ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ
ТЮМЕНСКОЙ ОБЛАСТИ «ГОСПИТАЛЬ ДЛЯ ВЕТЕРАНОВ ВОЙН»
(ГБУЗ ТО «ГОСПИТАЛЬ ДЛЯ ВЕТЕРАНОВ ВОЙН»)

ПРИКАЗ

27.02.2023 № 57д

г. Тюмень

**О назначении ответственных
за организацию обработки персональных данных**

В целях исполнения Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановления Правительства Российской Федерации от 21.03.2013 № 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, операторами, являющимися государственными или муниципальными органами», постановления Правительства от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Приказа ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», **приказываю:**

1. Назначить ответственным за организацию обработки персональных данных (далее – ПДн) в ГБУЗ ТО «Госпиталь для ветеранов войн» начальника организационно-методического кабинета.
2. Ответственному за организацию обработки ПДн обеспечить обработку ПДн на объектах информатизации, удовлетворяющих действующему законодательству.
3. Утвердить инструкцию ответственного за организацию обработки ПДн (Приложение № 1 к настоящему Приказу).
4. Ответственному за организацию обработки ПДн руководствоваться инструкцией, указанной в пункте 2 настоящего Приказа.
5. Утвердить:

5.1. инструкцию пользователя при работе в информационной системе персональных данных (Приложение № 2 к настоящему Приказу);

5.2. перечень должностей, ГБУЗ ТО «Госпиталь для ветеранов войн» допущенных к обработке персональных данных (Приложение № 3 к настоящему Приказу).

6. Сотрудникам, должности которых включены в перечень, указанный в пункте 5.2. настоящего Приказа и допущенным к работе с ПДн, в том числе при работе в ИСПДн, в своей деятельности руководствоваться инструкцией, указанной в пункте 5.1. настоящего Приказа.

7. Ознакомить всех сотрудников, задействованных в обработке персональных данных с настоящим приказом, под подпись.

8. Контроль исполнения настоящего приказа оставляю за собой.

Главный врач Н.Ю. Путина

Приложение № 1
Утверждено
приказом ГБУЗ ТО «Госпиталь для ветеранов войн»
от «27» 02 2023 г. № 57

Инструкция ответственного за организацию обработки персональных

1. Общие положения

1.1. Ответственный за организацию обработки персональных данных в ГБУЗ ТО «Госпиталь для ветеранов войн» (далее – Ответственный) назначается приказом *главного врача* ГБУЗ ТО «Госпиталь для ветеранов войн» (далее – Учреждение) и отвечает за организацию, обеспечение своевременного и квалифицированного выполнения сотрудниками Учреждения законодательства Российской Федерации о персональных данных (далее – ПДн), в том числе требований к обработке и защите ПДн.

1.2. Ответственный должен знать законодательные и иные нормативные правовые акты Российской Федерации, методические материалы в сфере обработки и защиты ПДн. Ответственный поддерживает в актуальном состоянии свои знания в сфере действующего законодательства и законодательных инициатив, связанных с защитой персональных данных.

1.3. В своей деятельности Ответственный руководствуется действующим законодательством Российской Федерации, правовыми актами Тюменской области, а также настоящей Инструкцией.

2. Основные функции ответственного за организацию обработки персональных данных

2.1. Ответственный изучает все стороны деятельности Учреждения и вырабатывает рекомендации по организации обработки ПДн при решении следующих основных вопросов:

- организация доступа к ПДн и учет сотрудников Учреждения, допущенных к обработке ПДн, как в программных комплексах, входящих в состав информационных систем (далее – ИС), так и на бумажных носителях;
- контроль за поддержанием в актуальном состоянии действующих локальных нормативных актов, журналов и форм учета по работе с ПДн;
- контроль за обеспечением соответствия проводимых работ в части обработки ПДн технике безопасности, правилам и нормам охраны труда;
- организация работы по заключению договоров на работы по защите ПДн;
- контроль изменений в процессах обработки ПДн и, в случае необходимости, отправка информации об этих изменениях в уполномоченный территориальный орган по защите прав субъектов персональных данных с целью актуализации уведомления Учреждения в реестре операторов ПДн;
- рассмотрение предложений по совершенствованию действующей системы защиты ПДн, предоставленных администратором информационной безопасности, назначаемым приказом *главного врача* Учреждения;

- осуществление в пределах своей компетенции иных функций в соответствии с целями и задачами Учреждения.

3. Должностные обязанности

3.1. Ответственный за организацию обработки персональных данных обязан:

3.1.1. Организовывать работу в структурных подразделениях по разработке и принятию организационно-распорядительной документации, устанавливать правила обработки персональных данных, которые определяют:

- порядок доступа к персональным данным;
- организацию приема и обработки обращений и запросов субъектов персональных данных или их представителей;
- процедуры, направленные на предотвращение и выявление в Учреждении нарушений действующего законодательства Российской Федерации о персональных данных и устранения последствий таких нарушений.

3.1.2. Обеспечивать своевременное размещение на официальном сайте Учреждения организационно-распорядительной документации, устанавливающей правила обработки персональных данных, в течение 10 дней после их утверждения;

3.1.3. Организовывать ознакомление сотрудников, непосредственно осуществляющих обработку персональных данных, с действующим законодательством Российской Федерации о персональных данных и организационно-распорядительной документации, принятой в Учреждение, определяющими правила обработки персональных данных и требования по защите персональных данных;

3.1.4. Руководить осуществлением приема необходимых правовых, организационных и технических мер для защиты персональных данных в Учреждении в соответствии с действующим законодательством Российской Федерации о персональных данных;

3.1.5. Осуществлять согласование мероприятий при создании в новых информационных систем персональных данных;

3.1.6. Координировать работу в структурных подразделениях по формированию и ведению перечней должностей сотрудников, замещение которых предусматривает осуществление обработки следующих персональных данных:

- персональных данных, обрабатываемых в Учреждении;
- информационных систем персональных Учреждения;

3.1.7. Организовать своевременное направление в Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Тюменской области, ХМАО-Югре и ЯНАО уведомления о намерении осуществлять обработку персональных данных в Учреждении или изменении положений об обработке персональных данных в Учреждении;

3.1.8. Организовывать и руководить проведением внутренних проверок организации состояния работ по вопросам информационной безопасности в для осуществления периодического контроля:

- условий обработки персональных данных в и их соответствие действующему законодательству Российской Федерации о персональных данных и принятыми в соответствии с ним организационно-распорядительной документации;
- организации приема и обработки запросов субъектов персональных данных или их представителей;
- выполнения установленных в соответствии с действующим законодательством Российской Федерации и организационно-распорядительной документации требований к защите персональных данных, обрабатываемых в Учреждении;

3.1.9. Координировать работу структурных подразделений на принятие мер, направленных на совершенствование защиты персональных данных, обрабатываемых в Учреждении;

3.1.10. Осуществлять методическое руководство работой при разработке условий обработки персональных данных и эффективности мер по защите персональных данных в Учреждении;

3.1.11. Организовывать работу по планированию прохождения обучения сотрудников Учреждения по вопросам обеспечения защиты персональных данных.

4. Права ответственного за организацию обработки ПДн

4.1. Ответственный за организацию обработки ПДн в Учреждении имеет право:

4.1.1. запрашивать в структурных подразделениях, в которых ведется обработка ПДн или планируется ведение обработки ПДн, любые сведения, необходимые для организации условий обработки ПДн и принятия необходимых правовых, организационных и технических мер для защиты ПДн;

4.1.2. принимать участие в рассмотрении жалоб и обращений граждан или юридических лиц по вопросам, связанным с обработкой ПДн в Учреждении, а также принимать решения по результатам рассмотрения указанных жалоб и обращений;

4.1.3. участвовать в расследовании нарушений в области защиты ПДн в Учреждении и принимать решения по устранению недостатков и предупреждению подобного рода нарушений;

4.1.4. требовать от структурных подразделений уточнения, блокирования или уничтожения недостоверных, или полученных незаконным путем ПДн, при обращении (запросе) субъекта ПДн или его представителя, либо уполномоченного органа по защите прав субъектов ПДн, либо по результатам проведенной внутренней проверки организации состояния работ по вопросам информационной безопасности;

4.1.5. принимать меры по приостановлению или прекращению обработки персональных данных в Учреждении, осуществляемой с нарушением требований действующего законодательства Российской Федерации о ПДн;

4.1.6. вносить предложения о совершенствовании нормативного правового регулирования обработки и защиты ПДн в Учреждении.

5. Ответственность

5.1. Ответственный за организацию обработки персональных данных в Учреждении несет ответственность за ненадлежащее выполнение возложенных на него обязанностей, изложенных в настоящей должностной инструкции, в соответствии с действующим законодательством Российской.

6. Заключительные положения

6.1. Должностная инструкция подлежит пересмотру в случае изменения законодательства Российской Федерации о ПДн.

Приложение № 2
Утверждена
приказом ГБУЗ ТО «Госпиталь для ветеранов войн»
от «27» 02 2023 г. №57

Инструкция пользователя при работе в информационной системе персональных данных

1. Общие положения

1.1. Настоящая Инструкция определяет порядок обеспечения безопасности информации при ее обработке пользователями на объектах информатизации (далее – ОИ) ГБУЗ ТО «Госпиталь для ветеранов войн» (далее – Учреждение).

1.2. Ответственность за функционирование системы защиты информации (далее – СЗИ) возлагается на администратора информационной безопасности (далее – АБИ).

1.3. Ответственность за выполнение установленных Инструкцией требований возлагается на работника Учреждения, производящего обработку информации с использованием средств вычислительной техники на автоматизированном рабочем месте (далее - АРМ пользователя).

1.4. К работе с защищаемой информацией допускаются только работники, ознакомленные с настоящей Инструкцией под личную подпись в листе ознакомления.

1.5. Вход в помещения, в которых производится автоматизированная обработка защищаемой информации, разрешается постоянно работающим в нём работникам. Лицам, привлекаемым к проведению ремонтных, наладочных и других работ, а также посетителям, вход в помещения разрешается только в сопровождении ответственных лиц.

1.6. По фактам и попыткам несанкционированного доступа (далее – НСД) к защищаемой информации, а также в случаях её утечки и (или) модификации (уничтожения) проводятся служебные расследования.

1.7. Пользователи имеют право письменно вносить предложения по изменению и дополнению настоящей Инструкции. Изменения и дополнения к настоящей Инструкции утверждаются в установленном порядке.

2. Обязанности

Пользователь обязан:

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

2.2. Знать и соблюдать установленные требования к обработке информации ограниченного доступа, учету и хранению носителей информации, обеспечению информационной безопасности.

2.3. Выполнять только те процедуры, которые определены технологическим процессом обработки информации ограниченного доступа.

2.4. Соблюдать требования парольной политики в соответствии с Инструкцией по организации парольной защиты. Получить уникальное имя и персональный идентификатор (при его наличии) от АБИ. Пользователь обязан помнить и соблюдать в тайне свои имена и пароли, не допускается их запись на каких-либо носителях в целях напоминания. При утере или подозрении на утечку своего имени, пароля и персональных идентификаторов пользователь должен немедленно сообщить об этом АБИ.

2.5. Во время работы располагать экран монитора так, чтобы затруднить посетителям просмотр отображаемой информации.

2.6. При отсутствии визуального контроля за рабочей станцией доступ к компьютеру должен быть немедленно заблокирован.

2.7. При отсутствии пользователя на рабочем месте либо в присутствии лиц, не имеющих допуска к ресурсам ОИ, все документы, содержащие защищаемую информацию, должны быть недоступны для просмотра и иного их использования.

2.8. Немедленно приостановить работы, вызывать АБИ и поставить в известность руководителя структурного подразделения в следующих случаях:

- возникновение подозрения на наличие вредоносного программного обеспечения (частые ошибки в работе программ, появление посторонних графических и звуковых эффектов, искажения данных, неконтролируемое пропадание файлов, появление сообщений о системных ошибках, замедление работы компьютера и т.п.);
- появления информационного окна средства антивирусной защиты, сигнализирующем об обнаружении вредоносного программного обеспечения;
- обнаружения нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на аппаратных средствах АРМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа к защищаемому АРМ;
- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АРМ;
- отклонениях в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения;
- некорректного функционирования установленных на АРМ средств защиты;
- обнаружения непредусмотренных отводов кабелей и подключенных к АРМ дополнительных устройств;
- обнаружении фактов и попыток НСД;
- нарушения установленного порядка обработки защищаемой информации.

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

2.10. Обо всех выявленных нарушениях, связанных с информационной безопасностью Учреждения, а также для получения консультаций по вопросам информационной безопасности, необходимо обратиться к АБИ.

2.11. Пользователям **запрещается:**

- разглашать защищаемую информацию посторонним лицам;
- копировать защищаемую информацию на неучтенные внешние носители;
- самостоятельно устанавливать, тиражировать или модифицировать программное и аппаратное обеспечение, изменять установленный порядок функционирования технических и программных средств;
- производить перемещение технических средств АРМ без согласования с АБИ;
- вскрывать корпуса технических средств АРМ и вносить изменения в схему и конструкцию устройство, производить техническое обслуживание (ремонт) средств вычислительной техники без согласования с АБИ.
- подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства;
- отключать (блокировать) средства защиты информации;
- выполнять на АРМ работы, не предусмотренные технологическим процессом обработки информации;
- использовать компоненты программного и аппаратного обеспечения в неслужебных целях сообщать (или передавать) посторонним лицам параметры своей учетной записи (имя, персональный идентификатор (при его наличии) и пароль);
- оставлять без присмотра и передавать другим лицам персональный идентификатор;
- привлекать посторонних лиц для ремонта или настройки АРМ без согласования с ответственным за защиту информации;
- оставлять без присмотра свое АРМ, не активизировав блокировку доступа, или оставлять свое АРМ включенным по окончании работы;
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к нарушению безопасности информации.

3. Организация парольной защиты

3.1. Личные пароли доступа создаются пользователем самостоятельно или выдаются АБИ.

3.2. Полная плановая смена паролей проводится не реже одного раза в 4 месяца.

3.3. Правила формирования пароля:

- пароль должен состоять не менее чем из 8 символов;
- в пароле должны присутствовать символы из числа прописных и строчных букв английского алфавита от A до Z; десятичных цифр (от 0 до 9); символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %);
- запрещается использовать в качестве пароля имя учетной записи, простые пароли типа «123», «111», «qwerty» и им подобные, а также имена и

даты рождения пользователей ОИ и их родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно вычислить, основываясь на информации о пользователе;

- запрещается использовать в качестве пароля один и тот же повторяющийся символ, либо повторяющуюся комбинацию из нескольких символов;
- запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);
- запрещается выбирать пароли, которые уже использовались ранее.

3.4. Правила ввода пароля:

- ввод пароля должен осуществляться с учетом регистра, в котором он был задан;
- во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами.

3.5. Правила хранения пароля:

- запрещается записывать пароли на бумаге, в файле и других носителях информации, в том числе на предметах;
- запрещается сообщать другим пользователям личный пароль и/или регистрировать их в системе под своей учетной записью.

3.6. Лица, использующие паролирование, обязаны:

- четко знать и строго выполнять требования настоящей Инструкции и других руководящих документов по паролированию;
- своевременно сообщать АБИ об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

4. Ответственность

4.1. Пользователь несет персональную ответственность за:

- сохранность носителей информации и содержащейся на них информации (в рабочее время);
- соблюдение требований данной Инструкции, неправомерное использование информационных ресурсов организации и за все действия, совершенные от имени его учетной записи, если со стороны пользователя не было предпринято действий для предотвращения несанкционированного использования его учетной записи.

4.2. За разглашение информации ограниченного доступа и нарушение порядка работы со средствами обработки информации, работники могут быть привлечены к гражданской, уголовной, административной, дисциплинарной и иной предусмотренной законодательством Российской Федерации ответственности.

Приложение № 3
Утверждено
приказом ГБУЗ ТО «Госпиталь для ветеранов войн»
от «27» 02 2023 г. №57

Перечень должностей, ГБУЗ ТО «Госпиталь для ветеранов войн» допущенных к обработке персональных данных

№ п/п	Наименование должности
1	2
1.	*Заведующий структурным подразделением*
2.	*Врач-терапевт*
3.	*Врач-невролог*
4.	*Врач-эндокринолог*
5.	*Врач-ревматолог*
6.	*Врач-офтальмолог*
7.	*Врач-кардиолог*
8.	*Врач-реаниматолог*
9.	*Врач-методист*
10.	*Медицинская сестра*
11.	*Старшая медицинская сестра*
12.	*Главная медицинская сестра*
13.	*Врач-эпидемиолог*
14.	*Заместитель главного врача*
15.	*Врач-психиатр*
16.	*Врач лечебной физкультуры*
17.	*Регистратор*
18.	*Врач-стоматолог*
19.	*Зубной врач*
20.	*Врач-хирург*
21.	*Врач-уролог*
22.	*Врач-оториноларинголог*
23.	*Начальник отдела управления персоналом*
24.	*Начальник общего отдела*
25.	*Главный экономист*
26.	*Главный бухгалтер*
27.	*Рентгенлаборант*
28.	*Врач-рентгенолог*
29.	*Врач-стажер*
30.	*Фельдшер*
31.	*Психолог*
32.	*Медицинский статистик*
33.	*Заведующий терапевтическим отделением*
34.	*Заведующий поликлиникой*