Государственное бюджетное учреждение
«Первомайский дом-интернат для престарелых и инвалидов».

ПРИКАЗ

«08» июля 2019г. г. Первомайск № 76/3 о/д

Об утверждении инструкций и назначении ответственных лиц по обработке и защите персональных данных в государственном бюджетном учреждении «Первомайский дом-интернат для престарелых и инвалидов»

В соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ "О персональных данных" и 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" и принятыми в соответствии с ним нормативными правовыми актами, приказываю:

1. Назначить ответственным лицом за организацию обработки персональных данных в государственном бюджетном учреждении «Первомайский дом-интернат для престарелых и инвалидов» Панькину Марию Николаевну, директора.

2. Назначить ответственными лицами за обработку персональных данных в государственном бюджетном учреждении «Первомайский дом-интернат для престарелых и инвалидов»: Комкову Е.Н., главного бухгалтера; Учирову В.Н., специалиста по кадрам; Трункину О.В., бухгалтера I категории, Суслину Е.В., экономиста II категории, Осипову В.И., специалиста по социальной работе, Курисеву Т.М., старшую медицинскую сестру, Недякину В.А., медицинскую сестру, Сарычеву А.Г. медицинскую сестру, Милину С.Н., медицинскую сестру, Обухова А.В., медицинскую сестру.

3. Утвердить Инструкцию ответственного за организацию обработки персональных данных в государственном бюджетном учреждении «Первомайский дом – интернат для престарелых и инвалидов» согласно приложению 1 к настоящему Приказу.

4. Утвердить Инструкцию ответственного за обработку персональных данных в государственном бюджетном учреждении «Первомайский дом – интернат для престарелых и инвалидов» согласно приложению 2 к настоящему Приказу.

5. Утвердить Инструкцию пользователя по работе с персональными данными в государственном бюджетном учреждении «Первомайский дом-интернат для престарелых и инвалидов» согласно приложению 3 к настоящему Приказу.

6. Утвердить Инструкцию по работе с обращениями субъектов персональных данных в государственном бюджетном учреждении «Первомайский дом-интернат для престарелых и инвалидов» согласно приложению 4 к настоящему Приказу.

7. Ответственному лицу за организацию обработки персональных данных в учреждении руководствоваться «Инструкцией ответственного за организацию обработки персональных данных в государственном бюджетном учреждении «Первомайский дом-интернат для престарелых и инвалидов».

8. Ответственным лицам за обработку персональных данных осуществлять свою деятельность в соответствии с «Инструкцией ответственного за обработку персональных данных в государственном бюджетном учреждении «Первомайский дом-интернат для престарелых и инвалидов».

9. Сотрудникам, допущенным к обработке персональных данных осуществлять свою деятельность в соответствии с «Инструкцией пользователя по работе с персональными данными в государственном бюджетном учреждении «Первомайский дом-интернат для престарелых и инвалидов» и «Инструкцией по работе с обращениями субъектов персональных данных государственном бюджетном учреждении «Первомайский дом-интернат для престарелых и инвалидов»

10. Считать утратившим силу приказ №7 от 09.01.2018 года «О назначении ответственных лиц по работе с персональными данными».

11. Контроль над исполнением настоящего Приказа оставляю за собой.

Директор М.Н.Панькина

Приложение 1 к приказу
ГБУ «Первомайский дом-интернат»
от "08" июля 2019 г. № 76/3 о/д

Инструкция лица, ответственного за организацию обработки персональных данных в государственном бюджетном учреждении «Первомайский дом-интернат для престарелых и инвалидов»

1. Общие положения

1.1. Настоящая инструкция лица, ответственного за организацию обработки персональных данных (далее – Инструкция) разработана в соответствии со ст. 22.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

1.2. Настоящая Инструкция закрепляет обязанности, права и ответственность лица, ответственного за организацию обработки персональных данных в государственном бюджетном учреждении «Первомайский дом-интернат для престарелых и инвалидов» (далее – Учреждение).

1.3. Лицо, ответственное за организацию обработки персональных данных, в своей работе руководствуется Федеральным законом от 27.07.2006 № 152 - ФЗ «О персональных данных», иными нормативными правовыми актами, настоящей Инструкцией, а также локальными нормативными актами Учреждения, регламентирующими вопросы обработки персональных данных.

2. Обязанности лица, ответственного за организацию обработки персональных данных в Учреждении

2.1. Лицо, ответственное за организацию обработки персональных данных в организации обязано:

- осуществлять внутренний контроль за соблюдением работниками Учреждения законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

- доводить до сведения работников Учреждения, положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

- организовывать прием и обработку обращений и запросов субъектов персональных, данных или их представителей и осуществлять контроль за приемом и обработкой указанных обращений и запросов.

3. Права лица, ответственного за организацию обработки персональных данных в Учреждении

3.1. Лицо, ответственное за организацию обработки персональных данных, имеет право:

- принимать решения в пределах своей компетенции;

- требовать от работников Учреждения соблюдения действующего законодательства, а также локальных нормативных актов Учреждения о персональных данных;

- контролировать в Учреждении осуществление мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами;

- взаимодействовать с министерством социальной политики Нижегородской области и структурными подразделениями Учреждения по вопросам обработки персональных данных.

4. Ответственность лица, ответственного за организацию обработки персональных данных в Учреждении

4.1. За ненадлежащее исполнение или неисполнение настоящей Инструкции, а также за нарушение требований законодательства о персональных данных лицо, ответственное за организацию обработки персональных данных в Учреждении, несет предусмотренную законодательством Российской Федерации ответственность.

Приложение 2 к приказу
ГБУ «Первомайский дом-интернат»
от "08"июля 2019 г. № 76/3 о/д

ИНСТРУКЦИЯ
ответственного за обработку персональных данных в государственном бюджетном учреждении «Первомайский дом-интернат для престарелых и инвалидов»

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Данная Инструкция определяет основные обязанности и права ответственного за обработку персональных данных в государственном бюджетном учреждении «Первомайский дом-интернат» для престарелых и инвалидов» (далее – Учреждение).

1.2. Ответственный за обработку персональных данных является сотрудником Учреждения и назначается приказом директора.

1.3. Решение вопросов обработки персональных данных в Учреждении входит в обязанности ответственного за обработку персональных данных.

1.4. Ответственный за обработку персональных данных обладает правами доступа к любым носителям персональных данных в Учреждении.

II. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. **Автоматизированное рабочее место (АРМ)** – персональный компьютер и подключенные к нему периферийные устройства – принтер, многофункциональные устройства, сканеры и т.д.

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

2.3. **Доступ к информации** – возможность получения информации и её использования.

2.4. **Защита информации** — деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на информацию, то есть процесс, направленный на достижение информационной безопасности.

2.5. **Информация** - сведения (сообщения, данные) независимо от формы их представления.

2.6. **Информационная система персональных данных (ИСПДн)** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.7. **Несанкционированный доступ (НСД)** – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путём изменения (повышения, фальсификации) своих прав доступа.

2.8. **Носитель информации** - любой материальный объект или среда, используемый для хранения или передачи информации.

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

2.10. **Персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных

данных).

2.11. **Средство защиты информации (СЗИ)** – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

2.12. **Угрозы безопасности персональных данных (УБПДн)** - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных.

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

III. ДОЛЖНОСТНЫЕ ОБЯЗАННОСТИ

Ответственный за обработку персональных данных обязан:

3.1. Знать перечень и условия обработки персональных данных в Учреждении.

3.2. Знать и предоставлять на утверждение директора Учреждения изменения к списку лиц, доступ которых к персональным данным необходим для выполнения ими своих служебных (трудовых) обязанностей.

3.3. Участвовать в определении полномочий пользователей ИСПДн (оформлении разрешительной системы доступа), минимально необходимых им для выполнения служебных (трудовых) обязанностей.

3.4. Осуществлять учёт документов, содержащих персональные данные, их уничтожение, либо контроль процедуры их уничтожения.

3.5. Блокировать доступ к персональным данным при обнаружении нарушений порядка их обработки.

3.6. Реагировать на попытки несанкционированного доступа к информации в установленном ст.4 настоящей Инструкции порядке.

3.7. Контролировать осуществление мероприятий по установке и настройке средств защиты информации.

3.8. По указанию руководства своевременно и точно отражать изменения в локальных нормативно-правовых актах по управлению средствами защиты информации в ИСПДн и правилам обработки персональных данных.

3.9. Проводить занятия и инструктажи с сотрудниками Учреждения о порядке работы с персональными данными и изучение руководящих документов в области обеспечения безопасности персональных данных.

3.10. Проводить разбирательства и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с документами, содержащими персональные данные, или по другим нарушениям, которые могут привести к снижению уровня защищённости персональных данных.

3.11. Контролировать соблюдение сотрудниками локальных документов, регламентирующих порядок работы с программными, техническими средствами ИСПДн и персональными данными.

3.12. Вносить свои предложения по совершенствованию мер защиты персональных данных в ИСПДн, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня защищённости персональных данных.

3.13. Организовать учет обращений субъектов персональных данных, контролировать заполнение «Журнала учета обращений субъектов персональных данных».

3.14. Представлять интересы Учреждения при проверках надзорных органов в

сфере обработки персональных данных.

3.15. Знать законодательство РФ о персональных данных, следить за его изменениями.

3.16. Выполнять иные мероприятия, требуемые нормативными документами по защите персональных данных.

IV. ДЕЙСТВИЯ ПРИ ОБНАРУЖЕНИИ ПОПЫТОК НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

4.1. К попыткам несанкционированного доступа относятся:

4.1.1. сеансы работы с персональными данными незарегистрированных пользователей, или пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истёк, или превышающих свои полномочия по доступу к данным;

4.1.2. действия третьего лица, пытающегося получить доступ (или уже получившего доступ) к ИСПДн, при использовании учётной записи администратора или другого пользователя ИСПДн, методом подбора пароля, использования пароля, разглашённого владельцем учётной записи или любым другим методом.

4.2. При выявлении факта несанкционированного доступа ответственный за обработку персональных данных обязан:

4.2.1. прекратить несанкционированный доступ к персональным данным;

4.2.2. доложить директору Учреждения служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;

4.2.3. известить пользователя, от имени учетной записи которого была осуществлена попытка несанкционированного доступа, о факте несанкционированного доступа;

4.2.4. известить администратора безопасности ИСПДн о факте несанкционированного доступа.

V. ПРАВА

Ответственный за обработку персональных данных имеет право:

5.1. Требовать от сотрудников выполнения локальных нормативно-правовых актов в части работы с персональными данными.

5.2. Блокировать доступ к персональным данным любых пользователей, если это необходимо для предотвращения нарушения режима защиты персональных данных.

5.3. Проводить служебные расследования и опрашивать пользователей по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с техническими и программными средствами ИСПДн, в том числе со средствами защиты информации, или по другим нарушениям, которые могут привести к снижению уровня защищённости персональных данных.

VI. ОТВЕТСТВЕННОСТЬ

6.1. Ответственный за обработку персональных данных несёт персональную ответственность за соблюдение требований настоящей Инструкции, за качество проводимых им работ по обеспечению безопасности персональных данных и за все действия, совершенные от имени его учётной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учётной записи.

6.2. Ответственный за обработку персональных данных при нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несёт дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

Приложение 3
к приказу
ГБУ «Первомайский дом-интернат»
от "08"июля 2019 г. № 76/3 о/д

ИНСТРУКЦИЯ
пользователя по работе с персональными данными в государственном бюджетном учреждении «Первомайский дом-интернат для престарелых и инвалидов»

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция определяет общие правила работы сотрудников государственного бюджетного учреждения «Первомайский дом-интернат для престарелых и инвалидов» (далее – Учреждение) с персональными данными.

1.2. Персональные данные в электронном виде обрабатывается в информационных системах персональных данных. Также устанавливается особый порядок обработки и хранения персональных данных, содержащихся на бумажных носителях.

1.3. Пользователем является каждый сотрудник Учреждения, участвующий в рамках своих функциональных обязанностей в процессах как автоматизированной обработки, так и обработки без использования средств автоматизации персональных данных, а также имеющий доступ к аппаратным средствам, программному обеспечению, носителям информации и средствам защиты.

1.4. Пользователь в своей работе руководствуется настоящей Инструкцией, Порядком обработки персональных данных, руководящими и нормативно-правовыми актами Российской Федерации и другими документами Учреждения, регламентирующими обработку персональных данных.

1.5. Методическое руководство по работе Пользователя осуществляет ответственный за организацию обработки персональных данных.

II. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

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

2.3. Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

2.4. Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

2.5. Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

2.6. Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.7. Автоматизированное рабочее место (АРМ) – программно-технический комплекс, посредством которого Пользователь выполняет свои должностные обязанности (персональный компьютер, ноутбук, терминал и т.п.).

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

2.9. Посторонние лица – лица, которые не имеют права самостоятельного доступа в помещение и (или) не имеют права самостоятельного доступа в ИСПДн и (или) не имеют допуска к персональным данным.

2.10. Средство защиты информации от несанкционированного доступа (СЗИ от НСД) – программное, техническое или программно-техническое средство, направленное на предотвращение или существенное затруднение несанкционированного доступа к информации.

III. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ

3.1. Не разглашать персональные данные, которые будут доверены или станут известны в ходе рабочего процесса во время выполнения должностных (договорных) обязанностей.

3.2. Не сообщать устно или письменно, не передавать в каком-либо виде третьим лицам и не раскрывать публично персональные данные без соответствующего разрешения директора Учреждения.

3.3. Знать и выполнять требования законодательных актов Российской Федерации, настоящей Инструкции и других внутренних документов, регламентирующих порядок обработки персональных данных.

3.4. Выполнять на АРМ только те процедуры обработки персональных данных, которые определены должностной инструкцией.

3.5. Знать и соблюдать установленные требования обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности персональных данных.

3.6. Использовать для хранения персональных данных только определенные места хранения и учтенные носители персональных данных.

3.7. Незамедлительно, в кратчайшие сроки, сообщать Учреждению об утрате или недостаче носителей информации, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов и о других фактах, которые могут привести к разглашению персональных данных.

3.8. При прекращении работ (трудовых отношений) все материальные носители, содержащие персональные данные (флеш-накопители, дискеты, оптические диски, документы, черновики, распечатки на принтерах, кино- и фотоматериалы, модели,

промышленные образцы и пр.), передать руководителю структурного позразделения Учреждения.

3.9. Соблюдать требования парольной политики (раздел 4).

3.10. Соблюдать требования антивирусной защиты (раздел 5).

3.11. Пользователи, имеющие выход в Интернет, обязаны соблюдать правила при работе в сетях связи общего пользования и (или) сетях международного информационного обмена (раздел 6).

3.12. Экран монитора в 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).

3.13. Обо всех выявленных нарушениях, связанных с порядком обработки персональных данных, а также для получений консультаций по вопросам обработки персональных данных, необходимо обращаться к ответственному за организацию обработки персональных данных.

Пользователям запрещается:

3.13.1. Нарушать установленные в Учреждении инструкции по работе с персональными данными.

3.13.2. Использовать компоненты программного и аппаратного обеспечения Учреждения в неслужебных целях.

3.13.3. Оставлять свое рабочее место без присмотра, предварительно не заблокировав (штатными средствами операционной системы Windows – комбинацией клавиш [WIN] + [L] или [CTRL] + [ALT] + [DEL] с дальнейшим нажатием кнопки «Блокировка» появившегося меню, либо при помощи штатных средств защиты информации от несанкционированного доступа при их наличии).

3.13.4. Оставлять без присмотра или неубранными в хранилища (шкаф, сейф) носители или документы, содержащие персональные данные.

3.13.5. Записывать и хранить персональные данные на неучтенных носителях информации (оптических дисках, гибких магнитных дисках, флеш-накопителях и т.п.).

3.13.6. Самовольно изменять состав и конфигурацию используемых программных, аппаратных, программно-аппаратных средств, самовольно устанавливать программное обеспечение, отключать/подключать оборудование или изменять режимы его работы.

3.13.7. Самовольно подключать АРМ или другие средства к ЛВС Учреждения, изменять IP-адрес, MAC-адрес и иные настройки сети АРМ.

3.13.8. Производить действия, направленные на получение несанкционированного доступа к АРМ и серверам, равно как и любым другим узламЛВС Учреждения или Интернет, в том числе:

- действия, направленные на нарушение нормального функционирования элементов сети (компьютеров, другого сетевого оборудования или программного обеспечения);

- установка программного обеспечения, осуществляющего перехват информации (информационных пакетов), адресованной другим пользователям;

- действия, направленные на получение несанкционированного доступа к информационным ресурсам, в последующем использовании такого доступа;

- уничтожение, модификация программного обеспечения или данных без согласования с директором или владельцами этого ресурса;

- попытки подбора паролей к любым информационным ресурсам методом перебора всех возможных вариантов паролей, либо атак по словарю;

- умышленные действия по созданию, использованию и распространению вредоносных программ, в том числе направленных на получение несанкционированного доступа к любым информационным и служебным ресурсам (как внутри Учреждения так и вне), либо на нарушение целостности и работоспособности этих систем;

- действия по сканированию локальной сети с целью определения ее внутренней структуры, списков открытых портов, наличия существующих сервисов и уязвимостей.

3.13.9. Самовольно изменять параметры средств защиты информации (в том числе и средств антивирусной защиты), а также завершать их работу и (или) самостоятельно их устанавливать.

3.13.10. Самостоятельно разрабатывать или использовать нерегламентированные (без разрешения директора, не относящиеся к производственному процессу) программы (например: игры; ГМ-клиенты, такие как GoogleMessenger, ICQ и т.п.; P2P-клиенты: Kazaa, eMule и т.п.).

3.13.11. Разрешать посторонним лицам работать под своей учетной записью в ИСПДн.

3.13.12. Получать доступ к персональным данным с рабочих мест, не оборудованными необходимыми средствами защиты информации.

3.13.13. Самовольно создавать совместно используемые сетевые ресурсы (папки общего доступа) на своих компьютерах и файловых серверах, несанкционированно удалять или изменять права доступа к ним.

3.13.14. В случае возникновения любых механических неисправностей в оборудовании осуществлять самостоятельные попытки их устранения.

3.13.15. Препятствовать должностным лицам при проведении проверок и служебных расследований, связанных с обеспечением безопасности информации.

3.13.16. Удалять или искажать программы и файлы с персональными данными и иной важной информацией (например, системной, необходимой для функционирования ИСПДн).

3.13.17. Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению внештатной ситуации. Об обнаружении такого рода ошибок - ставить в известность руководителя своего подразделения и сотрудников, ответственных за установку и (или) сопровождение программного обеспечения.

3.13.18. Подключать к ЛВС Учреждения личные средства вычислительной техники: ноутбуки, карманные компьютеры, смартфоны и т.п., а также личные носители и накопители информации. В случае необходимости переноса информации с личных носителей информации обращаться к ответственным.

IV. ПАРОЛЬНАЯ ПОЛИТИКА

4.1. Общие требования к паролям:

Минимальное требование: буквенно-цифровой пароль. Желательно использовать буквы в верхнем или нижнем регистрах, цифры или специальные символы (например: ~ ! @ # $ %л& * ( ) _ - + = | \ ? / . , : ; ’] [{ } <> . и т.п.).

Минимальная длина пароля: не менее 6 (шести) символов.

Максимальный срок действия пароля: 90 суток.

- Запрет использования трех ранее использовавшихся паролей.

- Пароль Пользователя не должен включать в себя легковычисляемые сочетания символов, общепринятые сокращения, имена, фамилии, должности, год рождения, номер паспорта, табельный номер, иную информацию о Пользователе, доступную другим лицам.

- Запрещается использовать в качестве пароля один и тот жеповторяющийся символ либо повторяющуюся комбинацию из нескольких символов.

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

4.2. Правила использования паролей:

Хранить в тайне свой пароль, не сообщать его другим лицам.

- Не предоставлять доступ в ИСПДн другим лицам под своейучетной записью и паролем.

Изменять свой пароль при первом требовании политики паролей операционной системы и/или ИСПДн.

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

- Запрещается записывать свои пароли в очевидных местах, внутренности ящика стола, на мониторе АРМ, на обратной стороне клавиатуры и т.д.

- Запрещается хранить пароли в записанном виде на отдельных листах бумаги.

4.3. Смена, удаление личного пароля любого Пользователяпроизводится в следующих случаях:

- в случае подозрения на компрометацию пароля;

- по окончании срока действия;

- в случае прекращения полномочий (увольнение, переход на другую работу внутри Учреждения) Пользователя после окончания последнего сеанса работы в информационных системах персональных данных;

- по указанию ответственного за организацию обработки персональныхданных.

4.4. При увольнении, переходе на новую должность сотрудника,имеющего доступ помимо своей учетной записи к другим ресурсам(межсетевые экраны, маршрутизаторы, серверы, другие учетные записи и т.п.) также производится внеплановая смена паролей к таким ресурсам.

V. ПРИМЕНЕНИЕ ЛИЧНЫХ ИДЕНТИФИКАТОРОВ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

5. Привязку идентификатора к пользователю (учетной записи) выполняет администратор безопасности.

5.1. Пользователи ИСПДн получают свой идентификатор у администратора безопасности.

5.2. Пользователь ИСПДн обязан хранить свой личный идентификатор в недоступных для других сотрудников хранилищах.

5.3. Пользователю ИСПДн запрещается передавать свой личный идентификатор.

5.4. В случае утери личного идентификатора, пользователь ИСПДн должен немедленно доложить об этом администратору безопасности информации.

5.5. В случае прекращения полномочий учетной записи пользователя ИСПДн (увольнение, переход на другую работу, в другой отдел или помещение, а также другие обстоятельства) учетная запись должна быть удалена, а её идентификатор должен быть сдан администратору безопасностиинформации после окончания последнего сеанса работы данного пользователя в ИСПДн.

5.6. В случае компрометации или утери личного идентификатора пользователя специалистом по защите информации должны быть немедленно предприняты меры в соответствии с п. 5.7 настоящей Инструкции.

5.7. Администратор безопасности информации должен провести служебное расследование для выяснения причин компрометации идентификатора с целью выработки новых или совершенствования принятых технических и организационных мер по устранению такой угрозы в будущем, а также выяснению величины ущерба, который может быть нанесен собственнику информационных ресурсов.

VI. АНТИВИРУСНАЯ ЗАЩИТА

6.1. В случае отсутствия штатных функций антивирусной программы,предусматривающих автоматическую проверку файлов, Пользователь обязан осуществлять проверку файлов, получаемых:

- по электронной почте;
- через сеть Интернет;
- на магнитном, оптическом диске, флеш-накопителе;
- ином съемном носителе информации;
- полученные иным способом.

6.2. Перед открытием вложения (ссылок) убедиться в том, что отправитель действительно послал вам этот файл, даже если он и должен был это сделать. Позвоните ему сами. Не доверяйте имени отправителя и указанным в тексте письма номерам телефонов, а также лицам, позвонившим вам самостоятельно с просьбой открыть файлы и пройти по ссылкам.

6.3. Пользователю запрещается:

6.3.1. Осуществлять действия, направленные на выключениеантивирусной программы.

6.3.2. Самостоятельно устанавливать на АРМ программное обеспечение.

6.3.3. Запускать файлы, полученные по сетям связи (электронной почте, Интернет), со съемных носителей, даже если они получены проверенного адресата, без предварительной их проверки антивирусной программой.

6.3.4. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) Пользователь самостоятельно или вместе с ответственным (Специалистом по защите информации) должен провести внеочередной антивирусный контроль своего рабочего места.

6.3.5. В случае обнаружения при проведении антивирусной проверки вирусного заражения Пользователи обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения вирусного заражения ответственному специалисту по защите информации;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов.

VII. ПОРЯДОК РАБОТЫ В ИСПДН И СЕТИ ИНТЕРНЕТ

7.1. Подключение к ИСПДн и сети Интернет

7.1.1. Целью работы Пользователя в ИСПДн и сети Интернет является сбор, обработка, хранение персональных данных, обмен электронными сообщениями в служебных целях.

7.1.2. Доступ к ИСПДн и сети Интернет предоставляется Пользователям только в том случае, если это не противоречит требованиям настоящей Инструкции и иными нормативными документами в области защиты информации.

7.1.3. Доступ пользователя к ИСПДн для обработки персональных данных производится только с рабочих мест, на которых установлены средства защиты информации.

7.1.4. Основанием для подключения сотрудника Учреждения к ИСПДн и сети Интернет является мотивированная заявка ответственному за организацию обработки персональных данных от непосредственного руководителя Пользователя с указанием полномочий доступа к таким ресурсам и сервисам.

7.1.5. Основанием для отключения пользователя от ИСПДн и сети Интернет являются следующие события:

- нарушение инструкций и иных локальных нормативных актов в области защиты информации Учреждения;

- увольнение Пользователя, либо перевод его в другое подразделение.

7.2. Порядок работы в сети Интернет

7.2.1. Использование сотрудниками Учреждения сети Интернет должно осуществляться исключительно для выполнения должностных обязанностей.

7.2.2. Информация, образованная (образующаяся) в процессе трудовой деятельности работника Учреждения является собственностью Учреждения и не подлежит использованию (в том числе использованию в сети Интернет или с помощью сети Интернет) в личных целях и (или) в корыстных интересах других лиц (организаций).

7.2.3. При проведении технических работ, связанных с настройкой оборудования (коммуникационное оборудование, прокси-сервера, маршрутизаторы и т.п.); в случае обнаружения попыток несанкционированного доступа к Интернет-шлюзу, АРМ Пользователей может проводиться временное отключение Пользователей от сервисов сети Интернет (в случае планового отключения Пользователи уведомляются об этом заблаговременно).

7.2.4. При работе в сети Интернет Пользователям запрещается:

- умышленное распространение и получение материалов в/из сети Интернет, противоречащих законодательству Российской Федерации, в том числе материалов, пропагандирующих насилие или экстремизм; разжигающих расовую, национальную или религиозную вражду; разъясняющих порядок изготовления и/или применения наркотиков, взрывчатых веществ, оружия и т.п.; материалов порнографического характера; компьютерных вирусов и других вредоносных программ;

- передавать в сеть Интернет информацию, к которой в соответствии с законодательством ограничен доступ (персональные данные, служебная информация) без соответствующего разрешения;

- фальсифицировать IP-адрес, MAC-адрес, иные адреса, используемые в сетевых протоколах, а также прочую информацию при передаче данных через сеть Интернет.

- предоставлять доступ в сеть Интернет со своей рабочей станции кому-либо, в том числе программно-техническими способами через локальную вычислительную сеть Учреждения (например: путем несанкционированной установки локального Интернет-шлюза на рабочее место);

- получать доступ к сети Интернет любыми способами, не предусмотренными действующими локальными документами (Инструкциями, Правилами, Регламентами Учреждения);

- осуществлять несанкционированный доступ к ресурсам и сервисам сети Интернет.

- выполнять действия (взлом, DoS (отказ в обслуживании), ARP-spoofing атаки, сканирование локальной вычислительной сети) направленные на нарушение

функционирования элементов сети Интернет (коммуникационного оборудования, серверов, рабочих станций, программного обеспечения).

7.3. Правила работы Пользователей с электронной почтой:

7.3.1. Пользователи обязаны использовать электронную почту только для выполнения служебных обязанностей.

7.3.2. Запрещается отправлять файлы, содержащие персональные данные в открытом виде (не зашифрованные).

7.3.3. Запрещается массовая рассылка почтовых сообщений (более 100) внешним адресатам без согласования с руководством (спама).

7.3.4. Запрещается использовать не свой обратный адрес при отправке электронной почты.

7.3.5. Запрещается отправлять по электронной почте исполняемые файлы (обычно имеют расширения exe, com, bat, js, vbs и т.п.). В случае необходимости отправки таких файлов, помещать их в архив и установить пароль.

7.3.6. Присоединяемые файлы рекомендуется упаковывать в архив при помощи программ-архиваторов.

7.3.7. Корпоративные рекомендации использования электронной почты:

- Вы должны оказывать то же уважение, что и при устном общении.

- Вы должны проверять правописание, грамматику и дважды перечитывать свое сообщение перед отправлением.

- Вы не должны участвовать в рассылке посланий, пересылаемых по цепочке (чаще всего это письма религиозно-мистического, развлекательного содержания).

- Вы не должны по собственной инициативе пересылать по произвольным адресам незатребованную информацию.

- Вы не должны рассылать сообщения, которые являются зловредными, раздражающими или содержащими угрозы другим пользователям.

- Вы не должны отправлять никаких сообщений противозаконного или неэтичного содержания.

- Вы должны помнить, что электронное послание является эквивалентом почтовой открытки и не должно использоваться для пересылки персональных данных без использования средств защиты (шифрование).

- Вы не должны использовать широковещательные возможности электронной почты за исключением выпуска уместных объявлений.

- Вы не должны использовать корпоративную электронную почту для посланий личного характера.

- Вы должны неукоснительно соблюдать правила и инструкции и помогать администраторам бороться с нарушителями правил.

VIII. ПОРЯДОК РАБОТЫ СО СЪЕМНЫМИ НОСИТЕЛЯМИ ИНФОРМАЦИИ

8.1.Под использованием носителей информации в ИСПДнУчреждения понимается их подключение к инфраструктуре ИСПДн с целью обработки, приема/передачи информации между информационными системами и носителями информации.

8.2.Допускается использование только учтенных носителей информации, которые являются собственностью Учреждения и подвергаются регулярной ревизии и контролю.

8.3.Учет и выдачу съемных носителей информации осуществляет лицо, ответственное за организацию обработки персональных данных. Факт выдачи носителя фиксируется в журнале учета машинных носителей информации.

8.4.Если доступ к ИСПДн производится при помощи персональных идентификаторов (eToken, Rutoken, др.), то факт получения и сдачи данных идентификаторов обязательно фиксируется ответственным за организацию обработки персональных данных, в соответствующих журналах.

8.5.Возможность подключения носителей информации, а также получение учтенных носителей информации предоставляются Пользователям по инициативе руководителей структурных подразделений в случаях:

- необходимости выполнения вновь принятым работником своих должностных обязанностей;

- возникновения у Пользователя служебной необходимости.

8.6.При использовании носителей информации необходимо:

- использовать носители информации исключительно для выполнения своих служебных обязанностей;

- бережно относится к носителям персональных данных;

- обеспечивать физическую безопасность носителей информациивсеми разумными способами;

- извещать ответственному за организацию обработкиперсональных данных о фактах утраты (кражи) носителей информации.

8.7.При использовании носителей персональных данных запрещено:

- использовать носители персональных данных в личных целях;

- передавать носители персональных данных другим лицам (за исключением администраторов);

- хранить съемные носители с персональными данными на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

- выносить съемные носители с персональными данными из служебных помещений для работы с ними на дому и т. д.

8.8.В случае выявления фактов несанкционированного и/или нецелевого использовании носителей информации инициируется служебная проверка, проводимая комиссией, состав

которой определяется ответственным за организацию обработки персональных данных. По факту выясненных обстоятельств составляется акт расследования инцидента и передается руководителю структурного подразделения для принятия мер согласно локальным нормативным актам Учреждения и действующему законодательству РФ.

8.9.При отправке или передаче персональных данных адресатам на съемные носители записываются только предназначенные адресатам данные.

8.10.Вынос съемных носителей персональных данных для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя структурного подразделения.

8.11.Съемные носители персональных данных, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с персональными данными осуществляется комиссией, состав которой определяется ответственным за организацию обработки персональных данных. По результатам уничтожения носителей составляется акт.

8.12.В случае увольнения или перевода работника в другое структурное подразделение, предоставленные носители персональных данных изымаются и делаются соответствующие пометки в журнале учета машинных носителей.

IX. ПРАВА ПОЛЬЗОВАТЕЛЯ

9.1. Использовать ИСПДн Учреждения для выполнения должностных обязанностей.

9.2. Обращаться к ответственному за организацию обработкиперсональных данных для консультаций по поводу использования программного обеспечения и АРМ, вопросам обработки персональных данных.

9.3. Направлять предложения по установке новых версий существующего программного обеспечения (с обоснованием необходимости замены старых версий на новые).

9.4. Направлять предложения по установке нового (а также дополнительного) программного обеспечения (с указанием цели использования, преимуществ перед существующими аналогами).

9.5. Направлять предложения по модернизации АРМ (замены на новые аналоги), с обязательным обоснованием замены и указанием преимуществ перед существующими аналогами.

9.6.Получать консультации и разъяснения по нормативным документам, регламентирующим работу с персональными данными в Учреждении.

X. ОТВЕТСТВЕННОСТЬ

10. Пользователь несет персональную ответственность за свои действия или бездействие, которые могут повлечь за собой разглашение персональных данных, а также за нарушение нормального функционирования ИСПДн или их отдельных компонентов, несанкционированный доступ к информации в соответствие с законодательством Российской Федерации и локальными нормативными актами Учреждения.

Приложение 4
к приказу
ГБУ « Первомайский дом-интернат»
от "08"июля 2019 г. № 76/3 о/д

ИНСТРУКЦИЯ

по работе с обращениями субъектов персональных данных в Государственном бюджетном учреждении « Первомайский дом- интернат для престарелых и инвалидов».

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция разработана на основании требований Федерального закона РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных» и определяет порядок и сроки обработки обращений субъектов персональных данных.

1.2. К рассмотрению обращений субъектов ПДн и граждан в соответствии с должностными инструкциями допускаются лица, имеющие по своим должностным обязанностям доступ к обработке персональных данных.

1.3. В соответствии со ст. 14 ФЗ РФ от 27.07.2006 г. № 152-ФЗ субъект персональных данных имеет право обратиться к Оператору персональных данных на получение информации, касающейся обработки его персональных данных. Требуемые сведения предоставляются субъекту персональных данных при личном обращении или по его письменному запросу (Приложение 1).

1.4. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных (или его полномочного представителя), сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных (или его полномочного представителя).

1.5. Субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

Оператор обязан в срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных сведений, подтверждающих что эти сведения являются неполными, неточными или неактуальными, внести необходимые изменения (в том числе уничтожить) в существующие базы данных, в том числе, на материальные носители, а затем уведомить субъекта персональных данных о внесенных изменениях и предпринятых мерах.

Кроме того, при необходимости, принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были или могли быть переданы в

соответствии с требованиями Федерального законодательства или существующими договоренностями.

1.6. При отзыве субъектом согласия на обработку его персональных данных Оператор обязан прекратить их обработку и в случае, если сохранение персональных данных более не требуется для целей их обработки, уничтожить персональные данные в срок, не превышающий тридцати дней с даты поступления указанного отзыва (при условии, что Оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральным законодательством) (Приложение 2).

2. ПОРЯДОК РАССМОТРЕНИЯ ОБРАЩЕНИЙ СУБЪЕКТОВ ПДн

2.1. Поступившее обращение субъекта персональных данных (письменный запрос или устное обращение) подлежит обязательной регистрации в Журнале регистрации обращений граждан (Приложение 3) и рассмотрению в течение трех дней с момента поступления.

2.2. Руководитель организации при получении запроса от субъекта персональных данных в своей резолюции назначает лицо, ответственное за рассмотрение запроса и подготовку ответа на поступившее обращение.

2.3. При подготовке письменного ответа ответственный сотрудник от лица Оператора персональных данных обязан:

2.3.1. Сообщить заявителю информацию о порядке и сроках рассмотрения обращения, подтвердив факт обработки персональных данных Оператором;

2.3.2. Предоставить при необходимости возможность личного ознакомления с имеющимися у Оператора персональными данными, в том числе:

- о полном наименовании и месте нахождения Оператора персональных данных;
- о правовых основаниях и целях обработки персональных данных;
- о применяемых оператором способах обработки персональных данных;
- о составе обрабатываемых персональных данных, относящихся к соответствующему субъекту персональных данных, источнике их получения;
- о сроках обработки персональных данных, в том числе порядке их хранения и уничтожения;
- о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
- о наименовании или фамилии, имени, отчестве и адресе лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
- об иных сведениях, предусмотренных Федеральным законодательством или иными нормативными актами.

2.3.3. Подготовить в течение тридцати дней с даты регистрации запроса письменный ответ и направить его субъекту персональных данных.

2.4. В случае, если указанные сведения были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к оператору не ранее чем через тридцать дней после первоначального обращения.

2.5. При подготовке отказа в предоставлении информации субъекту персональных данных Оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение Федерального законодательства, являющуюся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных.

Приложение № 1
к Инструкции по
работе
с обращениями
субъектов
персональных данных

Директору
ГБУ «Первомайский дом-интернат»

от_____
(ф.и.о. заявителя)
_____
_____
_____
(наименование и реквизиты документа,
удостоверяющего личность заявителя)

Заявление

Прошу предоставить мне для ознакомления обрабатываемую Вами информацию, составляющую мои персональные данные, указать цели, способы и сроки ее обработки; предоставить сведения о лицах, которые имеют к ней доступ (которым может быть предоставлен такой доступ); сведения о том, какие юридические последствия для меня может повлечь её обработка. В случае отсутствия такой информации, прошу Вас уведомить меня об этом.

_____ _____ _____
(должность) (подпись) (ФИО)

«___»_____20__г.

Приложение № 2
к Инструкции по
работе
с обращениями
субъектов
персональных данных

Директору
ГБУ «Первомайский дом-интернат»

от_____
(ф.и.о. заявителя)
_____
_____
_____
(наименование и реквизиты документа,
удостоверяющего личность заявителя)

ЗАЯВЛЕНИЕ
(отзыв согласия на обработку персональных данных)

На основании п. 2 ст. 9 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», отзываю ранее данное мной согласие на обработку персональных данных.

В случае, если согласие на обработку персональных данных давалось мной неоднократно, я отзываю все ранее данные мной согласия на обработку персональных данных. В соответствии с п. 5 ст. 21 Федерального закона «О персональных данных», в случае отзыва субъектом персональных данных согласия на их обработку, оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва. Я уведомлен, что в, случае отзыва согласия на обработку персональных данных, ГБУ «Первомайский дом-интернат» вправе продолжить обработку персональных данных без моего согласия при наличии оснований, указанных в пунктах 2-11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона № 152-ФЗ «О персональных данных». Уведомление о прекращении обработки и уничтожении моих персональных данных прошу предоставить в письменной форме.

_____ _____ _____
(должность) (подпись) (ФИО)

«___»_____20__г.

Приложение № 3
к Инструкции по
работе
с обращениями
субъектов
персональных данных

Журнал регистрации обращений сотрудников

Дата поступления и индекс док-та	Субъект ПДн	Краткое содержание обращения	Резолюция/ кому направлено	Отметка об исполнении	Результат рассмотрения