (жесткий диск, и т.п.).
5.12. Процедуры резервного копирования должны производиться в соответствии с режимом резервного копирования.
5.13. Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования; процедура резервного копирования должна быть зафиксирована в журнале электронных носителей персональных данных.
5.14. Носители должны храниться в несгораемом шкафу или помещении, оборудованном системой пожаротушения.

VI. Порядок доступа в серверное помещение

6.1. Доступ в помещение серверной комнаты Управления, расположенной по адресу улице 60 лет Октября, 46, кабинет 224, имеют начальник информационно-аналитического отдела, ответственный за обеспечение защиты персональных данных, администратор информационной безопасности.
6.2. Присутствие иных лиц в помещениях с оборудованием информационно-коммуникационных систем допускается только в сопровождении лиц, имеющих право доступа в данное помещение.

VII. Ответственность

Сотрудники Управления, допущенные к персональным данным, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

Руководитель управления
социальной защиты населения
администрации Свердловского района
в городе Красноярске А.Ю. Семенкевич