"УТВЕРЖДАЮ"

Главный врач

ГБУ РО "Онкодиспансер" в г. Таганроге

_____Г.Н. Беседовская

«09» января 2014 г.

Регламент обработки и защиты персональных данных в информационных системах ГБУ РО «Онкодиспансер» в г. Таганроге

г. Таганрог

2014 г.

Содержание

Сокращения, условные обозначения, термины **3**

Введение **4**

1. Цель и область применения **5**

2. Должностные лица и их обязанности **6**

3. Порядок обработки ПДн **8**

3.1. Определение ПДн, обрабатываемых в ИСПДн ГБУ РО «Онкодиспансер» в г. Таганроге 8
3.2. Определение ИС, участвующих в хранении и обработке ПДн 8
3.3. Получение ПДн и внесение в ИСПДн 9
3.4. Хранение ПДн 10
3.5. Предоставление доступа к ПДн 11
3.6. Режим обработки ПДн 12
3.7. Передача ПДн 12
3.9. Прекращение обработки и уничтожение ПДн 14

4. Порядок защиты ПДн **16**

4.1. Управление доступом 16
4.2. Контроль обработки ПДн 16
4.3. Аудит ИСПДн 17
4.4. Регламент защиты от вредоносного ПО 18
4.6. Резервное копирование и восстановление ПДн и ИС 19
4.7. Регламентное обслуживание ИСПДн 20
4.8. Анализ защищенности ИСПДн 21
4.9. Действия при внештатных ситуациях 22

5. Порядок изменения регламента **24**

Лист изменений **26**

Приложение 1 ..... **27**

Приложение 2 ..... **28**

Приложение 3 ..... **30**

Приложение 4 ..... **31**

Приложение 5 ..... **32**

СОКРАЩЕНИЯ, УСЛОВНЫЕ ОБОЗНАЧЕНИЯ, ТЕРМИНЫ

АРМ – Автоматизированное рабочее место

БД – База данных

ИС – Информационные системы

ИСПДн – Информационные системы персональных данных

ЛВС – Локальная вычислительная сеть

НСД – Несанкционированный доступ

ОС – Операционная система

ПДн – Персональные данные

ПО – Программное обеспечение

СЗПДн – Система защиты персональных данных

СУБД – Система управления базами данных

ФСТЭК – Федеральная служба по техническому и экспортному контролю

ФОМС – Федеральный фонд обязательного медицинского страхования

ФСБ – Федеральная служба безопасности

ВВЕДЕНИЕ

Настоящий Регламент определяет общие правила по обработке и защите ПДн при их хранении и обработке в ИСПДн ГБУ РО «Онкодиспансер» в г. Таганроге, а также порядок их реализации и контроля эффективности.

Положения и требования Регламента распространяются на все структурные подразделения ГБУ РО «Онкодиспансер» в г. Таганроге, эксплуатирующие технические и программные средства, в которых осуществляется обработка ПДн, а также на подразделения, осуществляющие сопровождение, обслуживание и обеспечение нормального функционирования ИСПДн.

Данный Регламент разработан в соответствии со следующими нормативными документами:

- «Политика обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных ГБУ РО «Онкодиспансер» в г. Таганроге»;
- «Положение о порядке организации и проведения работ по защите персональных данных в информационных системах персональных данных ГБУ РО «Онкодиспансер» в г. Таганроге»;
- Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных. Утверждены заместителем директора ФСТЭК России 15 февраля 2008 г.;
- Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены заместителем директора ФСТЭК России 15 февраля 2008 г.;
- «Специальные требования и рекомендации по технической защите конфиденциальной информации», решение Коллегии Гостехкомиссии России № 7.2/02.03.01 г.;

1. ЦЕЛЬ И ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1. Цель Регламента – определение состава и порядка проведения работ по обработке и защите персональных данных в ГБУ РО «Онкодиспансер» в г. Таганроге в целях предотвращения ущерба в результате разглашения, утраты, утечки, искажения и уничтожения персональных данных, их незаконного использования и нарушения работы информационно-телекоммуникационной системы ГБУ РО «Онкодиспансер» в г. Таганроге.

1.2. Требования настоящего Регламента обязательны для всех структурных подразделений ГБУ РО «Онкодиспансер» в г. Таганроге и распространяются на всех сотрудников, участвующих в обработке и защите ПДн и несущих ответственность за обеспечение безопасности ПДн.

1.3. Внутренние документы ГБУ РО «Онкодиспансер» в г. Таганроге, затрагивающие вопросы, рассматриваемые в данном документе, должны разрабатываться с учетом положений Регламента и не противоречить им.

2. ДОЛЖНОСТНЫЕ ЛИЦА И ИХ ОБЯЗАННОСТИ

Пользователи ИСПДн делятся на две категории: обслуживающие систему и работающие в системе.

В категорию пользователей, обслуживающих ИСПДн, входят сотрудники, которые занимаются настройкой, внедрением и сопровождением ИСПДн, и обладают следующими полномочиями:

- системные администраторы – сотрудники, обеспечивающие функционирование ИС, входящих в ИСПДн или связанных с ней в рамках обеспечения функционирования ИСПДн;
- сетевые администраторы – сотрудники, обеспечивающие управление сетевым оборудованием, участвующим в передаче ПДн и обеспечении функционирования ИСПДн;
- администраторы информационной безопасности – сотрудники, обеспечивающие функционирование, управление и мониторинг средств защиты информации, осуществляющие координацию взаимодействия с системными и сетевыми администраторами по вопросам обеспечения защиты информации.

Вторая категория (пользователи ИСПДн) включает в себя пользователей, которые являются сотрудниками подразделений ГБУ РО «Онкодиспансер» в г. Таганроге, участвующих в процессах обработки ПДн:

- сотрудники, участвующие в обработке данных застрахованных лиц;
- сотрудники, участвующие в ведении кадрового учета ГБУ РО «Онкодиспансер» в г. Таганроге и обрабатывающие данные сотрудников ГБУ РО «Онкодиспансер» в г. Таганроге;
- сотрудники, участвующие в ведении бухгалтерского учета ГБУ РО «Онкодиспансер» в г. Таганроге и обрабатывающие данные сотрудников ГБУ РО «Онкодиспансер» в г. Таганроге.

2.1. На системных администраторов возлагаются следующие обязанности:

- установка, настройка и администрирование ИС и общесистемного ПО для ИСПДн;
- создание ЛВС, участвующей в обработке ПДн;
- регламентное обслуживание ИСПДн;
- резервное копирование и восстановление конфигурации ИС и информационного обеспечения ИСПДн;
- обнаружение нарушений работоспособности ИСПДн и их устранение;
- участие в расследовании инцидентов ИБ и ликвидации их последствий.

2.2. На администраторов информационной безопасности возлагаются следующие обязанности:

- настройка и администрирование подсистем СЗПДн;
- управление и контроль доступа к ПДн;
- контроль соблюдения режима обработки ПДн;
- учет обрабатываемых ПДн, носителей информации, содержащих ПДн и передачи ПДн;
- обеспечение защищенного хранения ПДн;
- уничтожение ПДн;
- регламентное обслуживание СЗПДн;
- аудит ИСПДн;
- контроль целостности ПДн и среды обработки ПДн;
- анализ защищенности ИСПДн;
- обнаружение и устранение угроз ИБ;
- обнаружение инцидентов ИБ;
- расследование инцидентов ИБ и ликвидация и последствий;
- резервное копирование и восстановление ПДн, журналов аудита, информационного обеспечения СЗПДн;

2.3. На пользователей ИСПДн возлагаются следующие обязанности:

- соблюдение должностных инструкций и инструкций по работе в ИСПДн;
- соблюдение режима обработки ПДн;
- контроль вводимых данных при обработке ПДн;
- защита ПДн от НСД и нарушения целостности;
- обеспечение безопасности доверенных носителей информации, содержащих ПДн;
- информирование администраторов информационной безопасности о замеченных инцидентах информационной безопасности;
- содействие в расследованиях инцидентов информационной безопасности.

3. ПОРЯДОК ОБРАБОТКИ ПДН

3.1. Определение ПДн, обрабатываемых в ИСПДн ГБУ РО «Онкодиспансер» в г. Таганроге

Исходя из деятельности ГБУ РО «Онкодиспансер» в г. Таганроге, определяются процессы, требующие обработки ПДн.

Необходимо определить требования законодательных актов, предоставляющих обоснование необходимости ведения данной деятельности. Исходя из положений данных законодательных актов и регламентов деятельности ГБУ РО «Онкодиспансер» в г. Таганроге, составляется обоснование необходимости и цель обработки ПДн.

Определяется перечень ПДн, которые необходимо хранить и обрабатывать для осуществления деятельности ГБУ РО «Онкодиспансер» в г. Таганроге.

Определяется перечень субъектов обрабатываемых ПДн.

Определяется перечень операций, выполняемых в рамках обработки ПДн.

Определяется срок и условия хранения и обработки ПДн, а также условия прекращения обработки ПДн.

Необходимо определить ИСПДн, в которых обрабатываются ПДн. Выделение ИСПДн осуществляется в соответствии с определенными на первом этапе процессами, в рамках которых обрабатываются наборы ПДн. Каждая ИСПДн должна включать набор ПДн, необходимый в рамках одного вида деятельности и требующие единого режима обработки.

Для каждой ИСПДн составляется перечень ПДн, обрабатываемых в ГБУ РО «Онкодиспансер» в г. Таганроге. Перечень ПДн содержит:

- список ПДн, обрабатываемых в ИСПДн;
- субъекты ПДн;
- объем обрабатываемых ПДн;
- набор операций, выполняемых в рамках обработки ПДн;
- срок и условия хранения ПДн;
- обоснование обработки ПДн.

3.2. Определение ИС, участвующих в хранении и обработке ПДн

Необходимо определить способ обработки ПДн, вид хранения и вид носителей информации, участвующих в хранении и обработке ПДн.

Необходимо определить ИС, участвующие в обработке ПДн. Для каждой ИС определяется вид и способ хранения и обработки ПДн.

Необходимо определить способы и каналы передачи ПДн в рамках ИСПДн и за её пределы.

Для каждой ИСПДн составляется функциональная схема с указанием:

- состава функциональных узлов (сетевое оборудование, АРМы, базы данных, носители, серверы или ИС);
- каналов взаимодействия функциональных узлов;
- потоков ПДн в рамках функционирования ИСПДн.

3.3. Получение ПДн и внесение в ИСПДн

Персональные данные поступают в ИСПДн непосредственно от субъекта персональных данных или иного оператора ПДн.

В случае передачи ПДн непосредственно субъектом ПДн, решение о предоставлении ПДн принимает непосредственно субъект ПДн и дает согласие на их обработку своей волей и в своем интересе. Обработка ПДн осуществляется только с согласия в письменной форме (Приложение 1) субъекта персональных данных. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. При получении персональных данных необходимо сообщить субъекту персональных данных о целях и способах их обработки.

В случае передачи ПДн иным оператором ПДн, их передача и обработка осуществляется в рамках заключаемого договора (в данном случае оператор, передающий ПДн, несет ответственность за получение согласия на обработку и передачу ПДн у субъектов ПДн).

Передача ПДн в ГБУ РО «Онкодиспансер» в г. Таганроге осуществляется в соответствии с установленной процедурой занесения ПДн в ИСПДн.

В случае передачи ПДн непосредственно субъектом ПДн, регистрация и внесение данных осуществляется сотрудниками, ответственными за ведение кадрового учета ГБУ РО «Онкодиспансер» в г. Таганроге, в соответствии с порядком ведения личных дел сотрудников ГБУ РО «Онкодиспансер» в г. Таганроге и должностными инструкциями.

В случае передачи ПДн иными операторами ПДн, занесение данных в ИСПДн осуществляется сотрудниками, ответственными за обработку данных застрахованных лиц и осуществляется в соответствии с должностными инструкциями сотрудников и частными инструкциями по работе в ИСПДн.

При внесении ПДн в ИСПДн должна осуществляться проверка корректности и точности вводимых данных. В случае неавтоматизированного ввода проверка осуществляется сотрудником, осуществляющим ввод посредством непосредственной сверки вводимых данных. В случае использования автоматизированной загрузки данных должны использоваться средства контроля целостности данных.

Регистрируются факты занесения ПДн в ИСПДн. При регистрации указываются сведения о занесенных данных (ИСПДн, в которую были занесены данные, источник ПДн, тип ПДн, объем записей, время занесения, сотрудник, осуществивший занесение ПДн).

3.4. Хранение ПДн

Хранение ПДн осуществляется на определенных носителях в соответствии с требованиями по обеспечению безопасности ПДн.

Носители информации, содержащей ПДн, должны быть классифицированы и промаркированы с помощью легко-читаемых идентификаторов, содержащих следующую информацию:

- персональный идентификатор носителя;
- тип содержащейся информации;
- срок хранения и обработки ПДн;
- контактные данные или сведения о сотруднике или подразделении, ответственном за учет данного носителя.

Защиту носителей информации осуществляют сотрудники, которые в текущий момент являются ответственными за данные носители, в соответствии с требованиями обеспечения безопасности ПДн, «Положением о порядке организации и проведения работ по защите ПДн», должностными инструкциями, руководствами по работе в ИСПДн и должностными инструкциями. Ответственность за носители, входящие в состав ИС несут администраторы данных ИС. Ответственность за носители, выданные сотрудникам, несут данные сотрудники.

Хранение носителей информации, содержащей ПДн должно осуществляться в соответствии с требованиями по обеспечению безопасности ПДн, в защищенном месте или под контролем ответственных лиц.

ПДн должны храниться в соответствии со сроками и условиями хранения, определенными для конкретных ПДн в соответствии с необходимостью их обработки в ГБУ РО «Онкодиспансер» в г. Таганроге.

В том случае, если для научных, прикладных исследований, для решения задач статистики необходимо сохранить персональные данные, которые больше не используются в тех целях, ради которых они были собраны, эти данные могут сохраняться преимущественно только в обезличенной форме в виде анонимных сведений.

3.5. Предоставление доступа к ПДн

Первоначальные права доступа сотрудников ГБУ РО «Онкодиспансер» в г. Таганроге к ПДн назначаются в соответствии с их должностными обязанностями. Предоставляемый

доступ должен отвечать требованиям минимальной достаточности – назначаются только те права доступа, которые необходимы для осуществления функциональных обязанностей.

Запрещается предоставление доступа к ПДн третьим лицам.

Доступ к ПДн осуществляется в соответствии с заявками на предоставление/изменение доступа (Приложение 2). Заявки утверждаются главный врачом ГБУ РО «Онкодиспансер» в г. Таганроге. Заявка передается на обработку сотруднику, ответственному за предоставление/изменение прав доступа к ПДн.

Сотрудники, которым предоставляются права доступа к ПДн, в обязательном порядке ознакомляются под роспись с инструкциями по обеспечению безопасности ПДн и работе в ИС.

Доступ к ПДн предоставляется с использованием подсистемы управления доступа в ИСПДн. Изменение прав доступа осуществляется в соответствии с инструкцией администратора подсистемы управления доступом. Ответственным за назначение или изменение прав доступа являются администраторы информационной безопасности.

В случае предоставления доступа к носителям информации, сотрудник в обязательном порядке ознакомляется с правилами работы с носителями информации, содержащими информацию, составляющую ПДн и фиксируется передача носителей информации под роспись в журнале учета носителей (Приложение 3).

В случае предоставления сотрудникам прав доступа к помещениям, в которых размещается оборудование, участвующее в обработке ПДн, или носители, содержащие ПДн, фиксируется допуск сотрудника в эти помещения и сотрудник под роспись ознакомляется с правилами работы в помещениях, содержащих оборудование, участвующее в обработке ПДн, или носители информации, содержащие ПДн.

По осуществлению изменения прав доступа, изменения регистрируется в матрице доступа и заявка закрывается. Сотрудник, предоставивший/изменивший права доступа в соответствии с заявкой, информирует сотрудника, подавшего заявку.

Факт изменения прав доступа фиксируется в подсистеме регистрации и учета.

3.6. Режим обработки ПДн

Персональные данные обрабатываются на основе принципов, установленных действующим законодательством о персональных данных.

К обработке ПДн допускаются сотрудники ГБУ РО «Онкодиспансер» в г. Таганроге, которые имеют права доступа к ПДн в соответствии со своими должностными обязанностями и выполняемыми функциями.

Обработка ПДн осуществляется в соответствии с должностными инструкциями сотрудников, инструкциями по работе в ИС, в которых производится хранение и обработка ПДн, и в соответствии с частными регламентами обработки ПДн.

Факты обработки ПДн фиксируются подсистемой регистрации и учета.

Обработка ПДн осуществляется в пределах защищаемой территории, в помещениях, предназначенных для обработки ПДн.

При обработке ПДн должна обеспечиваться целостность ПДн. Сотрудникам запрещается изменять ПДн, за исключением операций по изменению ПДн, описанных в должностных инструкциях и частных инструкциях по выполнению операций.

Запись ПДн на отчуждаемые носители информации (цифровые и аналоговые) осуществляется назначенными ответственными сотрудниками и фиксируется в журнале учета носителей.

3.7. Передача ПДн

Передача ПДн осуществляется на основе принципов, установленных действующим законодательством о персональных данных.

Допускается передача ПДн:

- субъектам ПДн или их законным представителям;
- сотрудникам, имеющим доступ к данным ПДн и которым они необходимы в рамках должностных обязанностей;
- ФОМС, передача ПДн которым осуществляется в соответствии с регламентом информационного взаимодействия и необходима для осуществления деятельности ФОМС и ГБУ РО «Онкодиспансер» в г. Таганроге;
- операторам ПДн, которые предоставили данные ПДн в рамках существующих договоров;
- организациям, передача ПДн которым осуществляется в рамках существующих договоров о взаимодействии и предоставлении услуг и необходима в рамках выполнения положений данных договоров, в том случае если получено разрешение субъектов ПДн на данную передачу;
- третьим организациям и лицам, в соответствии с положениями Федерального закона РФ от 27 июля 2006 г. N 152-ФЗ О персональных данных или иных законодательных актов РФ.

Передача ПДн осуществляется в соответствии с заявками на передачу ПДн (Приложение 4). В том случае, если передача ПДн осуществляется в соответствии с регламентированной деятельностью ГБУ РО «Онкодиспансер» в г. Таганроге, используется

общая заявка, описывающая сроки выполнения обмена данными и процесс, в рамках которого осуществляется передача.

Передача ПДн осуществляется ответственными сотрудниками в соответствии с должностными инструкциями, правилами работы в ИСПДн и частными регламентами передачи ИСПДн.

Передача ПДн возможна с помощью передачи носителей информации или с использованием каналов передачи данных.

Передача носителей информации осуществляется только с использованием зарегистрированных носителей информации, предназначенных для записи ПДн в соответствии с процедурами записи и учета носителей информации. Передача носителей осуществляется или лично или с использованием курьерской службы, обеспечивающей необходимые требования по защите ПДн.

Факты передачи фиксируются в журнале учета передачи ПДн. При регистрации фактов передачи ПДн указывается следующая информация:

- сведения о передаваемой информации: перечень ПДн, объем записей, ИСПДн, к которой относятся ПДн;
- данные о получателе;
- время передачи ПДн;
- обоснование необходимости передачи ПДн и в рамках каких действий по обработке ПДн или договоренностей передаются ПДн;
- сотрудник, осуществивший передачу;
- тип носителя (с идентификатором) или вид передачи информации.
- подтверждение о получении ПДн.

3.9. Прекращение обработки и уничтожение ПДн

Прекращение обработки ПДн в ИСПДн ГБУ РО «Онкодиспансер» в г. Таганроге возможно в случаях:

- истечения определенного срока хранения и обработки ПДн;
- достижения или утраты необходимости в достижении цели обработки ПДн;
- отзыва субъектом ПДн согласия на обработку своих ПДн;
- истечения срока или прекращения действия договора со сторонними организациями, в соответствии с которым осуществляется обработка и хранение ПДн;
- выявления недостоверных ПДн или неправомерных действий с ними;

В случае достижения цели обработки ПДн ГБУ РО «Онкодиспансер» в г. Таганроге, незамедлительно прекращает обработку ПДн и уничтожает соответствующие ПДн в срок, не превышающий трех рабочих дней с даты достижения цели обработки ПДн, если иное не предусмотрено федеральными законами, и уведомляет об этом субъекта ПДн или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов ПДн, - также указанный орган.

В случае отзыва субъектом ПДн согласия на обработку своих ПДн оператор обязан прекратить обработку ПДн и уничтожить их в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между ГБУ РО «Онкодиспансер» в г. Таганроге и субъектом ПДн, уведомив об этом субъекта ПДн.

В случае выявления недостоверных ПДн или неправомерных действий с ними, блокируется использование ПДн, относящихся к соответствующему субъекту, с момента такого обращения, производится их уточнение на основании документов, представленных субъектом ПДн или его законным представителем либо уполномоченным органом по защите прав субъектов ПДн, после чего проводится разблокирование указанных данных.

В случае выявления неправомерных действий с ПДн, ГБУ РО «Онкодиспансер» в г. Таганроге в срок, не превышающий трех рабочих дней с даты такого выявления, устраняет допущенные нарушения. В случае невозможности устранения допущенных нарушений ГБУ РО «Онкодиспансер» в г. Таганроге в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с ПДн, проводит уничтожение персональных данных.

В случае истечения срока или прекращения действия договора со сторонними организациями, в соответствии с которым осуществляется обработка и хранение ПДн, прекращение обработки и уничтожение ПДн осуществляется в соответствии с положениями соответствующего договора.

Уничтожение ПДн осуществляется в соответствии с приказом на уничтожение ПДн (Приложение 5).

Уничтожение ПДн осуществляется ответственными сотрудниками в соответствии с должностными инструкциями, частными регламентами уничтожения информации и инструкциями пользователей ИС (в том случае, если они используются для уничтожения ПДн).

Уничтожение ПДн осуществляется следующими способами:

- физическое уничтожение бумажных или иных твердых носителей информации, предполагающих разовое использование;
- электронное уничтожение информации, хранимой на цифровых устройствах постоянного хранения информации.

Факты уничтожения ПДн протоколируются с указанием сотрудников, осуществивших уничтожение, перечня удаленных данных, причины удаления, даты удаления.

4. ПОРЯДОК ЗАЩИТЫ ПДН

4.1. Управление доступом

Управление доступом осуществляется ответственными сотрудниками с помощью подсистемы управления доступом в соответствии с порядком предоставления/изменения доступа, должностными инструкциями и частными инструкциями администратора подсистемы управления доступом.

Должна осуществляться ежемесячная проверка имеющихся прав доступа сотрудников к ПДн. Проверка осуществляется с помощью сверки текущих прав доступа, определенных в подсистеме управления доступом и имеющейся матрицы доступа. В случае обнаружения несоответствий, проводится уточнение реальных прав доступа (по заявкам на предоставление прав доступа), исправление несоответствий и начинается расследование инцидента ИБ в целях определения этапа, на котором было совершено нарушение и сотрудника, несущего ответственность за нарушение.

4.2. Контроль обработки ПДн

Контроль обработки ПДн осуществляется ответственными сотрудниками с помощью подсистемы регистрации и учета в соответствии с должностными инструкциями и частными инструкциями работы в подсистеме регистрации и учета.

В рамках контроля обработки ПДн осуществляется регистрация следующих событий в ИСПДн:

- занесение ПДн в ИСПДн;
- предоставление/изменение прав доступа к ПДн;
- события обработки ПДн (чтение, изменение, поиск, обработка в специальном ПО);
- запись ПДн на отчуждаемые носители информации;
- перевод ПДн в иные формы хранения и обработки (печать, занесение в БД или ПО);
- передача ПДн;
- выдача и прием отчуждаемых носителей информации сотрудникам;
- прекращение обработки и уничтожение ПДн;
- попытки несанкционированного доступа к ПДн или осуществления несанкционированных действий в ИСПДн;
- инциденты, связанные с нарушением целостности ПДн и среды их обработки.

Подсистема регистрации и учета должна автоматически осуществлять регистрацию попыток несанкционированной деятельности в ИСПДн и сообщать об этом ответственного

сотрудника с помощью системы мгновенного уведомления (электронная почта, sms-служба или иные системы мгновенных сообщений.)

Сотрудник, ответственный за контроль обработки ПДн, должен осуществлять непрерывный мониторинг оповещений об инцидентах безопасности в ИСПДн.

Сотрудник, ответственный за контроль обработки ПДн, должен выполнять ежедневный аудит регистрирующихся событий работы пользователей в ИСПДн.

Сотрудник, ответственный за контроль обработки ПДн, должен ежемесячно осуществлять проверку факта хранения и обработки в ИСПДн только тех ПДн, которые указаны в Перечне ПДн и хранение которых обосновано и регламентировано. В рамках проверки также осуществляется проверка сроков хранимой и обрабатываемой информации и в случае обнаружения наступления события, обуславливающего прекращение обработки ПДн и их уничтожения, должен быть инициирован соответствующий процесс.

Сотрудник, ответственный за контроль обработки ПДн, должен ежемесячно осуществлять инвентаризацию носителей информации, содержащих ПДн в соответствии с Перечнем носителей информации, содержащих ПДн.

Сотрудник, ответственный за контроль обработки ПДн, должен ежемесячно осуществлять проверку фактов уничтожения ПДн.

В случае возникновения инцидентов безопасности, осуществляется их регистрация и расследование в соответствии с порядком реагирования на инциденты ИБ в ИСПДн.

4.3. Аудит ИСПДн

Аудит ИСПДн осуществляется ответственными сотрудниками с помощью подсистемы регистрации и учета в соответствии с должностными инструкциями и частными инструкциями работы в подсистеме регистрации и учета.

Администратор информационной безопасности должен ежемесячно просматривать журналы работы подсистем обеспечения информационной безопасности в целях определения наиболее актуальных угроз, и их источников.

По результатам аудита составляется отчет, содержащий обобщенные сведения аудита, которые в дальнейшем анализируются в целях совершенствования СЗПДн.

4.4. Регламент защиты от вредоносного ПО

Ответственность за обеспечение защиты ИСПДн от воздействия вредоносного ПО несут администраторы информационной безопасности.

Защита от вредоносного ПО осуществляется с помощью автоматизированной системы антивирусной защиты.

В рамках защиты от вредоносного ПО осуществляется следующая деятельность:

– непрерывный мониторинг среды обработки ПДн на предмет выявления вредоносного ПО;
– регулярные сканирования ИС в целях выявления вредоносного ПО;
– сканирования по запросу;
– анализ обнаруженного ПО и принятие решения по его нейтрализации.

Непрерывный мониторинг среды обработки ПДн осуществляется в автоматическом режиме с помощью программных модулей антивирусной защиты, установленных в ИС.

Регулярные сканирования ИС осуществляются в автоматическом режиме в соответствии с графиком проведения и объемом сканирований, определенными в стандарте конфигурации средств антивирусной защиты. Стандартной считается еженедельная проверка, осуществляемая для всех постоянных запоминающих устройств в рамках узла ИСПДн.

Сканирования по запросу могут быть инициированы пользователями или администраторами подсистемы антивирусной защиты в случае подозрения на заражение или в целях разовой проверки съемного накопителя.

Определение вредоносного ПО осуществляется в автоматическом режиме средством антивирусной защиты. В случае обнаружения вредоносного ПО должны быть предприняты действия по его нейтрализации: лечение, удаление, перемещение в карантин (в порядке приоритета).

В случае невозможности осуществления всех приведенных действий по нейтрализации вредоносного ПО, а также в случае возникновения иных ситуаций, когда средство антивирусной защиты не в состоянии справиться с угрозой заражения, администратор информационной безопасности обязан предпринять меры по выявлению и ликвидации угрозы заражения в соответствии со своей компетенцией и с помощью использования дополнительных средств обнаружения и ликвидации вредоносного ПО. Данная процедура должна протоколироваться.

4.6. Резервное копирование и восстановление ПДн и ИС

Резервное копирование и восстановление ПДн и ИС осуществляется администраторами ИС и администраторами информационной безопасности в соответствии с должностными инструкциями и инструкцией администратора подсистемы резервного копирования и восстановления.

Осуществляется резервное копирование следующих данных:

– ПДн;
– конфигурационные файлы ИСПДн и СЗПДн;

– журналы аудита;
– информационное обеспечение ИСПДн и СЗПДн.

Резервное копирование ПДн осуществляется на регулярной еженедельной основе.

Резервное копирование конфигурационных файлов ИСПДн и СЗПДн осуществляется:

– перед внесением изменений в системное и прикладное программное обеспечение и задания необходимых параметров;
– после внесения изменений в системное и прикладное программное обеспечение и задания необходимых параметров и проверки нормального режима функционирования;
– регулярно на ежемесячной основе.

Резервное копирование журналов аудита осуществляется регулярно на еженедельной основе.

Резервное копирование информационного обеспечения ИСПДн и СЗПДн осуществляется регулярно на еженедельной основе.

Резервное копирование должно производиться в соответствии с утвержденным графиком резервного копирования в нерабочее время или при небольшой загрузке в целях снижения влияния подсистемы резервного копирования на работу ИСПДн.

Создание резервных копий должно регистрироваться в журнале подсистемы резервного копирования.

Должен проводиться ежеквартальный контроль состояния носителей резервных копий.

Должен проводиться ежеквартальный контроль целостности резервных копий.

Полные резервные копии должны храниться не менее 6 месяцев и их повторное использование (перезапись) может осуществляться в случае выполнения следующих условий:

– информация была признана устаревшей;
– существуют не менее 2 более свежих полных резервных копий;
– носитель после проверки был признан пригодным для использования;
– было проведена очистка запоминающего устройства согласно установленной в «Политике повторного использования и очистки ресурсов» процедуре.

В случае нарушения целостности информации или сбоев в работе ИСПДн и СЗПДн, требующих восстановления резервируемых данных осуществляется восстановление информации из резервных копий. Восстановление данных или ИС включает в себя:

– восстановление данных;
– восстановление конфигурации;

– тестирование работоспособности;
– включение компонент в ИСПДн.

4.7. Регламентное обслуживание ИСПДн

Регламентное обслуживание ИСПДн осуществляется администраторами ИС и администраторами информационной безопасности.

Регламентное обслуживание ИСПДн включает в себя:

– инвентаризацию ИС;
– мониторинг состояния ИС;
– мониторинг актуальности версий используемого ПО и их обновление;
– аудит настроек конфигурации ИС;

Администраторы информационной безопасности должны раз в полгода осуществлять инвентаризацию ИС. При инвентаризации ИС осуществляется проверка состава аппаратных и программных компонентов ИС.

Администраторы ИС должны проводить обновление используемого ПО. Обновление ПО осуществляется в автоматическом режиме. В случае невозможности автоматического обновления, его осуществляют администраторы путем непосредственной загрузки и установки обновлений в соответствии с инструкциями администраторов ИС. Проверка наличия обновлений производится в соответствии со спецификацией ПО и инструкциями администраторов ПО.

Администраторы информационной безопасности обязаны проводить ежеквартальный аудит настроек конфигурации ИС. Аудит осуществляется путем проверки соответствия имеющихся настроек ИС стандартам настройки данных ИС.

4.8. Анализ защищенности ИСПДн

Анализ защищенности ИСПДн осуществляется администраторами информационной безопасности с помощью подсистемы анализа защищенности и в соответствии с должностными инструкциями и инструкциями администратора средства анализа защищенности и методикой проведения анализа защищенности.

Анализ защищенности осуществляется на ежегодной основе, а также в случае значимых изменений в структуре ИСПДн.

Перед проведением анализа защищенности производится определение границ анализа защищенности. Определяется анализируемый сегмент, ИС и каналы передачи данных. Определяются точки проведения анализа.

Проводится инвентаризация ресурсов. Осуществляется:

– сбор информации о структуре сети, адресах узлов;

- получение информации о типах обнаруженных устройств;
- получение информации об используемых операционных системах и версиях сетевого оборудования;
- получение информации об имеющихся открытых ресурсах;
- получение информации об открытых сетевых портах и запущенных сервисах;
- получение доступной информации о системе, имеющихся пользователях, установленном программном обеспечении, обновлениях, настройках безопасности.

Осуществляется поиск полезной и критичной информации. В найденных ресурсах осуществляется поиск конфиденциальной информации, предоставляющей угрозу информационной безопасности (учётные записи, пароли, настройки безопасности и т.д.) а также конфиденциальной информации в свободном доступе.

Осуществляется поиск уязвимостей. Поиск уязвимостей осуществляется с использованием автоматизированных сканеров безопасности. При сканировании особое внимание уделяется системам хранения ПДн, компонентам СЗПДн и сетевому оборудованию. Допускается сканирование не всех рабочих станций пользователей, при условии, что они имеют идентичные настройки безопасности и существует возможность их обобщения.

Исследование защищенности рабочих станций. На типовой рабочей станции осуществляется изучение настроек безопасности, организации работы за компьютером. Проверяется возможность установки вредоносного ПО, изменения конфигурации, несанкционированной передачи информации.

По результатам работ формируется перечень объектов (прикладные системы, сетевое оборудование, компьютерные комплексы и т.д.) в виде обобщенной таблицы, по каждому из которых приведена возможность осуществления несанкционированного доступа, характер (вид) уязвимости и степень критичности. В отчёте предоставляются рекомендации по устранению обнаруженных уязвимостей, с учётом как аппаратно-программных средств обеспечения информационной безопасности, так и организационных мер.

4.9. Действия при внештатных ситуациях

В случае наступления внештатных ситуаций (наводнение, пожар, пропадание электропитания, теракт, вооруженное нападение, нарушения работы ИСПДн, нарушения режима конфиденциальности и других инцидентах и т.д.) необходимо обеспечить безопасность ПДн.

Действия сотрудников ГБУ РО «Онкодиспансер» в г. Таганроге в случае наступления внештатных ситуаций регламентированы Регламентом реагирования на чрезвычайные ситуации.

В случае наступления внештатных ситуаций необходимо предотвратить нарушение конфиденциальности ПДн. Предотвращение нарушения конфиденциальности осуществляется поддержанием функционирования подсистем обеспечения конфиденциальности, хранением в защищенном виде, а также блокированием доступа к ПДн в случае возникновения внештатных ситуаций.

В случае возникновения внештатных ситуаций необходимо предотвратить нарушение целостности ПДн. Нарушение целостности ПДн обеспечивается хранением на носителях, устойчивых к внешним воздействиям и в защищенных помещениях, или резервированием ПДн и хранением резервных копий на отчуждаемых носителях в защищенных помещениях, достаточно удаленных от основных помещений, в которых осуществляется хранение и обработка ПДн.

5. ПОРЯДОК ИЗМЕНЕНИЯ РЕГЛАМЕНТА

Внесение изменений в Регламент может носить как регламентный характер, так и быть вызванным изменениями в системе информационной безопасности или нормативных документах.

Изменение Регламента производится в следующих случаях:

- при изменении законодательства в области защиты ПДн;

  В случае внесения изменений в законодательства в области защиты ПДн необходимо провести пересмотр Регламента для оценки его соответствия новым требованиям.

Регламентный пересмотр

Регламентный пересмотр производится раз в год и обусловлен необходимостью соответствия Регламента текущему состоянию ИСПДн и используемых методов защиты ПДн.

Внесения изменений в регламентные документы ГБУ РО «Онкодиспансер» в г. Таганроге

Регламент разрабатывается на основе концептуальных документов по информационной безопасности. В случае изменения взглядов на проблему защиты ПДн или целей обеспечения безопасности ПДн изменения вносятся в концептуальные нормативные документы и, как следствие, требуется пересмотр Регламента.

Внесения изменений в информационную систему персональных данных

В случае внесения изменений в ИСПДн, Регламент должен быть дополнен и/или исправлен, чтобы отвечать текущему состоянию ИСПДн.

При внесении изменений в Регламент проводятся следующие мероприятия:

- обследование и анализ изменений:
  - В ИСПДн в целом;
  - В СЗПДн;
  - В системе нормативных и регламентных документов;
- внесение изменений в перечень защищаемых объектов и ресурсов (при необходимости).
- формулировка и описание дополнительных (изменённых) требований к СЗПДн, мер и процедур защиты ПДн.
- утверждение изменений в Регламенте;
- доведение изменений до сотрудников, ответственных за обеспечение безопасности ПДн.

ЛИСТ ИЗМЕНЕНИЙ

Версия	Дата	Номер раздела, рисунка или таблицы	Тип изменений*	Автор	Краткое содержание сути изменения

ПРИЛОЖЕНИЕ 1

СОГЛАСИЕ
(работника)

Я, _____,

проживающий по адресу: _____

_____

паспорт _____ № _____, выдан (орган, выдавший паспорт / дата выдачи)

_____

в соответствии с Трудовым кодексом Российской Федерации и Федеральным законом «О персональных данных» своей волей и в своем интересе выражаю ГБУ РО «Онкодиспансер» в г. Таганроге зарегистрированному по адресу: 347910, г.Таганрог, ул.Московская, 17,
согласие на обработку моих персональных данных или сообщения моих данных третьей стороне (*Ф.И.О., даты и места рождения, гражданства, места жительства, паспортных данных, сведений об образовании, о занимаемой должности, данных о предыдущих местах работы, доходов, идентификационного номера налогоплательщика, номера страхового свидетельства государственного пенсионного страхования, сведений о воинском учете, данных о допуске к сведениям, составляющим государственную тайну, сведений о наградах, сведений о социальных льготах, которые предоставляются в соответствии с законодательством*) в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия в моем трудоустройстве, обучении и продвижении по службе, для формирования общедоступных источников персональных данных (справочников, адресных книг и т.д.).

Если мои персональные данные возможно получить только у третьей стороны, то я должен быть уведомлен об этом заранее с указанием о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях моего отказа дать письменное согласие на их получение, и от меня должно быть получено письменное согласие.

Согласие вступает в силу со дня его подписания и действует до момента прекращения трудового договора.

В случае изменения моих персональных данных в течение срока действия трудового договора обязуюсь проинформировать об этом отдел правового и кадрового обеспечения ГБУ РО «Онкодиспансер» в г. Таганроге в установленном порядке.

Согласие может быть отозвано мною в любое время на основании моего письменного заявления.

«____» _____ 20__ г. _____

подпись, расшифровка подписи, дата

ПРИЛОЖЕНИЕ 2

ЗАЯВКА

на внесение изменений в списки пользователей информационной системы персональных данных ГБУ РО «Онкодиспансер» в г. Таганроге и наделение пользователей полномочиями доступа к ресурсам системы

Прошу зарегистрировать пользователя (исключить из списка пользователей, изменить полномочия пользователя) ИС _____
(ненужное зачеркнуть)

_____
(должность с указанием подразделения)

_____
(фамилия имя и отчество сотрудника)

предоставив ему полномочия, необходимые (лишив его полномочий, необходимых)
(ненужное зачеркнуть)

для решения задач: _____
(список задач согласно формуляров задач)

_____

_____

_____

на срок с «___» _____ 20__ г. по «___» _____ 20__ г

Начальник

_____
(наименование заказывающего подразделения)

«____» _____ 20___ г. _____ (подпись) _____ (фамилия)

ЗАДАНИЕ

на внесение изменений в права доступа пользователей

Администраторам серверов и баз данных

_____
(фамилии и инициалы исполнителей)

_____

_____

Произвести изменения в списках пользователей и правах доступа серверов и баз данных

Администратору информационной безопасности

_____
(фамилия и инициалы исполнителя)

Произвести изменения в списках пользователей и правах доступа в ИС

Главный врач ГБУ РО «Онкодиспансер» в г. Таганроге

_____

«_____» _____ 20___ г.

Обратная сторона заявки

Пользователю присвоены учетная запись _____, и пароль (выданы личные реквизиты доступа_____) и предоставлены следующие права доступа:

№ п/п	Описание ресурса, к которому предоставляется доступ ***(Данные, сетевой ресурс на файловом сервере, сервер баз данных, приложение, FTP, WWW серверы, общие папки на сервере Exchange, сеть Интернет, другие ресурсы)***	Предоставляемые права доступа	Срок предоставления доступа

Администратор сервера

_____
(подпись, фамилия)
«____» _____ 200___ г.

Администратор сервера

_____
(подпись, фамилия)
«____» _____ 200___ г.

Администратор базы данных

_____
(подпись, фамилия)
«____» _____ 200___ г.

Администратор информационной безопасности

_____
(подпись, фамилия)
«____» _____ 200___ г.

Учетную запись, пароль, (личные реквизиты доступа) получил, с порядком работы в ИСПДн и обязанностях по защите ПДн ознакомлен.

Пользователь

_____
(подпись, фамилия)

«____» _____ 20___ г.

ПРИЛОЖЕНИЕ 3

Журнал учета носителей информации

ID Носителя	Наименование носителя информации	Расположение носителя информации	Хранимая информация	Ответственный сотрудник	Срок предоставления доступа

ПРИЛОЖЕНИЕ 4

ЗАЯВКА

на передачу персональных данных, обрабатываемых в информационной системе персональных данных ГБУ РО «Онкодиспансер» в г. Таганроге

Прошу разрешить передачу персональных данных:

_____

(перечень персональных данных, с указанием субъектов ПДн и объема передаваемых данных)

_____

_____

_____

Следующему получателю:_____

(указание получателя (наименование, адрес, контактные данные) и лица, ответственного за получение ПДн.)

_____

_____

В целях:

_____

(указание целей передачи персональных данных или обоснование необходимости передачи)

_____

Посредством:

_____

(указание способов передачи персональных данных: носители, каналы передачи, метод доставки)

_____

Сотрудник

_____

(должность, подразделение, ФИО)

«____» _____ 20___ г. _____ _____

(подпись) (фамилия)

Утверждаю

Главный врач
ГБУ РО «Онкодиспансер» в г. Таганроге

_____

«_____» _____ 20___ г.

ПРИЛОЖЕНИЕ 5

ПРИКАЗ

на уничтожение персональных данных, обрабатываемых в информационной системе персональных данных ГБУ РО «Онкодиспансер» в г. Таганроге

Приказываю уничтожить персональные данные:

_____

(спецификация персональных данных, с указанием ИСПДн, субъектов ПДн и объема передаваемых данных)

_____

_____

_____

В соответствии с :_____

(указание причины прекращения обработки ПДн и их уничтожения.)

_____

_____

В срок:

_____

(указание срока уничтожения персональных данных)

_____

Назначить сотрудников, ответственных за уничтожение персональных данных:

1. _____
2. _____
3. _____

и осуществить уничтожение персональных данных в соответствии с приказом.

Главный врач
ГБУ РО «Онкодиспансер» в г. Таганроге

_____

«_____» _____ 20___ г.