«УТВЕРЖДАЮ»
Главный врач ГАУЗ «ССМП» г. Орска
_____ Кумзин К.А.
(подпись)
«11» января 2016 г.

Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных государственного автономного учреждения здравоохранения «Станция скорой медицинской помощи» города Орска

1. Общие положения

1.1. Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных ГАУЗ «ССМП» г. Орска (далее – «Положение») разработано в соответствии с Конституцией Российской Федерации, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и другими нормативными правовыми актами и нормативными методическими документами Российской Федерации, регулирующими отношения, связанные с обеспечением безопасности персональных данных при их обработке в информационных системах персональных данных.

1.2. Положение устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ГАУЗ «ССМП» г. Орска (далее - «Оператор персональных данных»).

1.3. Безопасность персональных данных при их обработке в информационных системах персональных данных обеспечивается применением организационных мер и технических средств защиты информации (в том числе средств предотвращения несанкционированного доступа). Организационные меры и технические средства защиты информации должны удовлетворять требованиям, установленным нормативными правовыми актами и нормативными методическими документами Российской Федерации, регулирующими отношения, связанные с обеспечением безопасности персональных данных при их обработке в информационных системах персональных данных.

1.4. Требования настоящего Положения являются обязательными для исполнения всеми лицами, получившими доступ к персональным данным.

1.5. Решение о необходимости изменения этого Положения принимается на основании:

результатов проведенных аудитов, мероприятий по контролю и надзору за обеспечением безопасности персональных данных, осуществляемых уполномоченными органами;

изменения нормативных правовых актов и (или) нормативных методических документов Российской Федерации в области защиты персональных данных;

изменения процессов обработки персональных данных в информационных системах (далее - ИС) персональных данных ГАУЗ «ССМП» г. Орска;

результатов анализа инцидентов информационной безопасности в ИС персональных данных.

Изменения Положения должны быть направлены на предотвращение инцидентов или устранение последствий уже реализованных инцидентов информационной безопасности.

Все предлагаемые изменения Положения подлежат предварительной оценке до их ввода в действие, на соответствие нормативным правовым актам и нормативным методическим документам Российской Федерации, регулирующим отношения, связанные с обеспечением безопасности персональных данных при их обработке в ИС персональных данных.

2. Обработка персональных данных

2.1. Оператор персональных данных осуществляет обработку персональных данных лиц, работающих в ГАУЗ «ССМП» г. Орска, а также пациентов, которым были предоставлены медицинские услуги ГАУЗ «ССМП» г. Орска.

2.2. Обработка персональных данных осуществляется оператором персональных данных в целях реализации возложенных на него функций, определяемых законами и иными нормативными правовыми актами Российской Федерации, регулирующими отношения, связанные с обеспечением безопасности персональных данных при их обработке в ИС персональных данных.

2.3. Объем и характер обрабатываемых персональных данных должен соответствовать целям их обработки. Обрабатываемые персональные данные должны соответствовать заявленным целям обработки. Недопустимо объединение созданных для несовместимых между собой целей баз данных ИС персональных данных.

2.4. Обработка персональных данных осуществляется оператором без проведения мероприятий по обезличиванию персональных данных.

2.5. Персональные данные оператор получает непосредственно от структурных подразделений Оренбургской области и субъектов персональных данных, которые принимают решение об их предоставлении и дают согласие на их обработку своей волей и в своем интересе.

2.6. Лица, доступ которых к персональным данным, обрабатываемым в ИС, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании списков сотрудников, допущенным к соответствующим персональным данным.

2.7. Принятые в ГАУЗ «ССМП» г. Орска организационно-распорядительные документы доводятся до сведения лиц, участвующих в обработке персональных данных, в части их касающейся.

2.8. Персональные данные, используемые для обработки в ИС, порядок использования, цель, периодичность и основания внесения изменений и дополнений, а также порядок хранения персональных данных устанавливаются оператором персональных данных.

2.9. Оператор не имеет права получать и обрабатывать персональные данные субъекта персональных данных о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, интимной жизни.

2.10. Хранение персональных данных в форме, позволяющей определить субъекта персональных данных, должно осуществляться не дольше, чем этого требуют цели обработки персональных данных. Персональные данные подлежат уничтожению по достижении всех целей их обработки или в случае утраты необходимости в достижении этих целей. Оператор по согласованию с субъектом персональных данных может изменить сроки хранения его

персональных данных в связи с обязанностями, возлагаемыми на оператора законодательством Российской Федерации.

3. Обязанности и права оператора персональных данных в ИС

3.1. Оператор персональных данных обязан предоставлять субъекту персональных данных возможность ознакомления с его персональными данными, а также вносить в них необходимые изменения, уничтожать или блокировать соответствующие персональные данные в случае предоставления субъектом персональных данных сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту и обработку которых осуществляет оператор в ИС персональных данных, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и принятых мерах оператор персональных данных уведомляет субъекта персональных данных или его законного представителя и третьих лиц, которым персональные данные этого субъекта были переданы.

3.2. В случае выявления недостоверных персональных данных или фактов неправомерных действий с ними оператора персональных данных, при обращении или по запросу субъекта персональных данных или его законного представителя, либо Управления Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций в Оренбургской области, оператор обязан осуществить блокирование персональных данных, относящихся к соответствующему субъекту персональных данных, с момента такого обращения или получения такого запроса на период проверки.

3.3. В случае подтверждения факта недостоверности персональных данных оператор на основании документов, представленных субъектом персональных данных или его законным представителем либо Управлением Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций в Оренбургской области, или иных необходимых документов, обязан уточнить персональные данные и отменить их блокирование.

3.4. В случае выявления неправомерных действий с персональными данными оператор персональных данных в срок, не превышающий тридцати дней с даты такого выявления, обязан устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений оператор персональных данных в срок, не превышающий тридцати дней с даты выявления неправомерности действий с персональными данными, обязан уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены Управлением Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций в Оренбургской области, – также указанный орган.

3.5. Оператор персональных данных в случае достижения всех целей обработки персональных данных обязан незамедлительно прекратить их обработку и уничтожить соответствующие персональные данные в срок, не превышающий тридцати дней с даты достижения всех целей обработки персональных данных, и уведомить об этом субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены Управлением Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций в Оренбургской области, – также указанный орган. По согласованию с субъектом персональных данных оператор может изменить сроки хранения его персональных данных в связи с обязанностями, возлагаемыми на оператора законодательством Российской Федерации.

3.6. Оператор персональных данных, в случае отзыва субъектом персональных данных согласия на обработку его персональных данных, обязан прекратить их обработку и уничтожить персональные данные в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между оператором и субъектом персональных данных.

3.7. Оператор при передаче персональных данных субъектов третьим лицам ограничивает передаваемую информацию только теми персональными данными субъектов, которые необходимы третьим лицам для выполнения своих функций. Передача персональных данных по телефону, факсимильной связи, электронной почте и сети Интернет (без использования средств защиты информации, удовлетворяющих требованиям, установленным нормативными правовыми актами и нормативными методическими документами Российской Федерации, регулирующими отношения, связанные с обеспечением безопасности персональных данных при их обработке в информационных системах персональных данных) запрещается.

4. Методы и способы защиты персональных данных в информационных системах персональных данных

4.1. С целью установления методов и способов защиты информации, необходимых для обеспечения безопасности персональных данных, оператором должны быть установлены уровни защищенности персональных данных ИС.

4.2. В целях обеспечения безопасности персональных данных определяются угрозы безопасности, оценивается актуальность угроз безопасности персональных данных. В результате разрабатывается модель угроз безопасности персональных данных.

Модель угроз безопасности персональных данных корректируется при изменении состава основных технических средств и условий эксплуатации ИС персональных данных отделом по обслуживанию информационно-коммуникационных систем управления делами.

4.3. Установка, изменение (обновление) и удаление программного обеспечения в ИС персональных данных производится специалистом по защите информации или в его присутствии.

4.4. Доступ лиц к ИС персональных данных, не допущенных к работе с персональными данными, должен быть исключен. ИС персональных данных должны быть защищены аппаратными и (или) программными средствами защиты информации от несанкционированного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Российской федерации, регулирующими отношения, связанные с обеспечением безопасности персональных данных при их обработке в информационных системах персональных данных.

4.5. Обработка персональных данных в ИС осуществляется без подключения к локальной вычислительной сети министерства здравоохранения Оренбургской области, в случае необходимости подключение осуществляется с использованием средств защиты информации в соответствии с установленными требованиями нормативных правовых актов Российской Федерации, регулирующих отношения, связанные с обеспечением безопасности информации.

4.6. Охрана помещений, в которых ведется работа с персональными данными, и организация режима безопасности в этих помещениях должна обеспечивать сохранность технических средств и носителей персональных данных, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

Все носители персональных данных должны быть учтены с помощью их маркировки, а их учетные данные занесены в журнал учета с отметкой об их выдаче (приеме).

4.7. В целях обеспечения безопасности персональных данных должны быть разработаны организационно-распорядительные и организационно-методические документы по обеспечению безопасности персональных данных, обрабатываемых в ИС:

перечень информационных систем персональных данных;

перечень персональных данных, обрабатываемых в ГАУЗ «ССМП» г. Орска в связи с реализацией служебных (трудовых) отношений;

список лиц, допущенных к соответствующим персональным данным;

инструкция по работе пользователей в ИС персональных данных;

инструкция по организации доступа в помещения, в которых ведется обработка персональных данных;

инструкция администратора безопасности ИС персональных данных;

инструкция по организации резервного копирования персональных данных;

инструкция по организации учета, использования и уничтожения машинных носителей информации, предназначенных для обработки и хранения персональных данных;

инструкция по организации парольной защиты в ИС персональных данных;

инструкция по проведению антивирусного контроля в ИС персональных данных;

инструкция по организации технического обслуживания и ремонта технических средств ИС персональных данных;

инструкция по правилам обращения с носителями ключевой информации в информационных системах персональных данных;

инструкция ответственного за организацию обработки персональных данных;

правила рассмотрения запросов субъектов персональных данных или их представителей в ГАУЗ «ССМП» г. Орска;

правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в ГАУЗ «ССМП» г. Орска;

правила обработки персональных данных в ГАУЗ «ССМП» г. Орска;

другие организационно-распорядительные документы по обеспечению безопасности персональных данных, обрабатываемых в ИС.

4.8. Лица, уполномоченные осуществлять обработку персональных данных, несут ответственность за соблюдение требований по защите персональных данных в порядке, предусмотренном действующим законодательством Российской Федерации.

5. Обязанности и права должностных лиц

5.1. Главный врач ГАУЗ «ССМП» г. Орска:

организует разработку, внедрение, совершенствование и эксплуатацию системы защиты ИС персональных данных, а также организует внутренний контроль за соблюдением нормативных правовых актов Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

обеспечивает реализацию мероприятий по защите персональных данных при их обработке в ИС персональных данных в ГАУЗ «ССМП» г.;

осуществляет финансовое, материально-техническое и иное обеспечение мероприятий по защите персональных данных при их обработке в ИС персональных данных ГАУЗ «ССМП» г. Орска;

назначает ответственного за организацию обработки персональных данных;

назначает ответственного за обеспечение безопасности персональных данных.

5.2. Ответственный за организацию обработки персональных данных:

осуществляет внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

доводит до сведения работников оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

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

5.3. Ответственный за обеспечение безопасности персональных данных:

несет ответственность за организацию обеспечения безопасности персональных данных при их обработке в ИС ГАУЗ «ССМП» г. Орска;

осуществляет контроль за режимом работы, использования и условиями эксплуатации вычислительной техники ГАУЗ «ССМП» г. Орска;

обеспечивает выполнение организационных мероприятий, направленных на обеспечение защиты персональных данных при их обработке в ИС персональных данных;

организует регистрацию и учет защищаемых носителей информации;

организует расследование причин и условий появления нарушений безопасности ИС персональных данных, разработку предложений по устранению недостатков и предупреждению подобного рода нарушений;

обеспечивает обнаружение фактов несанкционированного доступа к ИС персональных данных, о которых должен доложить главному врачу ГАУЗ «ССМП» г. Орска;

осуществляет установку и ввод в эксплуатацию средств защиты информации ИС персональных данных в соответствии с эксплуатационной и технической документацией;

обеспечивает работы по проведению антивирусного контроля в ИС персональных данных;

выполняет резервное копирование персональных данных;

осуществляет установку (обновление версий) программного обеспечения ИС персональных данных, обеспечивает его функционирование;

осуществляет установку, подключение и настройку технических средств ИС персональных данных в соответствии с технической документацией;

осуществляет установку (развертывание) новых ИС персональных данных или подключение дополнительных устройств (узлов, блоков), необходимых для решения конкретных задач.

организует выполнение мероприятий по защите персональных данных при их обработке в ИС персональных данных;

разрабатывает проекты распорядительных документов по защите персональных данных при их обработке в ИС персональных данных в ГАУЗ «ССМП» г. Орска;

разрабатывает совместно с другими структурными подразделениями ГАУЗ «ССМП» г. Орска настоящее Положение и вносит в него в установленном порядке изменения;

разрабатывает предложения по дальнейшему совершенствованию системы защиты персональных данных при их обработке в ИС персональных данных;

осуществляет планирование мероприятий по защите персональных данных при их обработке в ИС персональных данных, их выполнение и контроль их эффективности;

подготавливает предложения о привлечении к проведению работ по защите персональных данных при их обработке в ИС персональных данных на договорной основе организаций, имеющих лицензию на соответствующий вид деятельности;

обеспечивает обслуживание и ремонт сетевого оборудования, рабочих станций, серверного и периферийного оборудования в ИС персональных данных.

6. Контроль состояния защиты персональных данных

6.1. Контроль и надзор за выполнением требований по обеспечению безопасности персональных данных при их обработке в ИС персональных данных, установленных Правительством Российской Федерации, осуществляется представителями Управления Федеральной службы безопасности России в Оренбургской области, представителями центрального аппарата ФСТЭК России, Управления ФСТЭК России по Приволжскому федеральному округу в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в ИС персональных данных.

6.2. Повседневный контроль выполнения организационных мероприятий, направленных на обеспечение защиты персональных данных при их обработке в ИС персональных данных, осуществляется ответственным за организацию обработки персональных данных и ответственным за обеспечение безопасности персональных данных.

7. Заключительные положения

7.1. Настоящее Положение вступает в силу с момента его утверждения.

7.2. Настоящее Положение не заменяет собой действующее законодательство Российской Федерации, регулирующее отношения, связанные с обеспечением безопасности персональных данных при их обработке в ИС персональных данных.

Главный врач К.А. Кумзин