ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
«УПРАВЛЕНИЕ СОЦИАЛЬНОЙ ЗАЩИТЫ И СОЦИАЛЬНОГО ОБСЛУЖИВАНИЯ НАСЕЛЕНИЯ ПО ГОРОДУ УСОЛЬЕ-СИБИРСКОЕ И УСОЛЬСКОМУ РАЙОНУ»

ПРИКАЗ

Об утверждении правовых актов, регулирующих отношения, связанные с обработкой и защитой персональных данных

«24» октября 2024 года № 164

В соответствии с Федеральным законом от 27июля 2006 года № 152-ФЗ «О персональных данных» (далее — Федеральный закон «О персональных данных»), постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» , руководствуясь Уставом ОГБУ «Управление социальной защиты и социального обслуживания населения по городу Усолье-Сибирское и Усольскому району»,

Приказываю:

1. Утвердить в ОГБУ «Управление социальной защиты и социального обслуживания населения по городу Усолье-Сибирское и Усольскому району»:
1. Инструкцию по организации парольной защиты в локальных вычислительных сетях (Приложение 1);
2. Инструкцию пользователя по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций (Приложение 2);
3. Инструкцию пользователя информационных систем персональных данных (Приложение 3);
4. Регламент использования ресурсов глобальной сети Интернет (Приложение 4);
5. Положение о порядке учета, хранения и обращения со съемными носителями персональных данных (Приложение 5).
6. Контроль за исполнением настоящего распоряжения оставляю за собой.

Директор Воронина Е.В.

Исп. Шевнина Л.Ф.

Приложение 1
к приказу от «24» октября 2024г.
№ 164

Инструкция
по организации парольной защиты в локальных вычислительных сетях ОГБУ «Управление социальной защиты и социального обслуживания населения по городу Усолье-Сибирское и Усольскому району»

Общие положения

1.1. Инструкция по организации парольной защиты (далее -Инструкция) регламентирует установку, смену и прекращение действия паролей, блокировку учетных записей пользователей в локальной вычислительной сети (далее - ЛВС) ОГБУ «Управление социальной защиты и социального обслуживания населения по городу Усолье-Сибирское и Усольскому району» (далее —Учреждение).

1.2. Пароль пользователя ЛВС - это комбинация символов (буквы, цифры, специальные символы), известная только пользователю ЛВС, предназначенная для аутентификации пользователя в операционной системе автоматизированного рабочего места и в ЛВС.

1.3. Должностные лица, оформляемые на работу, должны быть ознакомлены отделом кадрово-правовой с настоящей инструкцией под подпись в журнале ознакомления.

1.4. Журналы ознакомления с настоящей инструкцией хранятся в отделе кадрово-правовой работы.

2. Требования к паролям, используемым в ЛВС

2.1. Пользователям ЛВС запрещается использовать пароли, имеющие в своем составе:

- имя, отчество или фамилию пользователя или близких родственников;
- идентификатор входа (имя пользователя в операционной системе);
- какую-либо информацию о пользователе (номера телефонов, номера в личных документах, номер или марка автомобиля, почтовый адрес и т.д.);
- повторяющиеся наборы цифр, букв, символов.

2.2. Пользователи ЛВС обязаны при формировании паролей включать в их состав:

- строчные и прописные буквы;
- цифры;
- специальные символы.

2.3. Пароль должен содержать не менее 8 символов.

2.4. Новый пароль пользователя ЛВС должен отличаться от четырех предыдущих паролей.

3. Порядок смены личных паролей, используемых в ЛВС

3.1. Первоначальную установку временного пароля производит администратор ЛВС, пользователь производит смену пароля при первом входе в операционную систему.

3.2. Пользователь обязан не реже одного раза в квартал самостоятельно осуществлять смену пароля.

3.3. При формировании пароля пользователь обязан руководствоваться разделом 2 настоящей Инструкции.

3.4. В случае компрометации пароля (либо подозрения на компрометацию) необходимо немедленно сообщить об этом в отдел автоматизированных систем. управления базами данных и изменить пароль.

3.5. В случае прекращения полномочий пользователя ЛВС (увольнение, перевод на другую должность и т. п.) в течение одного рабочего дня руководитель соответствующего структурного подразделения информирует начальника ОЗИ для организации блокирования учетной записи пользователя.

4. Обязанности пользователя КИВС и ЛВС

4.1. Пользователь ЛВС обязан:

сохранять свой пароль в тайне;

своевременно производить смену пароля;

информировать администратора КИВС и ЛВС обо всех случаях компрометации пароля;

информировать администратора КИВС и ЛВС обо всех случаях нарушения Инструкции.

4.2. Пользователю КИВС и ЛВС запрещается:

передавать свой пароль другим лицам;

записывать свой пароль на бумажных или электронных носителях;

пересылать свой пароль в электронных и иных открытых сообщениях.

5. Ответственность пользователя ЛВС

Нарушение требований Инструкции является дисциплинарным проступком.

За нарушение требований Инструкции, пользователь ЛВС может быть привлечен к дисциплинарной ответственности.

В случаях, предусмотренных законодательством Российской Федерации, за нарушение требований Инструкции пользователь ЛВС может быть привлечен к административной или уголовной ответственности.

Контроль за соблюдением пользователями ЛВС Инструкции по организации парольной защиты в ЛВС

Контроль за соблюдением требований Инструкции к паролям осуществляет администратор безопасности ЛВС путем установления групповых политик в ЛВС, а также в ходе проверки выполнения Инструкции пользователями ЛВС.

Контроль за соблюдением пользователями ЛВС иных требований Инструкции осуществляется их непосредственными руководителями в пределах их компетенции.

Директор Воронина Е.В.

Исп. Шевнина Л.Ф.

Приложение 2
к приказу от «24» октября 2024г.

Инструкция
пользователя по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций

1. Основные термины, сокращения и определения

Администратор ИСПДн - технический специалист, из числа сотрудников ОГБУ «Управление социальной защиты и социального обслуживания населения по городу Усолье-Сибирское и Усольскому району», обеспечивает ввод в эксплуатацию, поддержку и последующий вывод из эксплуатации программного обеспечения и оборудования вычислительной техники.

Администратор безопасности ИСПДн - технический специалист, из числа сотрудников ОГБУ «Управление социальной защиты и социального обслуживания населения по городу Усолье-Сибирское и Усольскому району» обеспечивают правильность использования и нормальное функционирование установленных систем защиты информации.

Оператор ИСПДн - юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки 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.

Носитель информации — любой материальный объект, используемый для хранения и передачи электронной информации.

RU — персональный компьютер.

ПО — программное обеспечение вычислительной техники.

Пользователь — работник министерства, использующий мобильные устройства и носители информации для выполнения своих служебных обязанностей.

2. Назначение и область действия

Настоящая Инструкция определяет возможные аварийные ситуации, связанные с функционированием ИСПДн в ОГБУ «Управление социальной защиты и социального обслуживания населения по городу Усолье-Сибирское и Усольскому району» (далее — учреждение), меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн после аварийных ситуаций.

Целью настоящего документа является превентивная защита элементов ИСПДн от прерывания в случае реализации рассматриваемых угроз.

Задачей данной Инструкции является:

- определение мер защиты от прерывания;
- определение действий восстановления в случае прерывания.

Действие настоящей Инструкции распространяется на всех пользователей министерства, имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

Пересмотр настоящего документа осуществляется по мере необходимости, но не реже раза в два года.

3. Порядок реагирования на аварийную ситуацию

3.1 Действия при возникновении аварийной ситуации

В настоящем документе под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн. Аварийная ситуация становится возможной в результате реализации одной из угроз, *приведенных в Приложении 1.*

Все действия в процессе реагирования на аварийные ситуации должны документироваться ответственным за реагирование сотрудником в «Журнале по учету мероприятий по контролю».

В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники учреждения (отдел автоматизированных систем, управления базами данных) предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

3.2. Уровни реагирования на инцидент

При реагировании на инцидент, важно, чтобы пользователь правильно классифицировал критичность инцидента. Критичность оценивается на основе следующей классификации:

Уровень 1 Незначительный инцидент. Незначительный инцидент определяется как локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов ИСПДн и средств защиты. Эти инциденты решаются ответственными за реагирование сотрудниками.

Уровень 2 Авария. Любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИСПДн и средств защиты. Эти инциденты выходят за рамки управления ответственными за реагирование сотрудниками.

К авариям относятся следующие инциденты:

- Отказ элементов ИСПДн и средств защиты из-за:

- повреждения водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения), а также подтопления в период паводка или проливных дождей;

- сбоя системы кондиционирования.

- Отсутствие Администратора ИСПДн и Администратора безопасности более чем на сутки из-за:

- химического выброса в атмосферу; сбоев общественного транспорта;

- эпидемии;

- массового отравления персонала;

- сильного снегопада;

- урагана (смерча - торнадо);

- сильных морозов.

Уровень 3 — Катастрофа. Любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИСПДн и средств защиты, а также к угрозе жизни пользователей ИСПДн, классифицируется как катастрофа. Обычно к катастрофам относят обстоятельства непреодолимой силы (пожар, взрыв), которые могут привести к неработоспособности ИСПДн и средств защиты на сутки и более.

К катастрофам относятся следующие инциденты:

- пожар в здании;

- взрыв;

- просадка грунта с частичным обрушением здания;

- массовые беспорядки в непосредственной близости от Объекта.

4. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийные ситуаций

4.1. Технические меры

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

системы жизнеобеспечения:
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.

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

Порядок предотвращения потерь информации и организации системы жизнеобеспечения ИСПДн описан в Положении о порядке учета, хранения и обращения со съемными носителями персональных данных.

4.2.Организационные меры

Ответственные за реагирование сотрудники ознакомляют всех сотрудников Учреждения, находящихся в их зоне ответственности, с данной инструкцией в срок, не превышающий 3-х рабочих дней с момента выхода нового сотрудника на работу.

По окончанию ознакомления сотрудник расписывается в журнале, предоставляемом Ответственным за реагирование сотрудником. Подпись сотрудника должна соответствовать его подписи в документе, удостоверяющем его личность.

Должно быть проведено обучение должностных лиц Учреждения, имеющих доступ к ресурсам ИСПДн, порядку действий при возникновении аварийных ситуаций. Должностные лица должны получить базовые знания в следующих областях:

оказание первой медицинской помощи; пожаротушение;
эвакуация людей;
защита материальных и информационных ресурсов;
методы оперативной связи со службами спасения и лицами, ответственными за реагирование сотрудниками на аварийную ситуацию;

- выключение оборудования, электричества, водоснабжения, газоснабжения.

Администраторы ИСПДн и Администраторы безопасности должны быть дополнительно обучены методам частичного и полного восстановления работоспособности элементов ИСПДн.

Навыки и знания должностных лиц по реагированию на аварийные ситуации должны регулярно проверяться. При необходимости должно проводиться дополнительное обучение должностных лиц порядку действий при возникновении аварийной ситуации.

5. **Источники угроз**

Таблица 1

Технологические угрозы	
1	Пожар в здании
2	Повреждение водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения)
3	Взрыв (бытовой газ, теракт, взрывчатые вещества или приборы, работающие под давлением)
4	Химический выброс в атмосферу
Внешние угрозы	
5	Массовые беспорядки
6	Сбои общественного транспорта
7	Эпидемия
8	Массовое отравление персонала
Стихийные бедствия	
9	Удар молнии
10	Сильный снегопад
11	Сильные морозы
12	Просадка грунта (подмыв грунтовых вод, подземные работы) с частичным обрушением здания
13	Затопление водой в период паводка
14	Наводнение, вызванное проливным дождем
15	Ураган, торнадо
16	Подтопление здания (воздействие подпочвенных вод, вызванное внезапным и непредвиденным повышением уровня грунтовых вод)
Телекоммуникационные и ИТ угрозы	
17	Сбой системы кондиционирования
18	Сбой ИТ — систем
Угроза, связанная с человеческим фактором	
19	Ошибка персонала, имеющего доступ к серверной
20	Нарушение конфиденциальности, целостности и доступности конфиденциальной информации
Угрозы, связанные с внешними поставщиками	
21	Отключение электроэнергии
22	Сбой в работе интернет-провайдера
23	Физически разрыв внешних каналов связи

Директор Воронина Е.В.

Исп. Шевнина Л.Ф.

Приложение 3
к приказу от «24» октября 2024г.

Инструкция
пользователя информационных систем персональных данных

1. Общие положения

Пользователь ИСПДн (далее Пользователь) осуществляет обработку персональных данных в информационной системе персональных данных.

Пользователем является сотрудник министерства социального развития, опеки и попечительства Иркутской области (далее - министерство), участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации 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, локальными актами министерства, руководящими и нормативными документами в сфере защиты конфиденциальной информации и персональных данных, в частности.

Методическое руководство работой пользователя осуществляется ответственным за обеспечение защиты персональных данных.

2. Обязанности пользователя

Пользователь обязан:

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.

Выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него в соответствии с правилами разграничения доступа.

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

Соблюдать требования парольной политики.

Соблюдать правила при работе в сетях общего доступа и (или) международного обмена — Интернет и других.

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

Обо всех выявленных нарушениях, связанных с информационной безопасностью министерства, а также для получений консультаций по вопросам информационной безопасности, необходимо обратиться в ответственному администратору безопасности.

Для получения консультаций по вопросам работы и настройке элементов ИСПДн необходимо обращаться к Администратору ИСПДн по внутреннему телефону **237, 6-62-54.**

Пользователям запрещается:

Разглашать защищаемую информацию третьим лицам.

Копировать защищаемую информацию на внешние носители без разрешения своего руководителя.

Самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.

Несанкционированно открывать общий доступ к папкам на своей рабочей станции.

Запрещено подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства.

Отключать (блокировать) средства защиты информации.

Обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн.

Сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн.

Привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты персональных данных.

При отсутствии визуального контроля за рабочей станцией: доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш Ctrl+A1t+Delete раздел Блокировка (Заблокировать).

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

Не разглашать информацию, к которой они допущены, в том числе сведения о крипто средствах, ключевых документах к ним и других мерах защиты;

Соблюдать требования к обеспечению безопасности персональных данных, требования к обеспечению безопасности криптосредств и ключевых документов к ним;

Сообщать о ставших им известными попытках посторонних лиц получить сведения об используемых криптосредствах или ключевых документах к ним;

Немедленно уведомлять оператора о фактах утраты или недостачи криптосредств, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых персональных данных.

Сдать криптосредства, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с порядком, установленным настоящими Требованиями, при увольнении или отстранении от исполнения обязанностей, связанных с использованием криптосредств;

Не разглашать информацию о ключевых документах;

Не допускать снятие копий с ключевых документов;

Не допускать вывод ключевых документов на дисплей (монитор) ПЭВМ или принтер;

Не допускать записи на ключевой носитель посторонней информации;

Не допускать установки ключевых документов в другие ПЭВМ.

Директор Воронина Е.В.

Исп. Шевнина Л.Ф.

Приложение 4
к приказу от «24» октября 2024г.

Регламент
использования ресурсов глобальной сети Интернет

1. Общие положения

Настоящий Регламент разработан для повышения эффективности работы сотрудников ОГБУ «Управление социальной защиты и социального обслуживания населения по городу Усолье-Сибирское и Усольскому району» (далее учреждение), использующих электронные информационные ресурсы глобальной сети Интернет, и повышения уровня информационной безопасности локальной информационно-вычислительной сети.

В учреждении устанавливается контроль, и специфицируются виды информации, к которой разрешается доступ сотрудников. В случае нарушения сотрудником учреждения данного Регламента он отстраняется от использования ресурсов сети Интернет.

2. Назначение доступа к ресурсам сети Интернет

Доступ к ресурсам сети Интернет предоставляется сотрудникам для выполнения ими прямых должностных обязанностей. Глобальная сеть Интернет используется для:

- доступа к гипертекстовым страницам (WWW);
- доступа к файловым ресурсам Интернета (FTP);
- доступа к специализированным (правовым и др.) базам данных;
- ответов на официальные запросы граждан;
- обмена электронной почтой с официальными лицами других правительственных структур по не конфиденциальным вопросам производственного характера;
- повышения квалификации работников, необходимой для выполнения работником своих должностных обязанностей;
- поиска и сбора информации по управленческим, производственным, финансовым, юридическим вопросам, если эти вопросы напрямую связаны с выполнением работником его должностных обязанностей, и др.

3. Доступ к Интернет-ресурсам

ОГБУ «Управление социальной защиты и социального обслуживания населения по городу Усолье-Сибирское и Усольскому району» обеспечивает доступ пользователей локальной сети, к ресурсам Интернет по специальным каналам связи в соответствии с установленными правилами и настоящим Регламентом.

Открытие и контроль доступа регулируется управлением информационной безопасности и межведомственного взаимодействия ОГБУ «Управление социальной защиты и социального обслуживания населения по городу Усолье-Сибирское и Усольскому району». Самостоятельная организация дополнительных точек доступа в глобальную сеть Интернет (удаленный доступ, VPN и пр.) запрещена.

4. Регистрация пользователя

Каждому физически подключенному к сети компьютеру назначается ответственный за этот компьютер пользователь, информация о котором заносится в базу данных пользователей соответствующего домена локальной сети.

Регистрация выполняется специалистами отдела автоматизированных систем, управления базами данных. Пользователь обязан хранить свои идентификационные данные (пароли и т.п.) в тайне. Запрещена передача идентификационных данных третьим лицам. За все деструктивные действия, произведенные в сети, отвечает сотрудник пользователь учетной записи (идентификационных данных), использовавшейся при их проведении.

При подозрении на то, что идентификационные данные стали известны третьим лицам, пользователь должен немедленно обратиться в отдел автоматизированных систем, управления базами данных с целью их изменения.

5. Основные ограничения при работе в сети Интернет

При работе в сети Интернет запрещается:

- посещение пользователем ресурсов с непристойным содержанием (эротико-порнографические ресурсы, нацистские или националистические ресурсы, ресурсы, призывающие к насилию);
- посещение игровых, развлекательных и прочих сайтов, не имеющих отношения к деятельности учреждения и деятельности пользователя;
- использование электронной почты в личных целях в любое время;
- массовая рассылка не согласованных предварительно электронных писем.

Под массовой рассылкой подразумевается как рассылка множеству получателей, так и множественная рассылка одному получателю. Здесь и далее под электронными письмами понимаются сообщения электронной почты, ICQ и других подобных средств личного обмена информацией;

- несогласованная рассылка электронных писем рекламного, коммерческого или агитационного характера, а также писем, содержащих грубые и оскорбительные выражения и предложения;
- использование собственных или предоставленных информационных ресурсов (почтовых ящиков, адресов электронной почты, страниц WWW и т.д.) в качестве контактных для осуществления действий, не связанных с выполнением служебных обязанностей;
- не допускается осуществление попыток несанкционированного доступа к ресурсам Сети, проведение или участие в сетевых атаках и сетевом взломе, за исключением случаев, когда атака на сетевой ресурс проводится с явного разрешения владельца или администратора этого ресурса;
- действия, направленные на нарушение нормального функционирования элементов Сети (компьютеров, другого оборудования или программного обеспечения), не принадлежащих пользователю;
- передача компьютерам или оборудованию Сети информации, не имеющей отношения к выполнению служебных обязанностей, создающей паразитную нагрузку на рабочие станции локальной сети и (или) оборудование, а также промежуточные участки сети, в объемах, превышающих минимально необходимые для проверки связности сетей и доступности отдельных ее элементов.
- публикация корпоративного электронного адреса на досках объявлений, в конференциях и гостевых книгах;
- использование некорпоративных E-mail. В случае если пользователю в служебных целях необходимо завести почтовый ящик в домене, отличном от UDSZN@IRMAIL.RU необходимо письменное разрешение руководителя подразделения, согласованное с отделом автоматизированных систем, управления базами данных;
- передача кому бы то ни было учетных данных пользователя;
- применение имен и паролей учетных записей, используемых в локальной сети учреждения, на иных (сторонних) компьютерах;
- установка и использование сетевых и автономных компьютерных игровых приложений на рабочей станции;
- посещение ресурсов трансляции потокового видео и аудио (вебкамеры, трансляция ТВ - и музыкальных программ в Интернете), создающих большую загрузку сети и мешающих нормальной работе остальных пользователей;
- загрузка развлекательных материалов;
- передача конфиденциальной информации третьей стороне;
- подключение к электронной сети под чужим логином и паролем;
- нанесение вреда электронной системе учреждения;
- проведение незаконных операций в глобальной сети Интернет;

- создание личных веб-страниц и хостинг (размещение web- или ftpсервера) на рабочих станциях локальной вычислительной сети учреждения;

- любые попытки деструктивных действий по отношению к нормальной работе электронной системы учреждения и ресурсам сети Интернет (рассылка вирусов, ф-атаки и т.п.);

- нарушение закона об авторском праве: копирование и использование материалов и программ, защищенных законом об авторском праве;

- совершение иных действий, противоречащих действующему законодательству Российской Федерации.

6. Соблюдение правил, установленных владельцами ресурсов.

Владелец любого информационного или технического ресурса сети Интернет может установить для этого ресурса собственные правила его использования. Правила использования ресурсов либо ссылка на них публикуются владельцами или администраторами этих ресурсов в точке подключения к таким ресурсам и являются обязательными к исполнению всеми пользователями этих ресурсов. Пользователь обязан соблюдать правила использования ресурса либо немедленно отказаться от его использования.

7. Недопустимость фальсификации.

Значительная часть ресурсов Сети не требует идентификации пользователя и допускает анонимное использование. Однако в ряде случаев от пользователя требуется предоставить информацию, идентифицирующую его, и используемые им средства доступа к Сети. При этом пользователю запрещается:

- использование идентификационных данных (имен, адресов, телефонов и т.п.) третьих лиц, кроме случаев, когда эти лица уполномочили пользователя на такое использование. В то же время пользователь должен принять меры по предотвращению использования ресурсов Сети третьими лицами от его имени (обеспечить сохранность паролей и прочих кодов авторизованного доступа);

- фальсификация своего IP-адреса, а также адресов, используемых в других сетевых протоколах, при передаче данных в Сеть;

- использование несуществующих обратных адресов при отправке электронных писем.

Ответственность за все действия в Сети, произведенные под именем и с паролем пользователя им самим или другими физическими, или юридическими лицами и организациями, полностью лежит на самом пользователе. Учреждение не несет никакой юридической, материальной или иной ответственности за качество, содержание, законность и любое другое свойство полученной или переданной пользователем информации в нарушение действующего законодательства Российской Федерации.

Учреждение не несет никакой юридической, материальной и иной ответственности за использование пользователем платных услуг других организаций, предоставляющих услуги в Сети.

8. Контроль использования ресурсов сети Интернет

Руководство учреждения оставляет за собой право в целях обеспечения безопасности электронной системы производить выборочные и полные проверки всей электронной системы и отдельных файлов без предварительного уведомления работников.

Директор Воронина Е.В.

Исп. Шевнина Л.Ф.

Приложение 5
к приказу от «24» октября 2024г.

Положение
о порядке учета, хранения и обращения со съемными носителями персональных данных

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с Федеральным законом № 149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации», Федеральным законом № 152-ФЗ от 27.07.2006 г. «О персональных данных», ГОСТ Р ИСО/МЭК 17799-2005 «Практические правила управления информационной безопасностью» и другими нормативными правовыми актами, и устанавливает порядок использования носителей информации, предоставляемых ОГБУ «Управление социальной защиты и социального обслуживания населения по городу Усолье-Сибирское и Усольскому району» для использования в информационных системах персональных данных.

1.2. Действие настоящего Положения распространяется на сотрудников ОГБУ «Управление социальной защиты и социального обслуживания населения по городу Усолье-Сибирское и Усольскому району».

2. Основные термины, сокращения и определения

Администратор ИСПДн — ведущий программист отдела автоматизированных систем, управления базами данных, обеспечивает ввод в эксплуатацию, поддержку и последующий вывод из эксплуатации программного обеспечения и оборудования вычислительной техники.

АРМ — автоматизированное рабочее место пользователя (персональный компьютер, предназначенный для выполнения определенной производственной задачи).

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

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.

Носитель информации — любой материальный объект, используемый для хранения и передачи электронной информации.

Паспорт ПК — документ, содержащий полный перечень оборудования и программного обеспечения АРМ.

ПК — персональный компьютер.

ПО — программное обеспечение вычислительной техники.

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

ПО коммерческое — ПО сторонних производителей (правообладателей). Предоставляется в пользование на возмездной (платной) основе.

Пользователь — работник ОГБУ «Управление социальной защиты и социального обслуживания населения по городу Усолье-Сибирское и Усольскому району», использующий мобильные устройства и носители информации для выполнения своих служебных обязанностей.

3. Порядок использования носителей информации

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

3.2. В ИСПДн допускается использование только учтенных носителей информации, которые являются собственностью учреждения и подвергаются регулярной ревизии и контролю.

3.3. К предоставленным учреждением носителям конфиденциальной информации предъявляются те же требования ИБ, что и для стационарных АРМ (целесообразность дополнительных мер обеспечения ИБ определяется администраторами ИСПДн).

3.4. Носители конфиденциальной информации предоставляются сотрудникам по инициативе Руководителей структурных подразделений в случаях:

- необходимости выполнения вновь принятым работником своих должностных обязанностей;
- возникновения у сотрудника производственной необходимости.

3.5. Процесс предоставления сотрудникам носителей конфиденциальной информации (персональных данных) состоит из следующих этапов:

4. Порядок учета и хранения со съемными носителями конфиденциальной информации (персональных данных), твердыми копиями и их утилизации.

4.1. Все находящиеся на хранении и в обращении съемные носители с конфиденциальной информацией (персональными данными) в учреждении подлежат учёту.

4.2. Каждый съемный носитель С записанными на нем конфиденциальной информацией (персональными данными) должен иметь этикетку, на которой указывается его уникальный учетный номер.

4.3. Учет и выдачу съемных носителей конфиденциальной информации (персональных данных) осуществляют сотрудники структурных подразделений, на которых возложены функции хранения носителей персональных данных. Факт выдачи съемного носителя фиксируется в журнале учета съемных носителей конфиденциальной информации.

4.4. Сотрудники получают учтенный съемный носитель от уполномоченного сотрудника для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнале учета. По окончании работ пользователь сдает

съемный носитель для хранения уполномоченному сотруднику, о чем делается соответствующая " запись в журнале учета.

5. **При использовании сотрудниками носителей конфиденциальной информации (персональных данных) необходимо:**

5.1. Соблюдать требования настоящего Положения.

5.2. Использовать носители информации исключительно для выполнения своих служебных обязанностей.

5.3. Ставить в известность администраторов ИСПДн о любых фактах нарушения требований настоящего Положения.

5.4. Бережно относится к носителям конфиденциальной информации (персональных данных).

5.5. Обеспечивать физическую безопасность носителей информации всеми разумными способами.

5.6. Извещать администраторов ИСПДн о фактах утраты (кражи) носителей конфиденциальной информации (персональных данных).

6. **При использовании носителей конфиденциальной информации (персональных данных) запрещено:**

6.1. Использовать носители конфиденциальной информации (персональных данных) в личных целях.

6.2. Передавать носители конфиденциальной информации (персональных данных) другим лицам (за исключением администраторов ИСПДн).

6.3. 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;

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

7. Порядок обращения со съемными носителями конфиденциальной информации (персональных данных)

7.1. Любое взаимодействие (обработка, прием/передача информации) инициированное сотрудником учреждения между ИСПДн и неучтенными (личными) носителями информации, рассматривается как несанкционированное (за исключением случаев оговоренных с администраторами ИСПДн заранее). Администратор ИСПДн оставляет за собой право блокировать или ограничивать использование носителей информации.

7.2. Информация об использовании сотрудником носителей информации в ИСПДн протоколируется и, при необходимости, может быть предоставлена руководителям структурных подразделений, а также начальнику отдела автоматизированных систем, управления базами данных.

7.3. В случае выявления фактов несанкционированного и/или нецелевого использовании носителей конфиденциальной информации (персональных данных) инициализируется служебная проверка, проводимая комиссией, состав которой определяется начальником отдела автоматизированных систем, управления базами данных.

7.4. По факту выясненных обстоятельств составляется акт расследования инцидента и передается Руководителю структурного подразделения для принятия

мер согласно локальным нормативным актам учреждения и действующему законодательству.

7.5. Информация, хранящаяся на носителях конфиденциальной информации (персональных данных), подлежит обязательной проверке на отсутствие вредоносного ПО.

7.6. При отправке или передаче конфиденциальной информации (персональных данных) адресатам на съемные носители записываются только предназначенные адресатам данные. Отправка конфиденциальной информации (персональных данных) адресатам на съемных носителях осуществляется в порядке, установленном для документов для служебного пользования.

7.7. Вынос съемных носителей конфиденциальной информации (персональных данных) для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя структурного подразделения.

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

7.9. 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 по прилагаемой форме.

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

8. Ответственность

8.1. Работники, нарушившие требования настоящего Положения, несут ответственность в соответствии с действующим законодательством и локальными нормативными актами учреждения.

Директор Воронина Е.В.

Исп. Шевнина Л.Ф.