УТВЕРЖДАЮ

Главный врач
ГБУЗ ПК «ССМП г. Березники»

_____ А.Б. Соседков

«19» 02 2015 г.

Политика информационной безопасности информационных систем персональных данных Государственного бюджетного учреждения здравоохранения Пермского края «Станция скорой медицинской помощи г. Березники»

На 23 листах

Березники
2015 г.

СОДЕРЖАНИЕ

ОПРЕДЕЛЕНИЯ

В настоящем документе используются следующие термины и их определения.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Биометрические персональные данные – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются для установления личности субъекта персональных данных.

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Доступ к информации – возможность получения информации и ее использования.

Доступность информации – состояние информации, характеризуемое способностью информационной системы обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе персональных данных.

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

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Инцидент информационной безопасности – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

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

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

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.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Событие информационной безопасности - идентифицированное возникновение состояния информационной системы, указывающее на возможное нарушение политики информационной безопасности, отказ защитных мер, а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Средство защиты информации – техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

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

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Целостность информации – способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АРМ	– автоматизированное рабочее место;
ИСПДн	– информационная система персональных данных;
НСД	– несанкционированный доступ;
ОС	– операционная система;
ПДн	– персональные данные;
ПО	– программное обеспечение;
СЗИ	– средства защиты информации;
СЗПДн	– система (подсистема) защиты персональных данных;
УБПДн	– угрозы безопасности персональных данных

ВВЕДЕНИЕ

Настоящая Политика информационной безопасности информационных систем персональных данных (далее – Политика) государственного бюджетного учреждения здравоохранения Пермского края «Станция скорой медицинской помощи г. Березники» (далее – Учреждение) определяет основные цели, задачи и принципы построения системы защиты персональных данных (далее – СЗПДн) в Учреждении.

Политика разработана в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Политика регламентирует организацию защиты персональных данных (далее – ПДн) при их обработке в информационных системах персональных данных (далее – ИСПДн) Учреждения. В Политике определены структура и требования к построению системы защиты персональных данных, порядок предоставления доступа к ИСПДн, требования к работникам по обеспечению безопасности ПДн, а также ответственность за нарушение требований по безопасности ПДн в ИСПДн Учреждения.

Требования настоящей Политики распространяются на всех работников Учреждения (штатных, временных, работающих по контракту и т.п.), а также всех третьих лиц, допущенных к ИСПДн Учреждения (подрядчики, аудиторы и т.п.).

Ответственным за контроль исполнения данной Политики, а также за её своевременное изменение и обновление является лицо, назначенное ответственным за организацию обработки персональных данных в Учреждении.

1 Общие положения

Безопасность персональных данных достигается путем принятия необходимых правовых, организационных и технических мер с целью исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иных неправомерных действий с персональными данными.

Мероприятия по защите персональных данных являются неотъемлемой частью управленческой и иной деятельности Учреждения.

Целью проведения мероприятий по защите персональных данных является:

– обеспечение безопасности объектов защиты Учреждения от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности персональных данных (далее – УБПДн);

– выполнение требований по безопасности персональных данных при их обработке в ИСПДн, регламентируемых законодательством Российской Федерации в области защиты ПДн, а также государственными стандартами, руководящими и нормативно-методическими документами ФСТЭК и ФСБ России.

Безопасность персональных данных при их обработке в ИСПДн обеспечивается с помощью системы защиты персональных данных, которая представляет собой совокупность организационных и технических мероприятий для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также иных неправомерных действий с ними.

Структура, состав и основные функции СЗПДн определяются исходя из перечня актуальных угроз безопасности персональных данных и информационных технологий, используемых в ИСПДн.

СЗПДн включает организационные меры и технические средства защиты информации, а также используемые в информационной системе информационные технологии. Организационные меры предусматривают создание и поддержание правовой базы безопасности ПДн и разработку (введение в действие) внутренних организационно-распорядительных документов. Технические меры защиты реализуются при помощи соответствующих программных и аппаратных средств и методов защиты.

2 Цели и задачи СЗПДн

Основной целью СЗПДн является защита интересов субъектов персональных данных, а также минимизация ущерба от возможной реализации угроз безопасности ПДн.

Для достижения основной цели система защиты ПДн ИСПДн должна обеспечивать эффективное решение следующих задач:

– защиту от вмешательства в процесс функционирования ИСПДн посторонних лиц (возможность использования ИСПДн и доступ к ее ресурсам должны иметь только зарегистрированные установленным порядком пользователи);

– разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам ИСПДн (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям ИСПДн для выполнения своих служебных (трудовых) обязанностей), то есть защиту от несанкционированного доступа к:

- обрабатываемой в ИСПДн информации, содержащей ПДн,
- средствам вычислительной техники ИСПДн,
- техническим средствам защиты, используемым в ИСПДн;

– регистрацию действий пользователей при использовании защищаемых ресурсов ИСПДн в системных журналах и периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов;

– защиту ПДн, хранимых, обрабатываемых и передаваемых по каналам связи, от несанкционированного разглашения или искажения;

– создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности ПДн.

Достижение поставленных целей и решение перечисленных задач защиты достигается за счет:

– применения физических и технических (программных или программно-аппаратных) средств защиты ресурсов ИСПДн Учреждения и непрерывной административной поддержкой их использования;

– регламентацией процессов обработки персональных данных с применением технических средств (действий работников структурных подразделений Учреждения, использующих ИСПДн, а также действий персонала, осуществляющего обслуживание и модификацию технических средств ИСПДн);

– предупреждением попадания ПДн на носители и файлы, доступ к которым не разграничивается, а также запретом передачи ПДн по незащищенным каналам связи;

– полнотой, реальной выполнимостью и непротиворечивостью требований организационно-распорядительных документов Учреждения по вопросам защиты персональных данных в ИСПДн Учреждения;

– назначением лиц, ответственных за обеспечение безопасности персональных данных, осуществление технической и криптографической защиты информации;

– подготовкой работников Учреждения, обеспечивающих защиту информации в ИСПДн;

– наделением каждого пользователя (работника Учреждения) полномочиями по доступу к ресурсам ИСПДн на минимально необходимый для выполнения функциональных обязанностей срок;

– четким знанием и строгим соблюдением всеми работниками, использующими и обслуживающими технические и программные средства ИСПДн, требований организационно-распорядительных документов Учреждения по вопросам защиты информации и персональных данных;

– персональной ответственностью лиц, участвующих в информационном обмене в ИСПДн, за полноту и достоверность сведений, их своевременную передачу и изменение, а также хранение и уничтожение в установленном порядке;

– строгим учетом всех подлежащих защите ресурсов ИСПДн (носителей информации, программных средств, серверов, АРМ и т.д.);

– постоянным контролем за соблюдением пользователями ИСПДн (работниками Учреждения) требований по обеспечению безопасности персональных данных при их обработке в ИСПДн;

– применением сертифицированных ФСТЭК и ФСБ России средств технической и криптографической защиты информации;

– юридической защитой интересов Учреждения при взаимодействии с внешними организациями (связанном с передачей персональных данных) от противоправных воздействий, как со стороны этих организаций, так и со стороны обслуживающего персонала и третьих лиц;

– проведением постоянного анализа эффективности и достаточности применяемых мер и средств защиты информации, разработкой и реализацией предложений по совершенствованию СЗПДн при развитии ИСПДн.

3 Основные принципы построения системы защиты персональных данных

Построение системы защиты персональных данных ИСПДн Учреждения и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

- законность;
- системность;
- комплексность;
- непрерывность;
- своевременность;
- преемственность и непрерывность совершенствования;
- персональная ответственность;
- минимизация полномочий;
- взаимодействие и сотрудничество;
- гибкость системы защиты;
- открытость алгоритмов и механизмов защиты;
- простота применения средств защиты;
- научная обоснованность и техническая реализуемость;
- специализация и профессионализм;
- обязательность контроля.

3.1 Законность

Предполагает осуществление защитных мероприятий и разработку СЗПДн Учреждения в соответствии с действующим законодательством в области защиты ПДн и других нормативных актов по безопасности ПДн, утвержденных органами государственной власти и управления в пределах их компетенции.

Пользователи и обслуживающий персонал ИСПДн Учреждения должны быть осведомлены о порядке работы с ИСПДн и об ответственности за нарушение порядка работы с ИСПДн.

3.2 Системность

Системный подход к построению СЗПДн Учреждения предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности ИСПДн Учреждения.

При создании системы защиты должны учитываться все слабые и наиболее уязвимые места системы обработки ПДн, а также характер, возможные объекты и направления атак на систему со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения нарушителей в систему и способы НСД к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и способов НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

3.3 Комплексность

Комплексное использование методов и средств защиты предполагает согласованное применение разнородных средств при построении целостной системы

защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов.

Защита должна строиться эшелонировано. Для каждого канала утечки информации и для каждой угрозы безопасности должно существовать несколько защитных рубежей. Создание защитных рубежей осуществляется с учетом того, чтобы для их преодоления потенциальному злоумышленнику требовались профессиональные навыки в нескольких невзаимосвязанных областях.

Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами.

3.4 Непрерывность защиты ПДн

Защита ПДн – не разовое мероприятие и не простая совокупность проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИСПДн.

ИСПДн должны находиться в защищенном состоянии на протяжении всего времени их функционирования. В соответствии с этим принципом должны приниматься меры по недопущению перехода ИСПДн в незащищенное состояние.

Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная техническая и организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных «закладок» и других средств преодоления системы защиты после восстановления ее функционирования.

3.5 Своевременность

Предполагает упреждающий характер мер обеспечения безопасности ПДн, то есть постановку задач по комплексной защите ИСПДн и реализацию мер обеспечения безопасности ПДн на ранних стадиях разработки ИСПДн в целом и ее СЗПДн, в частности.

Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы.

3.6 Преемственность и совершенствование

Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования ИСПДн и ее системы защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

3.7 Персональная ответственность

Предполагает возложение ответственности за обеспечение безопасности ПДн и системы их обработки на каждого работника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей работников строится таким образом,

чтобы в случае любого нарушения круг ответственных лиц был четко известен или сведен к минимуму.

3.8 Принцип минимизации полномочий

Означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью, на основе принципа «все, что не разрешено, запрещено».

Доступ к ПДн должен предоставляться только в том случае и в том объеме, в котором это необходимо работнику для выполнения его должностных обязанностей.

3.9 Взаимодействие и сотрудничество

Предполагает создание благоприятной атмосферы в коллективе, обеспечивающих функционирование ИСПДн Учреждения, для снижения вероятности возникновения негативных действий связанных с человеческим фактором.

В такой обстановке работники должны осознанно соблюдать установленные правила и оказывать содействие в деятельности подразделений обеспечивающих функционирование ИСПДн.

3.10 Гибкость системы защиты ПДн

Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности, средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса ее нормального функционирования.

3.11 Открытость алгоритмов и механизмов защиты

Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже авторам). Однако это не означает, что информация о конкретной системе защиты должна быть общедоступна.

3.12 Простота применения средств защиты

Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных установленным порядком пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.).

Должна достигаться автоматизация максимального числа действий пользователей и администраторов ИСПДн.

3.13 Научная обоснованность и техническая реализуемость

Информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, научно обоснованы с точки зрения достижения заданного уровня безопасности ПДн и должны соответствовать установленным нормам и требованиям по безопасности ПДн.

СЗПДн должна быть ориентирована на решения, возможные риски для которых и меры противодействия этим рискам прошли всестороннюю теоретическую и практическую проверку.

3.14 Специализация и профессионализм

Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности ПДн, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными специалистами Учреждения.

3.15 Обязательность контроля

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности ПДн на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств.

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

4 Система защиты персональных данных

Система защиты персональных данных (далее – СЗПДн) в Учреждении строится на основании следующих документов:

- Результатов обследования ИСПДн, полученных в ходе внутренней проверки и отраженных в Отчете о результатах проведения внутренней проверки, или полученных в ходе работы сторонней организации и отраженных в Актах обследования ИСПДн этой организации;
- Перечня персональных данных, подлежащих защите в ИСПДн Учреждения;
- Актов определения уровня защищенности ПДн при их обработке в ИСПДн;
- Частных моделей угроз безопасности ПДн при их обработке в ИСПДн;
- Технических заданий на разработку СЗПДн ИСПДн;
- Технического проекта на создание СЗПДн ИСПДн.

На базе вышеназванных документов определяется необходимый уровень защищенности ПДн в ИСПДн Учреждения. На основе исходных данных, полученных в ходе обследования ИСПДн, актуальных угроз безопасности ПДн, определённых Частными моделями угроз, и требований к системе защиты ПДн, изложенных в Технических заданиях, делается заключение о необходимых для обеспечения безопасности ПДн средствах защиты информации (далее – СЗИ) и организационных мероприятиях.

Выбранные необходимые мероприятия и перечень предполагаемых к использованию средств защиты информации отражаются в Техническом проекте на создание СЗПДн ИСПДн.

Кроме того, на ИСПДн должен быть составлен Технический паспорт, содержащий описание структуры и топологии ИСПДн, список технических и программных средств ИСПДн и используемых средств защиты информации для всех элементов ИСПДн.

Технический паспорт должен поддерживаться в актуальном состоянии. При изменении состава технических и программных средств ИСПДн соответствующие изменения должны быть внесены в Технический паспорт.

5 Структура системы защиты персональных данных

Система защиты персональных данных – это не только совокупность организационных и технических мероприятий, но и объекты защиты, а также те ответственные лица, которые обеспечивают проведение мероприятий по обеспечению безопасности персональных данных.

Организация и функционирование вышеназванных составных элементов СЗПДн регламентируется правилами и нормами, установленными организационно-распорядительными документами Учреждения по вопросам обработки и защиты ПДн.

Объектом защиты является не только обрабатываемая в ИСПДн информация, содержащая ПДн, также к объектам защиты относится:

- технологическая информация ИСПДн;
- технические средства обработки ПДн (средства вычислительной техники ИСПДн);
- технические средства защиты ПДн;
- объекты и помещения, в которых размещены компоненты ИСПДн.

Принятие необходимых организационных и технических мер по обеспечению безопасности персональных данных обеспечивают:

- ответственный за организацию обработки персональных данных в Учреждении;
- администратор ИСПДн.

Указанные лица назначаются руководителем Учреждения.

Обязанности и права ответственного за организацию обработки персональных данных в Учреждении и администратора ИСПДн определяются соответствующими инструкциями, утвержденными в Учреждении.

6 Требования к системе защиты персональных данных

Структура, состав и основные функции СЗПДн определяются исходя из установленного уровня защищенности ПДн при их обработке в ИСПДн и перечня актуальных угроз безопасности ПДн при их обработке в ИСПДн. Соответственно разработка СЗПДн проводится на основе результатов обследования ИСПДн, актов определения уровня защищенности ПДн при их обработке в ИСПДн и частных моделей угроз безопасности ПДн при их обработке в ИСПДн.

СЗПДн должна обеспечивать безопасность ПДн при обработке в ИСПДн согласно «Составу и содержанию организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденному приказом ФСТЭК России от 18 февраля 2013 года №21 по установленному уровню защищенности.

В состав организационных и технических мер по обеспечению безопасности персональных данных входят:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- защита машинных носителей персональных данных;
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности персональных данных;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных.

Состав и содержание мер по обеспечению безопасности ПДн:

6.1 Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

6.2 Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль за соблюдением этих правил.

6.3 Меры по защите машинных носителей персональных данных (средств обработки (хранения) персональных данных, съемных машинных носителей персональных данных) должны исключать возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированное использование съемных машинных носителей персональных данных.

6.4 Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

6.5 Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

6.6 Меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) персональные данные в целях добывания, уничтожения, искажения и блокирования доступа к персональным данным, а также реагирование на эти действия.

6.7 Меры по контролю (анализу) защищенности персональных данных должны обеспечивать контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных.

6.8 Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту персональных данных, представленных в виде информативных электрических сигналов и физических полей.

6.9 Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных.

7 Контроль эффективности СЗПДн Общества

Контроль эффективности СЗПДн должен осуществляться на периодической основе, не реже 1 раза в 3 года, в том числе до ввода в эксплуатацию ИСПДн. Целью контроля эффективности является своевременное выявление ненадлежащих режимов работы СЗПДн (отключение средств защиты, нарушение режимов защиты, несанкционированное изменение режима защиты и т.п.), контроль соблюдения требований по обеспечению безопасности ПДн (требований законодательства в области защиты ПДн, требований внутренних нормативно-методических и организационно-распорядительных документов Учреждения), а также прогнозирование и превентивное реагирование на новые угрозы безопасности ПДн.

Контроль может проводиться Учреждением как самостоятельно (например, оперативный контроль администраторами ИСПДн в процессе информационного взаимодействия в ИСПДн), так и с привлечением для этой цели на договорной основе компетентных организаций, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Государственный контроль осуществляется Роскомнадзором, при этом могут привлекаться иные госорганы в пределах их полномочий (ФСТЭК России, ФСБ России, правоохранительные органы).

Оценка эффективности мер защиты ПДн проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям. Контроль может осуществляться как с помощью штатных средств системы защиты ПДн, так и с помощью специальных программных средств контроля.

Решение по форме оценки эффективности и документов, разрабатываемых по результатам (в процессе) оценки эффективности, принимается оператором самостоятельно и (или) по соглашению с организацией, привлекаемой для проведения оценки эффективности реализованных мер по обеспечению безопасности ПДн.

Оценка эффективности реализованных мер может быть проведена в рамках работ по аттестации ИСПДн в соответствии с ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения».

8 Сферы ответственности за безопасность ПДн

Общую организацию обработки и защиты персональных данных работников осуществляет лицо, назначенное руководителем Учреждения ответственным за организацию обработки персональных данных в Учреждении.

Ответственный за организацию обработки персональных данных в Учреждении обеспечивает:

– доведение до сведения работников Учреждения положений законодательства РФ о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

– общий контроль за соблюдением Учреждением и его работниками законодательства РФ о персональных данных, в том числе требований к защите персональных данных;

– прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) контроль за приемом и обработкой таких обращений и запросов.

Организацию и контроль за обработкой и защитой персональных данных работников в структурных подразделениях Учреждения, работники которых имеют доступ к персональным данным, осуществляют их непосредственные руководители.

Кроме того, в обязанности Ответственного за организацию обработки персональных данных в Учреждении входят следующие направления обеспечения безопасности ПДн:

– планирование и реализация мер по обеспечению безопасности ПДн;

– анализ угроз безопасности ПДн;

– разработка, внедрение, контроль исполнения и поддержание в актуальном состоянии политики, положений, инструкций и других организационных документов по обеспечению безопасности;

– контроль защищенности ИТ-инфраструктуры Учреждения от УБПДн;

– обучение и информирование пользователей ИСПДн, о порядке работы с ПДн и средствами защиты;

– предотвращение, выявление, реагирование и расследование нарушений безопасности ПДн.

Ответственный за организацию обработки персональных данных в Учреждении может делегировать часть полномочий по обеспечению безопасности персональных данных, не входящих в его профессиональную компетенцию, иным структурным подразделениям Учреждения, либо привлечь на договорной основе организацию, имеющую лицензию на деятельность по технической защите конфиденциальной информации.

Администратор ИСПДн осуществляет сопровождение СЗПДн ИСПДн, обеспечивает функционирование подсистем управления доступом, регистрации и учёта, обеспечения целостности, антивирусной защиты и других подсистем СЗПДн, выявляет попытки и факты НСД к информации

9 Доступ к информационным системам персональных данных

В Учреждении устанавливается разрешительная система доступа к обработке персональных данных в ИСПДн, а также к администрированию, техническому обслуживанию, сопровождению и другим работам с ИСПДн.

Пользователям ИСПДн в соответствии с принципом минимизации полномочий устанавливаются права доступа к элементам ИСПДн. Перечень пользователей ИСПДн утверждается Приказом.

Приказом об утверждении списка лиц, которым необходим доступ к ПДн, обрабатываемым в ИСПДн, для выполнения служебных (трудовых) обязанностей, должны быть заданы:

- ИСПДн, к которой допущено лицо;
- виды работ, которые может производить допущенное лицо;

При взаимодействии со сторонними организациями в случаях, когда работникам этих организаций предоставляется доступ к объектам защиты, с этими организациями должно быть заключено «Соглашение о конфиденциальности», содержащее требования соблюдения конфиденциальности ПДн и режима их безопасности при выполнении работ в ИСПДн сторонней организацией. Допускается пункты о соблюдении требований по безопасности ПДн включать непосредственно в договора. Подготовка проекта «Соглашения о конфиденциальности» осуществляется при обязательном участии юриста Учреждения.

Доступ к ИСПДн представителей сторонних организаций (третьих лиц), выполняющих работу по договору, предоставляется на основании приказа руководителя Учреждения. Приказом должны быть заданы: часть ИСПДн, к которой допущено лицо; виды работ, которые может производить допущенное лицо; срок действия допуска.

Лица, получившие допуск к ИСПДн, должны быть ознакомлены с положениями законодательства Российской Федерации о персональных данных, требованиями к защите персональных данных и организационно-распорядительными документами Учреждения по вопросам обработки и защиты ПДн, а также пройти обязательный первичный инструктаж по соблюдению режима конфиденциальности персональных данных при работе с ИСПДн.

Допуск к ИСПДн аннулируется, а доступ незамедлительно прекращается в случае изменения статуса допущенного лица (перевод на другую должность, увольнение, изменение должностных обязанностей и т.п.). За своевременное предоставление информации об изменении статуса допущенного лица ответственному за организацию обработки персональных данных в Учреждении и администратору ИСПДн отвечают сами допущенные лица, а также их непосредственные начальники.

За организацию разрешительной системы доступа к ИСПДн отвечает лицо, назначенное ответственным за организацию обработки персональных данных в Учреждении. Администратор ИСПДн обеспечивает реализацию и надлежащее функционирование разрешительной системы доступа к ИСПДн, составляет и обновляет необходимые для этого документы в соответствии с порядком, установленным Технологическим процессом обработки персональных данных в ИСПДн.

10 Требования к работникам по обеспечению защиты персональных данных

Все работники Учреждения, имеющие допуск к ИСПДн, должны быть ознакомлены с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, настоящей Политикой и другими принятыми в Учреждении организационно-распорядительными документами по вопросам обработки и защиты ПДн.

Обязанности и права ответственного за организацию обработки персональных данных в Учреждении, администраторов и пользователей ИСПДн определяются соответствующими инструкциями, утвержденными в Учреждении.

Доведение требований указанных документов до лиц, допущенных к ИСПДн, должно осуществляться под роспись. Все работники Учреждения, допущенные к ИСПДн, должны четко знать и неукоснительно выполнять установленные правила и обязанности по обеспечению безопасности ПДн при их обработке и соблюдению установленного режима конфиденциальности ПДн.

При вступлении в должность нового работника ответственный за организацию обработки персональных данных в Учреждении обязан организовать его ознакомление с необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

Работники Учреждения должны быть проинформированы об угрозах безопасности ПДн и ответственности за нарушение требований безопасности ПДн. Работники обязаны информировать ответственного за организацию обработки персональных данных в Учреждении и администратора ИСПДн о ставших им известными фактах нарушения положений настоящей Политики и инцидентах информационной безопасности в незамедлительном порядке.

11 Ответственность работников за нарушение норм, регулирующих обработку и защиту персональных данных

В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Действующее законодательство Российской Федерации позволяет предъявлять требования по обеспечению безопасности ПДн при их обработке и предусматривает ответственность за нарушение установленных правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-коммуникационных сетей, неправомерный доступ к охраняемой компьютерной информации, если эти действия привели к уничтожению, блокированию, модификации или копированию компьютерной информации (статьи 272, 273 и 274 УК РФ).

При нарушениях работниками Учреждения правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

Приложение
к Политике информационной безопасности ИСПДн
ГБУЗ ПК «ССМП г. Березники»
от «19» 02 201__ г.

Лист ознакомления

№ п/п	Фамилия, имя, отчество	Наименование подразделения, отдела	Дата ознакомления	Подпись
	Соседов А.Б	гл. бух	20.02.15	
	Ведерева К.А.	секретарь	20.02.15	
	Заболотских А.А	начальник ОК	20.02.15г.	
	Белина Е.Б.	специалист ОК	20.02.15	
	Танькина О.Л.	бухгалтер	24.02.2015г.	
	Чикишева М.С.	бухгалтер	24.02.2015	
	Анкинина И.В	бухгалтер	24.02.2015	
	Залу ОИ	бухгалтер	24.02.2015	
	Ушаков М.М.	зам. гл. вр.	24.02.2015	
	Сальникова С.О.	менеджер	24.02.2015	
	Тетерина Н.А.	фармацевт	24.02.15г.	
	Гафиатова Г.П.	спец. по ОТ	24.02.15	
	Казанцева С.А	нач. э/о	25.02.15г.	
	Рясков А.Н.	стар. диспетчер	25.02.15	
	Журавлёв Н.А.	вед. спец. по ГО	25.02.15	
	Банакеров С.В.	нач. гар.	25.02.15г.	
	Субботина И.Н.	глав. бухгалтер	25.02.15	
	Савкин Е.Г.	главный фельдшер	25.02.15	
	Харина И.А	мед. статистик	26.02.15	
	Сосункова Е.М.	гл. мед. сестра	26.02.15г.	

Приложение
к Политике информационной безопасности ИСПДн
ГБУЗ ПК «ССМП г. Березники»
от «___»_____201__ г.

Лист ознакомления

№ п/п	Фамилия, имя, отчество	Наименование подразделения, отдела	Дата ознакомления	Подпись
	Буканова А.В.	мед. статистик	26.02.15г.	
	Гимаедуллин Р.А.	сис. администратор	28.03.2016	
	Артамонова О.С.	ведущий экон.	28.03.2016	
	Кривогова Д.В.	Зам гл бух по ЭВ	17.10.2016.	