Приложение
к приказу от «25» 02 2016 г. № 49/02

**УТВЕРЖДЕНО**
Директор ГАПОУ
«Байкальский базовый
медицинский колледж МЗ РБ»
_____В.А. Козин

«25» февраля 2016 г.

# ПОЛИТИКА
## В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ И ОБУЧАЮЩИХСЯ ГАПОУ «БАЙКАЛЬСКИЙ БАЗОВЫЙ МЕДИЦИНСКИЙ КОЛЛЕДЖ МЗ РБ»

ГАПОУ "Байкальский базовый медицинский колледж МЗ РБ"
ЮРИСТ
_____ Кибирев А.Г.
"23" 02 2016 г.

**СЕЛЕНГИНСК, 2016**

## 1. НАЗНАЧЕНИЕ

Настоящая Политика в отношении обработки персональных данных работников и обучающихся ГАПОУ «Байкальский базовый медицинский колледж МЗ РБ» (далее - Политика):

1.1. Содержит сведения о реализуемых требованиях к защите персональных данныхработников и обучающихся ГАПОУ «Байкальский базовый медицинский колледж МЗ РБ» (далее - Учреждение).

1.2. Настоящая Политика должна быть опубликована или иным образом должен быть обеспечен неограниченный доступ к ней.

1.3. При сборе персональных данных с использованием информационно-телекоммуникационных сетей настоящая Политика должна быть опубликована в соответствующей информационно-телекоммуникационной сети, а также должна быть обеспечена возможность доступа к настоящей Политике с использованием средств соответствующей информационно-телекоммуникационной сети.

## 2.ОПРЕДЕЛЕНИЯ

В настоящей Политике используются следующие 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 организующие и (или) осуществляющие обработку 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, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

**-автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники;

**-распространение персональных данных** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

**-предоставление персональных данных** - действия, направленные на раскрытие персональных данныхопределенному лицу или определенному кругу лиц;

**-блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения 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;

**-обезличивание персональных данных-** действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данныхконкретному субъекту персональных данных;

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

## 3.ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

**Обозначения и сокращения,** используемые в настоящей Политике:

**-ПД** – персональные данные;

**- АРМ** – автоматизированное рабочее место;

**- ИСПД** – информационная система персональных данных;

**- КЗ** – контролируемая зона;

**- СЗИ** – средства защиты информации;

**- СЗПД –** система (подсистема) защиты персональных данных

## 4. ПРИНЦИПЫ И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Обработка ПД, обрабатываемых Оператором, должна осуществляться в соответствии с требованиями Федерального закона от 27 июля 2006г. №152-ФЗ «О персональных данных».

4.2. Защита ПД, обрабатываемых без использования средств автоматизации, должна строиться на основании требований Постановления Правительства РФ от 15 сентября 2008г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

4.3. СЗПД, обрабатываемых в информационных системах персональных данных Оператора, должна строиться на основании требований нормативных правовых актов, принятых в соответствии с Федеральным законом от 27 июля 2006г. №152-ФЗ «О персональных данных», а также:

- Актов определения уровня защищенности ПД при их обработке в информационной системе персональных данных Оператора;

- Моделей угроз безопасности ПД при их обработке в ИСПД.

4.4. Определение уровня защищенности ПД при их обработке в ИСПД должно осуществляться в соответствии с порядком, установленным Постановлением Правительства РФ от 1 ноября 2012г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

4.5. СЗПД должна включать в себя следующие подсистемы:

– подсистема идентификации и аутентификации субъектов доступа и объектов доступа;

– подсистема управления доступом субъектов доступа к объектам доступа;

– подсистема защиты машинных носителей ПД;

– подсистема регистрации событий безопасности;

– подсистема антивирусной защиты;

– подсистема контроля (анализа) защищенности ПД;

– подсистема защиты технических средств;

– подсистема защиты ИСПД, ее средств, систем связи и передачи данных;

– подсистема управления конфигурацией ИСПД и СЗПД.

4.6. Состав требований, реализуемых каждой из подсистем СЗПД, зависит от:

– уровня защищенности ПД при их обработке в ИСПД;

– структурно-функциональных характеристик и особенностей функционирования ИСПД;

– состава актуальных угроз безопасности ПД при их обработке в ИСПД.

## 5. КРУГ СУБЪЕКТОВ, ПЕРСОНАЛЬНЫЕ ДАННЫЕ КОТОРЫХ ОБРАБАТЫВАЮТСЯ

В зависимости от субъекта ПД Оператор обрабатывает ПД следующих категорий субъектов ПД:

-ПД работников;

-ПД обучающихся;

- персональные данные;

-ПД физического лица, обратившегося к Оператору с жалобами, заявлениями и обращениями.

## 6. ПРАВА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

Субъект ПД имеет право:

- на получение сведений о ПД, обрабатываемых Оператором;

- требовать уточнения своих ПД, их блокирования или уничтожения в случае, если ПД 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 ПД, в том числе о сроках их хранения;

- требовать извещения всех лиц, которым ранее были сообщены неверные или неполные его ПД, обо всех произведенных в них исключениях, исправлениях или дополнениях;

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

## 7. КАТЕГОРИИ СОТРУДНИКОВ, УЧАСТВУЮЩИХ В ОБРАБОТКЕ, ХРАНЕНИИ И ЗАЩИТЕ ПД

в Учреждении выделяются следующие категории сотрудников, участвующих в обработке, хранении и защите ПД:

- Ответственный за обеспечение защиты ПД;

- Администратор информационной безопасности ИСПД;

- Администратор ИСПДН;

- Пользователь ИСПД.

## 8. ОТВЕТСТВЕННЫЙ ЗА ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ПД

8.1. Ответственный за обеспечение защиты ПД - работник Оператора, ответственный за:

- подготовку локальных актов Учреждения по вопросам обработки и защиты ПД;

- осуществление внутреннего контроля за соблюдением Учреждения и его работниками законодательства Российской Федерации, локальных актов по вопросам обработки и защиты ПД;

- проведение инструктажа работников в целях доведения до данных работников положений законодательства Российской Федерации, локальных актов по вопросам обработки и защиты ПД;

- организацию приема и обработки запросов (обращений, заявлений) субъектов ПД или их представителей.

8.3. Ответственным за обеспечение защиты ПД назначается лицо, занимающее должность заместителя руководителя Учреждения.

8.2. Ответственный за обеспечение защиты ПД несет ответственность за некачественное, неполное, несвоевременное исполнение или неисполнение своих обязанностей, предусмотренных должностной инструкцией ответственного за организацию обработки ПД или соответствующим договором со специализированной организацией.

## 9. АДМИНИСТРАТОР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИСПДН

9.1. Администратор информационной безопасности ИСПД – работник Оператора, ответственный за установку, настройку и сопровождение СЗИ.

9.3. Администратором информационной безопасности ИСПД назначается: юрист, системный администратор, администратор информационной безопасности и т.п.

9.2. Администратор информационной безопасности ИСПД несет ответственность за некачественное, неполное, несвоевременное исполнение или неисполнение своих обязанностей, предусмотренных должностной инструкцией администратора информационной безопасности ИСПД.

## 10. АДМИНИСТРАТОР ИСПДН

10.1. Администратор ИСПД - лицо ответственное за установку, настройку и сопровождение программных, программноаппаратных, аппаратных средств ИСПД. К данной группе могут относиться как работник Оператора, так и сотрудники сторонних организаций.

10.2. Администратором ИСПД назначается лицо, имеющее производственный стаж в области создания, обслуживания локальных вычислительных сетей не менее одного года.

10.3. Лицо этой категории:

- обладает информацией об алгоритмах и программах обработки информации на ИСПД;
- обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПД на стадии ее разработки, внедрения и сопровождения;

10.4. Администратор ИСПД несет ответственность за некачественное, неполное, несвоевременное исполнение или неисполнение своих обязанностей, предусмотренных должностной инструкцией администратора ИСПД.

## 11. ПОЛЬЗОВАТЕЛЬ ИСПД

11.1. Пользователь ИСПД, работник Оператора, осуществляющий обработку ПД. Обработка ПД включает: возможность просмотра ПД, ручной ввод ПД в систему ИСПД, формирование справок и отчетов по информации, полученной из ИСПД. Пользователь не имеет полномочий для управления подсистемами обработки данных и СЗПД.

11.2. Пользователь ИСПД обладает следующим уровнем доступа и знаний:

-обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПД;

- располагает конфиденциальными данными, к которым имеет доступ.

11.3. Пользователь ИСПД обязан выполнять на АРМ только те процедуры, которые определены для него в Положении «О разграничении прав доступа к персональным данным работников и обучающихся ГАПОУ «Байкальский базовый медицинский колледж МЗ РБ»»

11.4. Пользователь ИСПД несет ответственность за некачественное, неполное, несвоевременное исполнение или неисполнение своих обязанностей, предусмотренных должностной инструкцией пользователя ИСПД.

## 12. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

12.1. Безопасность ПД, обрабатываемых Оператором, обеспечивается реализацией правовых, организационных, технических и программных мер, необходимых и достаточных для обеспечения требований федерального законодательства в области защиты персональных данных.

12.2. Оператор предпринимает необходимые организационные и технические меры для обеспечения безопасности ПД от случайного или несанкционированного доступа, уничтожения, изменения, блокирования доступа и других несанкционированных действий.

12.3. Оператор применяет следующие организационно-технические меры:

- назначение должностных лиц, ответственных за организацию обработки и защиты ПД;
- ограничение и регламентация состава работников, имеющих доступ к ПД;
- ознакомление работников, обучающихся с требованиями федерального законодательства и нормативных документов Оператора по обработке и защите ПД;
- обеспечение учета и хранения материальных носителей информации и их обращения, исключающего хищение, подмену, несанкционированное копирование и уничтожение;
- определение угроз безопасности ПД при их обработке, формирование на их основе моделей угроз;
- реализация разрешительной системы доступа пользователей к информационным ресурсам, программно-аппаратным средствам обработки и защиты информации;
- регистрация и учет действий пользователей информационных систем ПД;
- парольная защита доступа пользователей к ИСПД;
-применение средств контроля доступа к коммуникационным портам, устройствам ввода-вывода информации, съемным машинным носителям и внешним накопителям информации;
- осуществление антивирусного контроля, предотвращение внедрения в корпоративную сеть вредоносных программ (программ-вирусов) и программных закладок;
- централизованное управление системой защиты ПД;
- резервное копирование информации;
- обеспечение восстановления ПД, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;
- проведение контрольных мероприятий по фактам нарушения требований безопасности ПД;
-размещение технических средств обработки ПД, в пределах КЗ;
-поддержание технических средств охраны помещений в состоянии постоянной готовности.

## 13. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

13.1. Настоящая Политика является внутренним документом Учреждения, общедоступной и подлежит размещению на официальном сайте Учреждения.

13.2. Настоящая Политика подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите ПД.

13.3. Контроль исполнения требований настоящей Политики осуществляется лицом, назначенным ответственным за обеспечение безопасности ПД Учреждения.

13.4. Ответственность должностных лиц Учреждения, имеющих доступ к ПД, за невыполнение требований норм, регулирующих обработку и защиту персональных данных, определяется в соответствии с законодательством Российской Федерации и внутренними документами Учреждения.