УТВЕРЖДАЮ

Главный врач
ГБУЗ «Баргузинская центральная районная больница»

_____ Л.В. Карпова

М.П.

«09» 01 2016 г.

ПОЛОЖЕНИЕ О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

обрабатываемых в информационных системах ГБУЗ «Баргузинская центральная районная больница»

СОГЛАСОВАНО

Заместитель главного врача по медицинской части

_____ В.В. Цыденова

«09» 01 2016г.

2016 г.

ОГЛАВЛЕНИЕ

1. Общие положения

Настоящее «Положение о защите персональных данных, обрабатываемых в информационных системах ГБУЗ «Баргузинская ЦРБ» (далее – Положение) разработано в соответствии с Законом Российской Федерации от 27 июля 2006 года №152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказом 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», иных нормативных и методических документов ФСТЭК России и ФСБ России, Приказом ФСТЭК России от 11 февраля 2013 г. №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Положение разработано в целях обеспечения безопасности персональных данных (далее – ПДн) при их обработке в информационных системах ГБУЗ «Баргузинская ЦРБ» (далее – ИСПДн).

Положение определяет порядок работы персонала ИСПДн в части обеспечения безопасности ПДн при их обработке, порядок использования средств защиты информации, разработку и принятие мер по предотвращению возможных опасных последствий таких нарушений, порядок приостановки предоставления ПДн в случае обнаружения нарушений при их обработке, порядок обучения персонала практике работы в ИСПДн, порядок контроля соблюдения условий использования средств защиты информации, предусмотренные эксплуатационной и технической документацией, правила обновления общесистемного и прикладного программного обеспечения, правила организации антивирусной защиты и парольной защиты ИСПДн, порядок охраны и допуска посторонних лиц в защищаемые помещения.

2. Порядок предоставления допуска пользователей к работе в ИСПДн

Настоящий порядок определяет действия персонала ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн.

Пользователями ИСПДн являются работники лечебно-профилактического учреждений (далее - Работники).

Первоначальный допуск пользователей к работе в ИСПДн осуществляется на основании приказа, который издается руководителем (далее - Руководитель). В приказе определяется список работников, допущенных к работе в ИСПДн.

С целью обеспечения ответственности за ведение, нормальное функционирование и контроль работы средств защиты информации и выполнения необходимых мероприятий по обеспечению безопасности в ИСПДн назначается администратор информационной безопасности.

С целью соблюдения принципа персональной ответственности за свои действия каждому работнику, допущенному к работе в ИСПДн, должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать в ИСПДн.

Использование несколькими работниками при работе в ИСПДн одного и того же имени пользователя ***запрещено.***

В дальнейшем, процедура регистрации (создания учетной записи) пользователя и предоставления ему (или изменения его) прав доступа к ресурсам ИСПДн инициируется заявкой.

В заявке указывается:

- содержание запрашиваемых изменений (регистрация нового пользователя ИСПДн, удаление учетной записи пользователя, расширение или сужение полномочий и прав доступа к ресурсам ИСПДн ранее зарегистрированного пользователя);

- должность (с полным наименованием отдела), фамилия, имя и отчество работника;

- имя пользователя (учетной записи) данного работника;

- полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользователем задач в ИСПДн).

Заявку рассматривает и визирует руководитель, утверждая тем самым производственную необходимость допуска (изменения прав доступа) данного работника к необходимым для решения им указанных в заявке задач ресурсам ИСПДн. Затем заявка передается администратору информационной безопасности ИСПДн для внесения необходимых изменений в списки пользователей ИСПДн.

На основании заявки администратор информационной безопасности ИСПДн производит необходимые операции по созданию (удалению) учетной записи пользователя, присвоению ему начального значения пароля, а также регистрацию персонального идентификатора и другие необходимые действия, указанные в заявке.

После внесения изменений в списки пользователей администратор информационной безопасности должен обеспечить настройки средств защиты соответствующие требованиям безопасности указанной ИСПДн.

Работнику, зарегистрированному в качестве нового пользователя ИСПДн, сообщается имя соответствующего ему пользователя и может выдаваться персональный идентификатор (для работы в режиме усиленной аутентификации) и начальное значение пароля, которое он обязан сменить при первом же входе в систему.

Исполненная заявка хранится у администратора информационной безопасности ИСПДн.

Она может впоследствии использоваться:

- для восстановления полномочий пользователей после возникновения внештатных ситуаций;

- для контроля правомерности наличия у конкретного пользователя прав доступа к тем или иным ресурсам ИСПДн при разборе конфликтных ситуаций;

- для проверки сотрудниками контролирующих органов правильности настройки средств разграничения доступа к ресурсам ИСПДн.

3. Порядок работы пользователей ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн

Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн.

Пользователь несет ответственность за правильность включения и выключения средств вычислительной техники (СВТ), входа в систему и все действия при работе в ИСПДн.

Перед началом работы в ИСПДн, работники, допущенные к работе с ПДн, принимают под роспись обязательство о неразглашении персональных данных.

Вход пользователя в систему должен осуществляться по выдаваемому ему электронному идентификатору и по персональному паролю.

Запись информации, содержащей ПДн, должна осуществляться только на машинные носители информации, соответствующим образом учтенные в Журнале учета защищаемых носителей информации. Ответственным за ведение Журнала учета является администратор информационной безопасности.

При работе со съемными машинными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов с использованием штатных антивирусных программ, установленных на компьютерах ИСПДн. В случае обнаружения вирусов пользователь обязан немедленно прекратить их использование и действовать в соответствии с требованиями данного Положения;

Каждый работник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и ***обязан***:

- строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;
- знать и строго выполнять правила работы со средствами защиты информации, установленными на компьютерах ИСПДн;
- хранить в тайне свой пароль (пароли). В соответствии с п. 7.5. данного Положения и с установленной периодичностью менять свой пароль (пароли);
- хранить установленным порядком свое индивидуальное устройство идентификации (ключ) и другие реквизиты в недоступном для посторонних месте;
- выполнять требования Положения по организации антивирусной защиты в полном объеме.

Немедленно известить администратора информационной безопасности в случае утери индивидуального устройства идентификации (ключа) или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

- фактов совершения попыток несанкционированного доступа (далее - НСД) к ИСПДн;
- несанкционированных изменений в конфигурации программных или аппаратных средств ИСПДн;
- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию СВТ, выхода из строя или неустойчивого функционирования узлов СВТ или периферийных устройств (сканера, принтера и т.п.), а также перебоев в системе электроснабжения;

– некорректного функционирования установленных на компьютеры технических средств защиты;

– непредусмотренных отводов кабелей и подключенных устройств.

Пользователю категорически ***запрещается***:

- использовать компоненты программного и аппаратного обеспечения ПЭВМ в неслужебных целях;

- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения;

- осуществлять обработку ПДн в присутствии посторонних (не допущенных к данной информации) лиц;

- записывать и хранить ПДн на неучтенных машинных носителях информации;

- оставлять включенным без присмотра компьютер, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

- оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации, машинные носители и распечатки, содержащие ПДн;

- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к нарушению конфиденциальности ПДн;

- размещать средства отображения информации (монитор, принтер и т.п.) таким образом, чтобы с них существовала возможность визуального считывания информации посторонними лицами.

Администратор информационной безопасности обязан:

– знать состав основных и вспомогательных технических систем и средств (далее - ОТСС и ВТСС) установленных и смонтированных в ИСПДн, перечень используемого программного обеспечения (далее - ПО) в ИСПДн;

– контролировать целостность печатей (пломб, защитных наклеек) на периферийном оборудовании, защищенных СВТ и других устройствах;

– производить необходимые настройки подсистемы управления доступом установленных в ИСПДн СЗИ от НСД и сопровождать их в процессе эксплуатации, при этом:

- реализовывать полномочия доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (файлам, каталогам, принтеру и т.д.);
- вводить описания пользователей ИСПДн в информационную базу системы разграничения доступа в ИСПДн;
- своевременно удалять описания пользователей из базы данных СЗИ при изменении списка допущенных к работе лиц;
- проводить инструктаж пользователей ИСПДн по правилам работы с используемыми техническими средствами и системами защиты информации;
- контролировать своевременное проведение смены паролей для доступа пользователей к компьютерам и ресурсам ИСПДн;
- обеспечивать постоянный контроль выполнения пользователями установленного комплекса мероприятий по обеспечению безопасности информации в ИСПДн;
- осуществлять контроль порядка создания, учета, хранения и использования резервных и архивных копий массивов данных;
- настраивать и сопровождать подсистемы регистрации и учета действий пользователей при работе в ИСПДн;
- организовывать печать файлов пользователей на принтере и осуществлять контроль соблюдения установленных правил и параметров регистрации и учета бумажных носителей информации;
- периодически тестировать функции СЗИ от НСД с использованием специальных средств анализа защищенности, особенно при изменении программной среды и полномочий исполнителей;
- восстанавливать программную среду, программные средства и настройки СЗИ при сбоях;
- вести две копии программных средств СЗИ от НСД и контролировать их работоспособность;
- периодически обновлять антивирусные средства (базы данных), контролировать соблюдение пользователями порядок и правила проведения антивирусного тестирования;
- проводить работу по выявлению возможных каналов вмешательства в процесс функционирования ИСПДн и осуществления несанкционированного доступа к информации и техническим средствам вычислительной техники;
- обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации технического обслуживания ИСПДн и отправке его в

ремонт (контролировать затирание персональных данных на носителях информации);

- присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию ИСПДн;
- вести документацию на ИСПДн в соответствии с требованиями нормативных документов.

4. Порядок резервирования и восстановления работоспособности технических средств, программного обеспечения, баз данных, защищаемой информации и средств защиты информации

Настоящий порядок определяет организацию резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации.

К использованию для создания резервных копии в ИСПДн, допускаются только зарегистрированные в Журнале учета носители.

Администратор информационной безопасности ***обязан*** осуществлять периодическое резервное копирование персональных данных.

Носители информации, предназначенные для создания резервной копии и хранения персональных данных, выдаются установленным порядком администратором информационной безопасности. По окончании процедуры резервного копирования электронные носители сдаются на хранение администратору информационной безопасности.

При восстановлении работоспособности программного обеспечения сначала осуществляется резервное копирование защищаемой информации, затем производится полная деинсталляция некорректно работающего программного обеспечения.

Восстановление программного обеспечения производится путем его инсталляции с использованием эталонных дистрибутивов, хранение которых осуществляется администратором информационной безопасности в специальном хранилище.

При работе на компьютерах ИСПДн рекомендуется использовать источники бесперебойного питания, с целью предотвращения повреждения технических средств и(или) защищаемой информации в результате сбоев в сети электропитания.

При восстановлении работоспособности средств защиты информации следует выполнить их настройку в соответствии с требованиями безопасности информации, изложенными в техническом задании на создание системы защиты персональных данных.

Восстановление средств защиты информации производится с использованием эталонных сертифицированных дистрибутивов, которые хранятся у администратора информационной безопасности. После успешной настройки средств защиты информации необходимо выполнить резервное копирование настроек данных средств с помощью встроенных в них функций на зарегистрированный носитель.

Ответственность за проведение резервного копирования, мероприятий по восстановлению работоспособности технических средств, мероприятий по восстановлению средств защиты информации возлагается на администратора информационной безопасности ИСПДн.

5. Порядок обучения персонала практике работы в ИСПДн в части обеспечения безопасности персональных данных

Перед началом работы в ИСПДн пользователи должны пройти инструктаж по обеспечению безопасности персональных данных при работе с ними в ИСПДн, под роспись;

Пользователи должны продемонстрировать администратору информационной безопасности наличие необходимых знаний и умений для выполнения требований по обеспечению безопасности персональных данных при работе с ними в ИСПДн;

Ответственным за организацию обучения и оказание методической помощи в Управлении является администратор информационной безопасности.

6. Правила антивирусной защиты

Настоящие правила определяют требования к организации защиты объекта ИСПДн от разрушающего воздействия вредоносного программного обеспечения, компьютерных вирусов и устанавливает ответственность руководителей и работников, эксплуатирующих и сопровождающих компьютеры в составе ИСПДн, за их выполнение.

К использованию на компьютерах допускаются только лицензионные антивирусные средства, прошедшие сертификацию по требованиям безопасности ФСТЭК

России.

Установка и начальная настройка средств антивирусного контроля на компьютерах осуществляется администратором информационной безопасности, либо с привлечением организаций – лицензиатов ФСТЭК России.

Администратор информационной безопасности осуществляет периодическое обновление антивирусных средств и контроль их работоспособности.

Ярлык (ссылка) для запуска антивирусной программы должен быть доступен всем пользователям информационной системы.

Еженедельно в начале работы, после загрузки компьютера в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов компьютеров. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, лентах, CD-ROM и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

Файлы, помещаемые в электронный архив на магнитных носителях, должны в обязательном порядке проходить антивирусный контроль.

Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера, администратором информационной безопасности должна быть выполнена антивирусная проверка ИСПДн.

На компьютеры пользователей запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации;

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 администратором информационной безопасности) должен провести внеочередной антивирусный контроль компьютера.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь ***обязан***:

- приостановить обработку данных в ИСПДн;
- немедленно поставить в известность о факте обнаружения зараженных вирусом

файлов администратора информационной безопасности, а также смежные подразделения, использующие эти файлы в работе;

- совместно с владельцем зараженных вирусом файлов провести анализ возможности, дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов.

Ответственность за организацию антивирусного контроля в ИСПДн в соответствии с требованиями настоящего Положения возлагается на администратора информационной безопасности;

Ответственность за проведение мероприятий антивирусной защиты в конкретной ИСПДн и соблюдение требований настоящего Положения возлагается на администратора информационной безопасности и всех пользователей данной ИСПДн.

7. Правила парольной защиты

Данные правила регламентируют организационно-технические мероприятия по обеспечению процессов генерации, смены и прекращения действия паролей в ИСПДн, а также контроль действий пользователей при работе с паролями.

Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль действий пользователей при работе с паролями возлагается на администратора информационной безопасности.

При доступе пользователя в систему должна осуществляться идентификация и проверка подлинности по идентификатору и паролю, а также с использованием электронных идентификаторов.

Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями самостоятельно с учетом следующих требований:

- пароль должен быть длиной не менее шести буквенно-цифровых символов;

- символы паролей для рабочих станций, на которых установлено средство защиты информации от несанкционированного доступа, должны вводиться в режиме латинской раскладки клавиатуры;

- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

- при смене пароля новое значение должно отличаться от предыдущих;

- пользователь не имеет права сообщать личный пароль другим лицам.

Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в течение 3 месяцев.

Удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение, переход на другую работу внутри учреждения и т.п.) должна производиться администратором информационной безопасности немедленно после окончания последнего сеанса работы данного пользователя с системой, на основании указания руководителя или начальника отдела кадров.

Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри учреждения и другие обстоятельства) администратора информационной безопасности.

В случае компрометации личного пароля пользователя ИСПДн должны быть немедленно предприняты меры по изменению его пароля.

Контроль действий пользователей при работе с паролями, соблюдение порядка их смены, хранения и использования возлагается на администратора информационной безопасности.

8. Правила обновления общесистемного и прикладного программного обеспечения, технического обслуживания ИСПДн

Настоящие правила регламентируют обеспечение безопасности информации при проведении обновления, модификации общесистемного и прикладного программного обеспечения, технического обслуживания и при возникновении нештатных ситуаций в работе ИСПДн.

Право на установку, обновление и модификацию общесистемного и прикладного программного обеспечения компьютеров ИСПДн предоставляется системному администратору ИСПДн и администратору информационной безопасности ИСПДн.

Право внесения изменений в конфигурацию аппаратно-программных средств защиты информации предоставляется системному администратору по согласованию с администратором информационной безопасности. Изменение конфигурации аппаратно-программных средств ИСПДн другим лицам ***запрещено***.

Заявку на внесение изменений в конфигурацию аппаратно-программных средств защищенных рабочих мест ИСПДн, рассматривает руководитель, визирует ее, утверждая тем самым производственную необходимость проведения указанных в заявке изменений.

После чего заявка передается администратору информационной безопасности для непосредственного исполнения работ по внесению изменений в конфигурацию компьютера, указанного в заявке.

Установка или обновление подсистем ИСПДн должны проводиться в строгом соответствии с технологией проведения модификаций программных комплексов данных подсистем.

Установка и обновление ПО (системного, прикладного, тестового и т.п.) на компьютерах производится только с оригинальных лицензионных дистрибутивных носителей (дискет, компакт дисков и т.п.).

Все добавляемые программные и аппаратные компоненты должны быть предварительно проверены на работоспособность, а также отсутствие опасных функций.

После установки (обновления) ПО, администратор информационной безопасности должен произвести требуемые настройки средств управления доступом к компонентам компьютера и проверить работоспособность ПО и правильность их настройки.

При возникновении ситуаций, требующих передачи технических средств в сервисный центр с целью ремонта, администратор информационной безопасности обязан предпринять необходимые меры для затирания защищаемой информации, которая хранилась на дисках компьютера.

9. Порядок контроля обеспечения защиты информации в ИСПДн и приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления

Контроль защиты информации в ИСПДн - комплекс организационных и технических мероприятий, которые организуются и осуществляются в целях предупреждения и пресечения возможности получения посторонними лицами охраняемых сведений, выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации, предотвращения

специальных программно-технических воздействий, вызывающих нарушение характеристик безопасности информации или работоспособности систем информатизации.

Основными задачами контроля являются:

- проверка организации выполнения мероприятий по защите информации в ГБУЗ «Баргузинская ЦРБ», учета требований по защите информации в разрабатываемых плановых и распорядительных документах;
- выявление демаскирующих признаков объектов ИСПДн;
- уточнение зон перехвата обрабатываемой на объектах информации, возможных каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;
- проверка выполнения установленных норм и требований по защите информации от утечки по техническим каналам, оценка достаточности и эффективности мероприятий по защите информации;
- проверка выполнения требований по защите ИСПДн от несанкционированного доступа;
- проверка выполнения требований по антивирусной защите автоматизированных систем и автоматизированных рабочих мест;
- проверка знаний пользователей по вопросам защиты информации и их соответствия требованиям уровня подготовки для конкретного рабочего места;
- оперативное принятие мер по пресечению нарушений требований (норм) защиты информации в ИСПДн;
- разработка предложений по устранению (ослаблению) демаскирующих признаков и технических каналов утечки информации.

Контроль защиты информации проводится с учетом реальных условий по всем физическим полям, по которым возможен перехват информации, циркулирующей в ИСПДн, и осуществляется по объектовому принципу, при котором на объекте одновременно проверяются все вопросы защиты информации. Перечень каналов утечки устанавливается в соответствии с моделью угроз.

В ходе контроля проверяются:

- соответствие принятых мер по обеспечению безопасности персональных данных;

- своевременность и полнота выполнения требований настоящего Положения и других руководящих документов по защите персональных данных;

- эффективность применения организационных и технических мероприятий по защите информации;

- устранение ранее выявленных недостатков.

Кроме того, проводятся необходимые измерения и расчеты, приглашенными для этих целей специалистами организации, имеющей соответствующие лицензии ФСТЭК России.

Основными видами технического контроля являются визуально-оптический контроль, контроль эффективности защиты информации от утечки по техническим каналам, контроль несанкционированного доступа к информации и программно-технических воздействий на информацию.

Полученные в ходе ведения контроля результаты обрабатываются и анализируются в целях определения достаточности и эффективности предписанных мер защиты информации и выявления нарушений. При обнаружении нарушений норм и требований по защите информации администратор информационной безопасности докладывает руководителю для принятия ими решения о прекращении обработки информации и проведения соответствующих организационных и технических мер по устранению нарушения. Результаты контроля защиты информации оформляются актами либо в соответствующих журналах учета результатов контроля.

Невыполнение предписанных мероприятий по защите ПДн, считается предпосылкой к утечке информации (далее - предпосылка). По каждой предпосылке для выяснения обстоятельств и причин невыполнения установленных требований по указанию руководителя или ответственного за защиту информации проводится расследование. Для проведения расследования назначается комиссия с привлечением администратора информационной безопасности. Комиссия обязана установить, имела ли место утечка сведений, и обстоятельства ей сопутствующие, установить лиц, виновных в нарушении предписанных мероприятий по защите информации, установить причины и условия, способствовавшие нарушению, и выработать рекомендации по их устранению. После окончания расследования руководитель принимает решение о наказании виновных лиц и необходимых мероприятиях по устранению недостатков.

Ведение контроля защиты информации осуществляется путем проведения периодических, плановых и внезапных проверок объектов защиты. Периодические, плановые и внезапные проверки объектов организации проводятся, как правило, силами администратора информационной безопасности, в соответствии с утвержденным планом или по согласованию с руководителем.

Одной из форм контроля защиты информации является обследование объектов ИСПДн. Оно проводится не реже одного раза в год рабочей группой в составе администратора информационной безопасности, ответственного за эксплуатацию объекта. Для обследования ИСПДн может привлекаться организация, имеющая лицензию ФСТЭК России на деятельность по технической защите информации.

Обследование ИСПДн проводится с целью определения соответствия помещений, технических и программных средств требованиям по защите информации, установленным в «Аттестате соответствия» и(или) требованиям по безопасности.

В ходе обследования проверяется:

- соответствие текущих условий функционирования обследуемого объекта ИСПДн условиям, сложившимся на момент проверки;

- соблюдение организационно-технических требований помещений, в которых располагается ИСПДн;

- сохранность печатей, пломб на технических средствах передачи и обработки информации, а также на устройствах их защиты, отсутствие повреждений экранов корпусов аппаратуры, оболочек кабелей и их соединений с шинами заземления;

- соответствие выполняемых на объекте ИСПДн мероприятий по защите информации данным, изложенным в настоящем положении;

- выполнение требований по защите информационных систем от несанкционированного доступа;

- выполнение требований по антивирусной защите.

Государственный контроль состояния защиты информации осуществляется Федеральной службы по техническому и экспортному контролю России и Федеральной службой безопасности России в рамках их полномочий в соответствии с действующим законодательством Российской Федерации. Доступ представителей указанных федеральных органов исполнительной власти на объекты для проведения проверки, а также к работам и документам в объеме, необходимом для осуществления контроля, обеспечивается в установленном порядке по предъявлении служебного удостоверения сотрудника, а также документа установленной формы на право проведения проверки.

10. Порядок охраны и допуска посторонних лиц в помещения ИСПДн

В ГБУЗ «Баргузинская ЦРБ» должна быть предусмотрена физическая охрана технических средств ИСПДн (устройств и носителей информации),

предусматривающая контроль доступа в помещения посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения и хранилище носителей информации.

В помещениях должна быть установлена охранная и пожарная сигнализация.

Серверное и коммутационное оборудование ИСПДн должно находиться под надежным замком, в отдельном помещении или запирающемся шкафу, ключ должен храниться у администратора информационной безопасности.

Вскрытие и закрытие помещений осуществляется сотрудниками, работающими в данных помещениях. Список сотрудников, имеющих право вскрывать (сдавать под охрану) и опечатывать помещения утверждается руководителем и передаётся на пост охраны.

При закрытии помещений и сдачей их под охрану сотрудники, ответственные за помещения проверяют закрытие окон, выключают освещение, бытовые приборы, оргтехнику и проверяют противопожарное состояние помещения, а документы и носители информации на которых содержатся персональные данные, убираются для хранения в запираемый ящик стола или сейф.

При обнаружении повреждения замков, дверей или наличия других признаков, указывающих на возможное проникновение в помещение посторонних лиц, помещение не вскрывается, а составляется акт, в присутствии охранника. О происшествии немедленно сообщается руководителю и(или) ответственному за защиту информации.

При срабатывании охранной сигнализации в служебных помещениях в нерабочее время охранник сообщает о случившемся ответственному за помещение, или ответственному за защиту информации, или руководителю, или администратору информационной безопасности.

11. Заключительные положения

Требования настоящего Положения обязательны для всех работников, обрабатывающих персональные данные.

Нарушение требований настоящего Положения влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.