

ГБУЗ КО «Городская поликлиника ГП «Город Кременки»

УТВЕРЖДАЮ

Главный врач ГБУЗ КО

«Городская поликлиника

ГП «Город Кременки»



Хохлова Н. А.

Положение

по защите персональных данных

Оглавление

1. Определения.	3
2. Сокращения.	3
3. Общие положения.	4
4. Раздел 1. Реализация мер защиты персональных данных.	6
4.1. Идентификация и аутентификация пользователей ИСПДн.	6
4.2. Управление доступом к ПДн.	7
4.3. Управление программным обеспечением ТС ИСПДн и СЗИ.	7
4.4. Защита машинных носителей ПДн.	7
4.5. Управление событиями информационной безопасности.	7
4.6. Антивирусная защита.	7
4.7. Контроль (анализ) защищенности ИСПДн.	8
4.8. Защита технических средств ИСПДн.	8
4.9. Управление конфигурацией ИСПДн и ПДн.	8
5. Раздел 2. Управление обработкой персональных данных.	9
6. Заключительные положения.	10
7. Лист ознакомлений.	11

1. Определения.

- 1.1 **Администратор безопасности** – пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) системы защиты информации информационной системы в соответствии с установленной ролью.
- 1.2 **Администратор системный** – пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) информационной системы в соответствии с установленной ролью.
- 1.3 **Внутренний пользователь** – пользователь информационной системы персональных данных, являющийся сотрудником организации, эксплуатирующей информационную систему персональных данных.
- 1.4 **Внешний пользователь** – пользователь информационной системы персональных данных, не являющийся сотрудником организации, эксплуатирующей информационную систему персональных данных.
- 1.5 **Компьютерный вирус** – компьютерная программа либо иная компьютерная информация, предназначенная для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации.
- 1.6 **Конфигурация ИСПДн и ее системы защиты информации** – состав и взаимосвязи (электрические, логические, программные, геометрические) составных частей ИСПДн и СЗИ.
- 1.7 **Пользователь** – лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в информационной системе или использующее результаты ее функционирования.
- 1.8 **Событие информационной безопасности** – идентифицированное возникновение состояния информационной системы (сегмента, компонента информационной системы), сервиса или сети, указывающее на возможное нарушение безопасности информации, или сбой средств защиты информации, или ранее неизвестную ситуацию, которая может быть значимой для безопасности информации.
- 1.9 **Ответственный за организацию обработки персональных данных** – руководитель Организации, организующий и контролирующий выполнение требований регламентных документов, определяющих политику Организации в области обработки персональных данных, в том числе требований по защите персональных данных.

2. Сокращения.

- 2.1 **ИСПДн** – информационная система персональных данных.
- 2.2 **ОРД** – организационно – распорядительная документация.
- 2.3 **ПДн** – персональные данные.
- 2.4 **СЗИ** – средства защиты информации.
- 2.5 **ТС** – технические средства.

3. Общие положения.

- 3.1 Настоящее Положение по защите персональных данных (далее ПДн) разработано в соответствии со следующими нормативными правовыми актами и документацией на ИСПДн и ее систему защиты информации:
 - 3.1.1 Федеральный закон от 27.07.2006 года № 149 – ФЗ «Об информации, информационных технологиях и защите информации».
 - 3.1.2 Федеральный закон от 27.07.2006 года № 152 – ФЗ «О персональных данных».
 - 3.1.3 Приказ ФСТЭК России от 18.02.2013 года №21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
 - 3.1.4 Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
 - 3.1.5 Постановление правительства РФ от 21.03.2012 №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».
 - 3.1.6 Нормативно – технический документ «Специальные требования и рекомендации по технической защите конфиденциальной информации» (СТР-К) (Утвержден приказом Гостехкомиссии России №282 от 30.08.2002).
 - 3.1.7 Организационно-распорядительная документация на ИСПДн.
- 3.2 В настоящее Положение включены организационные меры, указанные в Приказе ФСТЭК №21, для организации защиты персональных данных, обрабатываемых в ИСПДн по **3 уровню** защищенности.

- 3.3 Настоящее Положение определяет порядок действий сотрудников Организации и внешних пользователей при защите **персональных данных**, содержащихся в ИСПДн.
- 3.4 Необходимый в соответствии с Постановлением правительства РФ №211 перечень персональных данных, обрабатываемых в ИСПДн, утверждает руководитель ГБУЗ КО «Городская поликлиника ГП «Город Кременки» (далее – Организация) по форме документа «Списки и перечни (формы)».
- 3.5 Настоящее Положение вступает в силу после его утверждения руководителем Организации и действует бессрочно, до момента его замены новым.
- 3.6 Все пользователи ИСПДн, должны быть ознакомлены с настоящим Положением под роспись.
- 3.7 Для организации обработки персональных данных в ИСПДн, на основании Постановления правительства РФ №211, руководитель Организации приказом назначает должностное лицо Организации **ответственным за организацию обработки ПДн** (далее – **ответственный по ПДн**). Форма приказа о назначении ответственного по ПДн приведена в документе «Приказы (формы)». При выполнении своих обязанностей ответственный по ПДн действует в соответствии с требованиями документа «Руководство ответственного за организацию обработки персональных данных», содержащего должностные обязанности ответственного по ПДн.
- 3.8 Для непосредственного выполнения работ с программно-аппаратными средствами защиты персональных данных (далее СЗИ), а так же для сопровождения и контроля работы пользователей ИСПДн, руководитель Организации (в соответствии с требованиями Постановления правительства РФ №1119 п.14) назначает должностное лицо Организации **ответственным за обеспечение безопасности персональных данных, обрабатываемых в ИСПДн** (далее - **администратор безопасности**). Форма приказа о назначении администратора безопасности приведена в документе «Приказы (формы)» (Форма 2). При выполнении своих обязанностей по обеспечению безопасности ПДн, обрабатываемых в ИСПДн, администратор безопасности действует в соответствии с требованиями «Руководство администратора безопасности» и требованиями эксплуатационной документации на СЗИ.
- 3.9 Все пользователи информационной системы персональных данных участвуют в защите ПДн и обязаны знать и выполнять требования:
- 3.9.1 нормативно – правовых документов по защите ПДн;

- 3.9.2 настоящего Положения и перечисленных в нем инструкций, в части их касающейся;
- 3.9.3 «Руководства пользователя ИСПДн» 48357148.7492070.@002.ИЗ.01.
- 3.10 В соответствии с требованиями п.8 Приказа ФСТЭК №21 защита ПДн по 3 уровню защищенности в ходе эксплуатации ИСПДн осуществляется реализацией мер защиты:
- 3.10.1 идентификация и аутентификация пользователей ИСПДн;
 - 3.10.2 управление доступом к ПДн;
 - 3.10.3 управление программным обеспечением ТС ИСПДн и СЗИ;
 - 3.10.4 защита машинных носителей ПДн;
 - 3.10.5 управление событиями информационной безопасности;
 - 3.10.6 антивирусная защита;
 - 3.10.7 контроль (анализ) защищенности ПДн;
 - 3.10.8 защита технических средств ИСПДн;
 - 3.10.9 управление конфигурацией ИСПДн и ПДн.
- 3.11 В соответствии с требованиями Постановления правительства РФ №211 организация защиты ПДн, требует документирования и утверждения руководителем Организации локальных актов, определяющих политику в отношении обработки персональных данных. В настоящем Положении политика в отношении обработки ПДн определена:
- 3.11.1 правилами обработки ПДн;
 - 3.11.2 правилами рассмотрения запросов субъектов ПДн;
 - 3.11.3 правилами осуществления внутреннего контроля соответствия обработки ПДн требованиям к их защите;
 - 3.11.4 правилами работы с обезличенными ПДн;
 - 3.11.5 рабочими документами по организации обработки ПДн.

4. Раздел 1. Реализация мер защиты персональных данных.

4.1 Идентификация и аутентификация пользователей ИСПДн.

- 4.1.1 Порядок действий пользователей ИСПДн при прохождении процедур идентификации (узнавании) и аутентификации (подтверждении подлинности узанного пользователя) при входе в ИСПДн описаны в «Инструкции по идентификации и аутентификации пользователей информационной системы персональных данных».

- 4.1.2 Выполнение требований инструкции в части его касающейся и контроль соблюдения пользователями требований инструкции обеспечивает администратор безопасности.

4.2 Управление доступом к ПДн.

- 4.2.1 Порядок управления доступом пользователей к информационным ресурсам ИСПДн описан в «Инструкции по управлению доступом к персональным данным».
- 4.2.2 Выполнение требований инструкции в части его касающейся и контроль соблюдения пользователями требований инструкции обеспечивает администратор безопасности.

4.3 Управление программным обеспечением ТС ИСПДн и СЗИ.

- 4.3.1 Порядок действий пользователей ИСПДн при реализации ограничений в применении программного обеспечения, установки разрешенного программного обеспечения, его настройки и обновления, описаны в «Инструкции по управлению программным обеспечением».
- 4.3.2 Выполнение требований инструкции обеспечивает администратор безопасности.

4.4 Защита машинных носителей ПДн.

- 4.4.1 Порядок действий пользователей ИСПДн при работе с машинными носителями информации, правила учета, хранения и доступа к машинным носителям и к ПДн, содержащихся на машинных носителях описаны в «Инструкции по защите машинных носителей персональных данных».
- 4.4.2 Выполнение требований инструкции обеспечивает администратор безопасности.

4.5 Управление событиями информационной безопасности.

- 4.5.1 Порядок действий пользователей ИСПДн при появлении событий безопасности описаны в «Инструкции по управлению событиями информационной безопасности».
- 4.5.2 Выполнение требований инструкции обеспечивает администратор безопасности.

4.6 Антивирусная защита.

4.6.1 Порядок действий пользователей при обнаружении в ИСПДн компьютерных вирусов, описаны в «Инструкции по антивирусной защите».

4.6.2 Выполнение требований инструкции обеспечивает администратор безопасности.

4.7 Контроль (анализ) защищенности ИСПДн.

4.7.1 Порядок действий ответственных пользователей и администратора безопасности с целью;

4.7.1.1 выявления ошибок и недостатков программного обеспечения и аппаратных средств ИСПДн и СЗИ;

4.7.1.2 контроля установки обновлений программного обеспечения, контроля работоспособности и настроек программного обеспечения;

4.7.1.3 контроля состава технических средств ИСПДн и системы защиты информации;

4.7.1.4 контроля правил работы с паролями и учетными записями.

описан в «Инструкции по контролю защищенности персональных данных».

4.7.2 Выполнение требований инструкции в части его касающейся и контроль соблюдения ответственными пользователями требований инструкции обеспечивает администратор безопасности.

4.8 Защита технических средств ИСПДн.

4.8.1 Порядок доступа пользователей к техническим средствам ИСПДн и СЗИ, описаны в «Инструкции по защите технических средств информационной системы персональных данных».

4.8.2 Выполнение требований инструкции в части его касающейся и контроль соблюдения пользователями требований инструкции обеспечивает администратор безопасности.

4.9 Управление конфигурацией ИСПДн и ПДн.

4.9.1 Порядок управления конфигурацией ИСПДн и ПДн описан в «Инструкции по управлению конфигурацией».

4.9.2 Выполнение требований инструкции в части его касающейся и контроль соблюдения пользователями требований инструкции обеспечивает ответственный по ПДн.

5. Раздел 2. Управление обработкой персональных данных.

5.1 Правила обработки ПДн.

5.1.1 Порядок действий пользователей ИСПДн при организации обработки персональных данных, содержащихся в ИСПДн, приведен в документе «Правила обработки персональных данных».

5.1.2 Контроль выполнения требований документа осуществляет ответственный по ПДн.

5.2 Правила рассмотрения запросов субъектов ПДн.

5.2.1 Порядок действий пользователей ИСПДн при организации рассмотрения запросов субъектов персональных данных, содержащихся в ИСПДн, приведен в документе «Правила рассмотрения запросов субъектов персональных данных».

5.2.2 Контроль выполнения требований документа осуществляет ответственный по ПДн.

5.3 Правила осуществления внутреннего контроля обработки ПДн.

5.3.1 Порядок действий пользователей ИСПДн при осуществлении внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, содержащихся в ИСПДн, приведен в документе «Правила осуществления внутреннего контроля обработки персональных данных».

5.3.2 Контроль выполнения требований документа осуществляет ответственный по ПДн.

5.4 Правила работы с обезличенными ПДн.

5.4.1 Порядок действий пользователей ИСПДн при работе с обезличенными персональными данными, содержащимися в ИСПДн, приведен в документе «Правила работы с обезличенными персональными данными».

5.4.2 Контроль выполнения требований документа осуществляет ответственный по ПДн.

5.5 Рабочие документы по организации обработки ПДн.

5.5.1 Рабочие документы предназначены для организации рабочего процесса обработки персональных данных.

5.5.2 К рабочим документам в Организации отнесены:

- 5.5.2.1 Перечень ПДн, обрабатываемых в ИСПДн по форме «Списки и перечни (формы)» Форма 1.
- 5.5.2.2 Перечень должностей и сотрудников, ответственных за обезличивание ПДн, обрабатываемых в ИСПДн по форме «Списки и перечни (формы)» Форма 2.
- 5.5.2.3 Типовое обязательство обработчика ПДн по форме «Типовые административные документы (формы)» Форма 1.
- 5.5.2.4 Типовое согласие на обработку ПДн по форме «Типовые административные документы (формы)» Форма 2.
- 5.5.2.5 Типовое разъяснение на отказ в обработке ПДн по форме «Типовые административные документы (формы)» Форма 3.

6. Заключительные положения.

- 6.1 Пользователи ИСПДн должны быть предупреждены об ответственности за действия с информацией, содержащейся в ИСПДн и действия с техническими средствами ИСПДн и СЗИ, нарушающие требования настоящего Положения.
- 6.2 Пользователи ИСПДн должны быть ознакомлены в части их касающейся, с настоящим Положением до начала работы с ИСПДн под роспись. Обязанность ознакомления сотрудников Организации с настоящим Положением лежит на ответственном по ПДн.