Утверждена приказом начальника
ФБУЗ «МСЧ № 52» ФМБА России № 666 от 11.12.2014г.
(внесены изменения приказом № 451 от 15.12.2017г.)

Политика
в отношении обработки персональных данных
в федеральном бюджетном учреждении здравоохранения
«Медико–санитарная часть № 52» ФМБА России
(ФБУЗ «МСЧ № 52» ФМБА России)

1. Общие положения

1.1 Политика представляет собой изложение целей, задач защиты, правил и руководящих принципов в области информационной безопасности, которыми руководствуется ФБУЗ «МСЧ № 52» ФМБА России в своей деятельности, а также принципов обеспечения безопасности персональных данных.

Политика, является документом, определяющим категории субъектов персональных данных, цели, правовое основание, принципы и правила обработки персональных данных, а также содержит сведения о реализуемых требованиях к защите персональных данных оператора ФБУЗ «МСЧ № 52» ФМБА России – ИНН 4341000054, ОГРН 1034313500704, юридический адрес: 613040, Кировская область, г. Кирово-Чепецк, ул. Островского, 2

Законодательной основой Политики являются Конституция Российской Федерации, Гражданский, Уголовный и Трудовой кодексы, Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных, законы, постановления, другие нормативные документы действующего законодательства Российской Федерации, документы ФСТЭК и ФСБ России.

При разработке учитывались основные принципы создания комплексных мер информационной безопасности персональных данных в ФБУЗ «МСЧ № 52» ФМБА России. Соблюдение принципов Политики является обязательным для всех работников, которые имеют непосредственное отношение к обработке персональных данных и может быть пересмотрена в случае изменения законодательства РФ о персональных данных и нормативных правовых актов, регламентирующих деятельность ФБУЗ «МСЧ № 52» ФМБА России, все изменения и дополнения вносятся на основании Приказа руководителя.

1.2 Термины и определения

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

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Обработка персональных данных- любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, в том числе, следующие действия: сбор, запись, систематизация, накопление, хранение, уточнение(обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

Автоматизированная обработка- обработка персональных данных при помощи любых средств вычислительной техники.

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

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

Блокирование персональных данных - временное прекращение любой обработки персональных данных (за исключением случав, когда такая обработка необходима для уточнения персональных данных).

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

Обезличивание персональных данных- действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Информационная система персональных данных-совокупность содержащихся в базах данных персональных данных и обеспечивающих обработку информационных технологий и технических средств.

Основные понятия используются в тех значениях, в каких они определены Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее- Федеральный закон от 27.07.2006 № 152 –ФЗ)

1.3 Политика подлежит опубликованию на официальном сайте Учреждения в сети Интернет.

2. Правовое основание обработки персональных данных

Обработка персональных данных в ФБУЗ «МСЧ № 52» ФМБА России осуществляется на основании:

- Конституции Российской Федерации;
- Трудового кодекса Российской Федерации;
- Гражданского кодекса Российской Федерации;
- Налогового кодексом Российской Федерации;
- Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федерального закона Российской Федерации от 24.07.1998 № 125-ФЗ «Об обязательном социальном страховании от несчастных случаев на производстве и профессиональных заболеваний»;
- Федерального законам Российской Федерации от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»;
- Федерального закона Российской Федерации от 21.11.2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- Федерального закона Российской Федерации от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан РФ»;
- Федерального закона Российской Федерации от 15.11.1997 № 143-ФЗ «Об актах гражданского состояния»;
-Федерального закона Российской Федерации от 01.04.1996 № 27-ФЗ «Об индивидуальном (персонифицированном учете и системе обязательного пенсионного страхования»;
- Устава ФБУЗ «МСЧ № 52» ФМБА России.

3. Цели обработки персональных данных

ФБУЗ «МСЧ № 52» ФМБА России осуществляет обработку персональных данных в целях:

обеспечение требований соблюдения Конституции Российской Федерации, федеральных и областных законов, нормативных правовых актом Российской Федерации и Кировской области в рамках выполнения, условий с трудового договора между учреждением и работником;

реализации государственного задания, по оказанию медицинской, медико-санитарной помощи, стоматологической помощи, организация обеспечения донорской кровью;

в целях ведения кадрового учета и делопроизводства, проведения кадровых конкурсов по замещению вакантных должностей и в резерв кадров, ведение бухгалтерского учета, заключение договоров гражданско-правового характера, рассмотрение обращений граждан.

4. Категории персональных данных

Обрабатываемые персональные данные субъекта	Пациент	Работник
Фамилия, Имя, Отчество	X	X
Пол	X	X
Паспортные данные	X	X
Дата рождения	X	X
Место рождения		X
Адрес регистрации	X	X
Адрес места жительства		X
Семейное положение		X
Состав семьи (муж / жена, дети)		X
Данные свидетельства о рождении		X
Социальное положение		X
Сведения о доходах		X
Образование		X
Трудовая деятельность до приёма на работу		X
Трудовой стаж		X
Телефон (домашний, рабочий, мобильный)		X
Знание иностранных языков		X
Фотография	X	X
Оклад		X
Данные о трудовом договоре		X
Воинский учёт		X
Данные свидетельства о постановке на налоговый учёт (ИНН)		X
Данные об аттестации работников		X
Данные о повышении квалификации		X
Данные о наградах, медалях		X
Данные о поощрениях		X
Данные о почетных званиях		X
Данные о приёме на работу		X
Данные о перемещении по должности		X
Данные об увольнении		X
Данные об отпусках		X
Данные о командировках		X
Данные свидетельств о заключении и расторжении брака		X
Данные о государственном пенсионном страховании		X
Данные о негосударственном пенсионном обеспечении		X
Данные о полисе обязательного медицинского страхования	X	X
Данные свидетельства о смерти	X	X
Данные банковских карт		X
Сведения о членстве в профсоюзе		X
Сведения о болезнях	X	
Сведения о диагнозах	X	
Данные об инвалидности	X	X
Сведения о состоянии здоровья	X	
Оказанные медицинские услуги	X	
Биометрические данные	X	
Место работы и (или) учебы	X	
Сведения о наличии судимости у родителей несовершеннолетних пациентов	X	

5. Категории субъектов, персональных данных

- сотрудники, состоящие в трудовых отношениях с ФБУЗ «МСЧ № 52» и их несовершеннолетние дети;
- бывшие сотрудники;
- студенты, проходящие практику в ФБУЗ «МСЧ № 52» ФМБА России;
- физические лица, обратившиеся за медицинской помощью и их родственники;
- интерны, проходящие обучение;
- лица, командированные в ФБУЗ «МСЧ № 52» ФМБА России;
- физические лица, состоящие в договорных и гражданско-правовых отношениях с ФБУЗ «МСЧ № 52» ФМБА России;
- соискатели вакансий

6. Основные принципы обработки персональных данных

6.1 Обработка персональных данных осуществляется на законной и справедливой основе. Осуществляя обработку персональных данных должны выполнять все требования действующего законодательства в области защиты персональных данных и быть справедливыми по отношению к субъекту данных.

6.2 Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимых с целями сбора персональных данных.

6.3 Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой

6.4 Содержание и объем обрабатываемых персональных данных соответствует заявленным целям обработки. Обрабатываемые персональные данные не являются избыточными по отношению к заявленным целям их обработки.

6.5 При обработке персональных данных в ФБУЗ «МСЧ № 52» ФМБА России обеспечивается точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор обеспечивает принятие необходимых мер по удалению или уточнению неполных или неточных данных.

6.6 Хранение персональных данных в ФБУЗ «МСЧ № 52» ФМБА России осуществляется в форме, позволяющей определить субъекта персональных данных и на срок, которого требуют цели обработки персональных данных, если срок хранения не установлен федеральным законом, приказами вышестоящих организаций, договором стороной, которого является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

7. Способы обработки персональных данных

7.1 ФБУЗ «МСЧ № 52» ФМБА России осуществляет обработку персональных данных следующими путями: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

7.2 При обработке используется смешанный способ обработки персональных данных:

-неавтоматизированным способом обработки персональных данных;

-автоматизированным способом обработки персональных данных (с помощью ПЭВМ и программных продуктов)

7.3 Трансграничной передачи персональных данных ФБУЗ «МСЧ № 52» ФМБА России не осуществляется.

8. Цели и задачи обеспечения безопасности персональных данных

8.1 Субъекты информационных отношений заинтересованы в обеспечении:
- своевременного доступа к необходимым им персональным данным (их доступности);
- достоверности (полноты, точности, адекватности, целостности) персональных данных;
- конфиденциальности (сохранения в тайне) персональных данных;
- защиты от навязывания им ложных (недостоверных, искаженных) персональных данных;
- разграничения ответственности за нарушение их прав (интересов) и установления правил обращения с персональными данными;
- защиты персональных данных от незаконного распространения.

8.2 Основной целью, на достижение которой направлены все статьи настоящей Политики, является защита субъектов информационных отношений ФБУЗ «МСЧ № 52» ФМБА России от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на персональные данные, их носители, процессы обработки и передачи.

Указанная цель достигается посредством обеспечения и постоянного поддержания следующих действий с персональными данными:

- доступность персональных данных для легальных пользователей, которые в свою очередь имеют возможность получения необходимых персональных данных и результатов решения задач за приемлемое для них время);

- целостности и конфиденциальности персональных данных, хранимых и обрабатываемых в информационных системах и передаваемых по каналам связи;

8.3 Для достижения основной цели защиты и обеспечения указанных действий с персональными данными информационная система обеспечивает решение следующих задач:

- своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба заинтересованным субъектам;

- создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;

- защиту от вмешательства в процесс функционирования информационных систем посторонних лиц (доступ к информационным ресурсам имеют только зарегистрированные в установленном порядке пользователи);

- разграничение доступа пользователей к информационным, аппаратным, программным ресурсам ФБУЗ «МСЧ № 52» ФМБА России (возможность доступа только к тем ресурсам и выполнение только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей), то есть защиты от несанкционированного доступа;

- обеспечение подтверждения подлинности отправителя и получателя информации;

- защита системы от внедрения несанкционированных программ, включая компьютерные вирусы;

- защита информации ограниченного пользования от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

8.4 Поставленные основные цели защиты и решение выше перечисленных задач достигаются:

- учетом всех подлежащих защите ресурсов информационных систем;

- четким знанием, выполнением и соблюдением всеми пользователями требований организационно-распорядительных документов по вопросам обеспечения безопасности информации;

- проведением инструктажа с сотрудниками, назначенными ответственными за процессы обработки персональных данных в подразделениях;

- наделением каждого сотрудника (пользователя) минимально необходимым для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам;

- персональной ответственностью за свои действия каждого сотрудника, в рамках своих функциональных обязанностей имеющего доступ к информационным ресурсам и обеспечивающего несанкционированный доступ к ним третьих лиц;

- поддержанием необходимого уровня защищенности элементов информационной системы ФБУЗ «МСЧ № 52» ФМБА России;

- контролем за соблюдением пользователями информационных ресурсов, требований по обеспечению безопасности информации;

- юридической защитой интересов при взаимодействии с внешними организациями от противоправных действий, как со стороны этих организаций, так и от несанкционированных действий обслуживающего персонала и третьих лиц.

При передаче персональных данных Субъектов сотрудники, имеющие доступ к персональным данным, соблюдают следующие требования:

- не разглашать персональные данные Субъекта третьей стороне без письменного согласия Субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью Субъекта, а также в других случаях, предусмотренных Трудовым кодексом РФ или иными федеральными законами.

9. Основные принципы построения системы безопасности

Построение всей системы безопасности персональных данных в ФБУЗ «МСЧ № 52» ФМБА России и ее функционирование должны осуществляться в соответствии со следующими принципами:

9.1 Законность обработки персональных данных в соответствии с действующим законодательством в области защиты персональных данных, а также других законодательных актов по безопасности информации РФ. Принятые меры не должны препятствовать доступу правоохранительных органов в предусмотренных законодательством случаях.

Все сотрудники, имеющие доступ к персональным данным должны иметь представление об ответственности за правонарушения в области обработки персональных данных.

9.2 Системный подход к построению системы защиты информации в ФБУЗ «МСЧ № 52» ФМБА России предполагает учет всех взаимосвязанных, взаимодействующих условий и факторов, для решения проблемы обеспечения безопасности персональных данных. При создании системы безопасности должны учитываться более уязвимые места утечки данных.

9.3 Комплексное использование методов и средств защиты компьютерных систем предполагает согласованное применение разнородных средств при построении целостной системы защит. Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами.

9.4 Обеспечение безопасности персональных данных- процесс осуществляемый руководством ФБУЗ «МСЧ № 52» ФМБА России, ответственным за организацию обработки персональных данных и сотрудниками всех уровней, которые принимают участие в этом процессе. Кроме того большинству физических и технических средств защиты для эффективного выполнения своих функций оказывается необходимая постоянная поддержка (своевременная смена паролей, имен, переопределение полномочий и т.п.)

9.5 Предполагается постоянное совершенствование системы мер защиты персональных данных, на основе организационных и технических решений, кадрового состава, анализа функционирования информационных систем с учетом нормативных требований по защите, пока персональные данные находятся в обращении, поэтому принимаемые меры помогут снизить вероятность негативных воздействий или ущерб от них.

9.6 Персональная ответственность предполагает возложение ответственности за обеспечение безопасности персональных данных и системы их обработки на каждого сотрудника, в пределах его полномочий. В соответствии с этим, распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен и (или)сведен к минимуму.

9.7 Минимизация полномочий, означает предоставление пользователям минимальных прав доступа к соответствии со служебной необходимостью. Доступ к персональным данным должен предоставляться только в том случае и объеме, если это необходимо сотруднику для выполнение его должностных обязанностей. Для снижение риска манипулирования персональными данными и риска хищения, такие полномочия должны быть в максимально возможной степени разделены между различными сотрудниками или подразделениями ФБУЗ «МСЧ № 52» ФМБА России.

9.8 Важным элементом эффективной системы обеспечения безопасности персональных данных в ФБУЗ «МСЧ № 52» ФМБА России является высокая культура работы с информацией. Руководство ФБУЗ «МСЧ № 52» ФМБА России несет ответственность за строгое соблюдение этических норм и стандартов профессиональной деятельности. Все сотрудники должны понимать свою роль в обеспечении информационной безопасности и принимать участие в этом процессе, при работе с любой конфиденциальной информацией. Все это создает больше возможностей для обнаружения фактов ее нарушения.

9.9 Обязательность контроля, предполагает своевременность выявления и пресечения попыток нарушения установленных правил, обеспечения безопасности персональных данных.

Контроль за деятельность любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляется на основе применения средств оперативного контроля и регистрации, а также должен охватывать как несанкционированные, так и санкционированные действия пользователей.

Недостатки системы обеспечения информационной безопасности, выявленные сотрудниками, должны немедленно доводятся до сведения руководителя ФБУЗ «МСЧ № 52» ФМБА России и оперативно устраняются.

10. Методы, меры и средства обеспечения уровня защиты персональных данных

Документальное обеспечение:

- Положение об обработке персональных данных, осуществляемых без использования средств автоматизации, утвержденное постановлением Правительства Российской Федерации от 15.09.2008г. № 687.
- Постановление Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при обработке в информационных системах персональных данных».
- Инструкция пользователя информационной системы персональных данных ФБУЗ «МСЧ № 52» ФМБА России.
- Положение по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в ФБУЗ «МСЧ № 52» ФМБА России, утвержденное приказом начальника учреждения.
- Положение о порядке обработки персональных данных без использования средств автоматизации в ФБУЗ «МСЧ № 52» ФМБА России, утвержденное приказом начальника учреждения.
- Инструкция администратора безопасности информационных систем персональных данных в ФБУЗ « МСЧ № 52» ФМБА России утвержденная приказом начальника учреждения.
- Положение о защите персональных данных в ФБУЗ «МСЧ № 52» ФМБА России, утвержденное приказом начальника учреждения..

- Приказ Минздрава России от 29.06.2016г. № 425н «Об утверждении Порядка ознакомления пациента либо его законного представителя с медицинской документацией, отражающей состояние здоровья пациента».

- Перечень сведений конфиденциального характера в ФБУЗ «МСЧ № 52» ФМБА России, утвержденный приказом начальника от 08.08.2016г. № 279.

10.1 ФБУЗ «МСЧ № 52» ФМБА России при защите персональных данных Субъектов принимает все необходимые меры:

- правовые (законодательные), включающие в себя законы, указы и нормативные акты, регламентирующие правила обращения с персональными данными, а также устанавливающие ответственность за нарушение этих правил;

- морально-этические нормы поведения, которые традиционно сложились или складываются по мере распространения информационных технологий. Они не являются обязательными, но их не соблюдение может привести к падению авторитета, престижа человека, группы лиц или ФБУЗ «МСЧ № 52» ФМБА России в целом;

- технологические меры защиты основанные на использовании и направлении уменьшения возможности совершения сотрудниками ошибок и нарушений в рамках предоставления им прав и полномочий;

- организационные (административные) меры защиты регламентирующие процессы функционирования системы обработки персональных данных, использование ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить и (или) исключить возможность реализации угроз безопасности и (или) снизить размер потерь в случае их реализации;

10.2 Главная цель мер по обеспечению безопасности, предпринимаемых на высшем управленческом уровне - это сформированная политика в области обеспечения безопасности персональных данных, которая очерчивает сферу влияния и ограничения при определении целей безопасности персональных данных в ФБУЗ «МСЧ № 52» ФМБА России в целом и обеспечение ее выполнения.

Для сотрудников политика в области персональных данных должна определять процедуры и правила достижения целей и решения задач безопасности персональных данных:

- роли и обязанности должностных лиц, отвечающих за проведение политики безопасности персональных данных;

- права доступа к персональным данным, кто и при каких условиях может читать и модифицировать персональные данные;

- регламента информационных отношений, исключающих возможность произвольных или несанкционированных действий в отношении информационных ресурсов;

- разграничение доступа к персональным данным;

10.3 Информационные системы ФБУЗ «МСЧ № 52» ФМБА России, размещаются в помещениях, находящихся под сигнализацией или наблюдением и должны исключать возможность бесконтрольного проникновения в помещения посторонних лиц, и обеспечивать физическую сохранность находящихся в помещении защищаемых ресурсов.

По окончании рабочего дня, помещения, в которых размещаются компоненты информационных систем ФБУЗ «МСЧ № 52» ФМБА России, должны запираться на ключ, а помещения оснащенные средствами охранной сигнализации, а также автоматизированной системой приема и регистрации сигналов от этих средств, сдаются под охрану.

10.4 Допуск пользователей к работе с информационными системами ФБУЗ «МСЧ № 52» ФМБА России должен быть регламентирован. Любые изменения состава и полномочий пользователей должны производиться в установленном порядке.

Расширение прав доступа и предоставление доступа к дополнительным ресурсам, должно определяться руководителями подразделений, а также в обязательном порядке, согласовываться с ответственным за организацию обработки и защиты персональных данных в учреждении.

10.5 Каждый сотрудник должен пользоваться только той информацией, которая необходима ему по роду своей деятельности в соответствии с его должностными обязанностями.

10.6 Пользователи информационных систем ФБУЗ МСЧ № 52» ФМБА России, а также руководящий состав должны быть ознакомлены со своим уровнем полномочий, а также с организационно- распорядительной, нормативной, технической документацией, определяющей требования и порядок обработки персональных данных в ФБУЗ «МСЧ № 52» ФМБА России. Должны знать и неукоснительно выполнять инструкции и знать общие обязанности по обеспечению безопасности персональных данных. Доведение требований указанных документов до лиц, допущенных к обработке защищаемых персональных данных, должно осуществляться под роспись.

10.7 Мера ответственности персонала за действия, совершенные в нарушении установленных правил обеспечения безопасной работы с персональными данными, должна определяться нанесенным ущербом, наличием злого умысла и другими фак торами по усмотрению руководства ФБУЗ «МСЧ № 52» ФМБА России

Для реализации принципа персональной ответственности пользователей за свои действия необходимы:

-индивидуальная идентификация пользователей;

- проверка подлинности пользователей на основе паролей;

- реакция на попытки несанкционированного доступа (блокировка и т.д).

10.8 Для обеспечения информационной безопасности ФБУЗ «МСЧ № 52» ФМБА России должны использоваться следующие средства защиты:

10.8.1 Физические меры защиты основаны на применении разного рода механических, предназначенных для создания физических препятствий от проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемым персональным данным, а также технических средств визуального наблюдения, связи и охранной сигнализации. Введение дополнительных ограничений по доступу в помещения, предназначенные для хранения и обработки персональных данных.

10.8.2 Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ выполняющих функцию защиты.

В состав системы защиты должны быть включены следующие средства:

- разграничение доступа к данным;

- средства регистрации доступа к информационным системам и контролем за использованием информации;

- средства реагирования на нарушения режима информационной безопасности.

На технические средства возлагается решение следующих задач:

- идентификация пользователей;

- регламентация и управления доступом в помещения, где ведется обработка персональных данных;

- защита от проникновения компьютерных вирусов и разрушительного действия вредоносных программ;

- регистрация всех действий пользователя в защищенном журнале;

10.8.3 В целях предотвращения работы с ресурсами посторонних лиц необходимо обеспечить возможность распознавания каждого легального пользователя (или групп пользователей). Подтверждение подлинности пользователей может осуществляться путем проверки знания ими паролей.

10.8.4 Зоны ответственности по средствам разграничения доступа должны быть составной частью единой системы контроля доступа:

- на контролируемую территории;

- на отдельные помещения;

- к компонентам информационной среды ФБУЗ «МСЧ № 52» ФМБА России (физический доступ);

- к информационным ресурсам (документам, носителям информации, файлам, архивам и т.д);

- к активным ресурсам программам, задачам и т.п);

- к операционной системе, системным программам, задачам и т.п).

10.8.5 Средства обеспечения целостности включают в себя средства резервного копирования, программы антивирусной защиты, программы восстановления целостности операционной среды и баз данных. Контроль целостности информации и средства защиты, должен обеспечиваться:

- средствами разграничения доступа (в помещения, к документам, к носителям информации, к серверам и т.п);

- средствами электронной подписи;

10.8.6 Средства оперативного контроля и регистрации событий безопасности (действий пользователей, попыток НСД) позволяют выявить факты нарушений, их характер, подсказать методы его расследования, способы исправления ситуации. Средства контроля должны предоставлять возможность:

- ведения и анализа журналов регистрации событий безопасности (системных журналов);

-оперативного оповещения руководителя учреждения и ответственного за организацию обработки и защиты персональных данных о нарушениях.

При регистрации событий безопасности в журнале должна фиксироваться следующая информация:

-дата и время события;

-идентификатор субъекта, осуществляющего регистрируемое действие;

- действие (тип доступа).

10.9 Контроль эффективности защиты персональных данных осуществляется с целью своевременного выявления и предотвращения утечки персональных данных за счет несанкционированного доступа, а также предупреждения возможных специальных воздействий, направленных на уничтожение персональных данных. Оценка эффективности мер защиты персональных данных проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

11. Права и обязанности Субъекта персональных данных

11.1 Субъект персональных данных имеет право:

- требовать уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

- получать информацию о сроках обработки своих персональных данных, в том числе о сроках их хранения.

- требовать информирования всех субъектов, которым ранее были сообщены неверные или неполные его персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях;

- на доступ к своим персональным данным и на получение информации, касающейся обработки его персональных данных, по запросу субъекта персональных данных учреждение предоставляет информацию предусмотренную Федеральным законами: «Персональных данных от 27.07.2006 № 152-ФЗ, от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» и другими федеральными актами и законами.

Запрос должен содержать ФИО субъекта или его законного представителя, номер документа удостоверяющего личность субъекта персональных данных или его законного представителя, дата выдачи документа, с указанием запрашиваемой информации, а также с указанием цели запроса.

Предоставление персональных данных субъекта, его законному представителю (определение статуса законного представителя в соответствии с Федеральными законами и ст. Гражданского и Семейного Кодексов), также осуществляется на основании запроса, в котором необходимо указать ФИО лица, на которое делается запрос, с обязательным указанием степени родства.

- обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия при обработке его персональных данных.

11.2 Обязанности Субъекта персональных данных:
- предоставить ФБУЗ «МСЧ № 52» ФМБА России достоверные персональные данные;
- оформить соглашение на обработку персональных данных;
- правильно оформить запрос, для получения информации по персональным данным.

12. Права и обязанности Учреждения

ФБУЗ «МСЧ № 52» ФМБА России обязано:

- соблюдать федеральное законодательство в части защиты персональных данных в соответствии с действующим законодательством.
- неукоснительно следовать заявленной политике и добиваться понимания всеми работниками своей роли и места в обеспечении поставленных целей, задач и принципов.
- в случае отказа Субъекта в предоставлении персональных данных ФБУЗ «МСЧ № 52» ФМБА России:

– пациентам оказывается только неотложная медицинская помощь;

– претенденту на должность ФБУЗ «МСЧ № 52» ФМБА России отказывает в приеме на работу.

13. Ответственность

Лица, виновные в нарушении требований Федерального закона № 152-ФЗ «О персональных данных», несут персональную ответственность, предусмотренную законодательством Российской Федерации.

Лицо, ответственное за организацию обработки, защиты персональных данных и контроль за ПДн в ФБУЗ «МСЧ № 52» ФМБА России -инженер по режиму, телефон (83361) 4 – 07 – 81.