Федеральное государственное бюджетное учреждение «Федеральный центр сердечно-сосудистой хирургии» Министерства здравоохранения Российской Федерации (г. Красноярск)

УТВЕРЖДАЮ

Главный врач

_____ В.А. Сакович

«___»_____2017 г.

Регламент

подключения абонентских пунктов к порталу «Единый регистр пациентов с врождёнными пороками сердца»

г. Красноярск

2017

ОГЛАВЛЕНИЕ

Термины, определения и сокращения.

Термин	Описание
Абонентский пункт	Автоматизированное рабочее место, используемое для доступа к порталу
ИСПДн	Информационная система персональных данных
Оператор портала	ФГБУ «ФЦССХ» Минздрава России (г. Красноярск)
Владельцы абонентских пунктов	Организации, взаимодействующие с ФГБУ «ФЦССХ» Минздрава России (г. Красноярск) при ведении учета пациентов с врождёнными пороками сердца посредством портала «Регистр ВПС»
ПО	Программное обеспечение
СЗИ	Средство защиты информации
СКЗИ, криптосредство	Средство криптографической защиты информации

1. Общие положения

1.1. Настоящий регламент определяет порядок подключения абонентских пунктов к порталу «Единый регистр пациентов с врождёнными пороками сердца» и порядок взаимодействия между Оператором портала и владельцами абонентских пунктов.

1.2. Сокращенное наименование системы: «Регистр ВПС».

1.3. Адрес доступа к порталу: edregvps.ru

1.4. Оператор портала: Федеральное государственное бюджетное учреждение «Федеральный центр сердечно-сосудистой хирургии» Министерства здравоохранения Российской Федерации (г. Красноярск).

1.5. Владельцами абонентских пунктов могут являться учреждения и организации, взаимодействующие с ФГБУ «ФЦССХ» Минздрава России (г. Красноярск) при ведении учета пациентов с врождёнными пороками сердца посредством портала «Регистр ВПС».

1.6. Регламент разработан в соответствии со следующими документами по защите персональных данных:

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных».
- Требования к защите персональных данных при их обработке в информационных системах персональных данных (утв. постановлением Правительства РФ от 1 ноября 2012 г. №1119).
- Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (утв. приказом ФСТЭК России от 18 февраля 2013 г. N 21).
- Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (ФСБ России, № 149/6/6-622, 2008);
- Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (ФСБ России, № 149/5-144, 2008);
- «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных правительством российской федерации требований к защите персональных данных для каждого из уровней защищенности», (утвержден приказом ФСБ России от 10 июля 2014 г. N 378).

1.7. Обмен информацией, содержащей информацию ограниченного доступа, в рамках портала «Регистр ВПС» осуществляется по телекоммуникационным каналам связи.

1.8. Обеспечение защиты информации ограниченного доступа осуществляется с использованием следующих или аналогичных по характеристикам СКЗИ:

- СКЗИ «МагПро КриптоПакет» версии 2.1 в комплектации «МагПро OpenVPN-ГОСТ»

1.9. При работе с информацией ограниченного доступа, в рамках портала «Регистр ВПС», пользователи портала руководствуются законодательными актами Российской Федерации в области защиты персональных данных и настоящим Регламентом.

2. Порядок подключения абонентского пункта к порталу «Регистр ВПС»

2.1. В информационных системах и на рабочих местах подключаемые к порталу «Регистр ВПС», должны быть соблюдены требования законодательства РФ по защите персональных данных.

2.2. Владелец абонентского пункта оформляет заявку на предоставление доступа к порталу и направляет по адресу support@edregvps.ru

2.3. Оператор портала предоставляет установочный пакет программного обеспечения, учетные данные для доступа к порталу (логин и пароль).

2.4. Оператор портала выдает владельцу абонентского пункта ключевые документы для настройки средств шифрования каналов связи.

2.5. После передачи необходимых ключевых документов производится настройка СКЗИ. Настройку СКЗИ выполняет организация, имеющая необходимые лицензии в соответствии с Постановлением правительства №313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, …» от 16.04.2012.

2.6. Допускается установка программного обеспечения непосредственно на абонентский пункт или на компьютер, выполняющий роль маршрутизатора в защищенную сеть.

2.7. Подключение к порталу выполняется в соответствии с «Инструкцией по подключению к закрытой части портала «Единый регистр пациентов с ВПС».

3. Порядок взаимодействия при обеспечении работы портала

3.1. Оператор и Владелец абонентского пункта должны:

3.2. обеспечить функционирование всего необходимого оборудования со своих сторон, необходимого для работы портала;

3.3. немедленно информировать другую Сторону о компрометации ключей шифрования;

3.4. немедленно приостанавливать работу с порталом при получении от другой Стороны или сообщения о компрометации ключей шифрования;

3.5. оказывать содействие друг другу в настройке и обеспечении правильности эксплуатации СКЗИ;

3.6. соблюдать правила работы и требования эксплуатационной документации на СКЗИ;

3.7. содержать в исправном состоянии компьютеры, участвующие в электронном взаимодействии, принимать организационные меры для предотвращения несанкционированного доступа к данным компьютерам, установленному на них программному обеспечению и СКЗИ, а также в помещения, в которых они установлены;

3.8. не допускать появления на взаимодействующих компьютерах компьютерных вирусов;

3.9. руководствоваться правилами и техническими требованиями, установленными действующим законодательством Российской Федерации и другими нормативными актами.

3.10. Владелец абонентского пункта использует для подключения к порталу узлы, для которых выполнены технические и организационные меры по защите персональных данных в соответствии с категорией и объемом обрабатываемых персональных данных.

3.11. Владелец абонентского пункта обязан предоставить копию документа, подтверждающего соответствие информационной системы персональных данных, планируемой к работе с порталом, требованиям законодательства к заявленному уровню защищенности ИСПДн.

4. Требования по обеспечению безопасности персональных данных, обрабатываемых на абонентском пункте

4.1. Владелец абонентского пункта обязан выполнить все технические и организационные меры по защите информации в соответствии с законодательством РФ в части защиты персональных данных.

4.2. На абонентском пункте должен обеспечиваться второй уровень защищенности персональных данных в соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных» (утв. постановлением Правительства РФ от 1 ноября 2012 г. №1119).

4.3. Владелец абонентского пункта выполняет меры по обеспечению безопасности персональных данных самостоятельно или с привлечением организаций, имеющих необходимые в соответствии с Постановлениями Правительства РФ №79 от 03.02.2012 и №313 от 16.04.2012 для проведения работ лицензии.

4.4. Перечень мер по обеспечению безопасности персональных данных, предусмотренных Федеральным законом от 27 июля 2006 года № 152-ФЗ:

1) определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учет машинных носителей персональных данных;

6) обнаружение фактов несанкционированного доступа к персональным данным и принятием мер;

7) восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

9) контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

5. Требования по применению СКЗИ на абонентском пункте

5.1. Владельцем абонентского пункта должен быть назначен ответственный пользователь криптосредств, на которого возлагаются задачи организации работ по использованию СКЗИ, выработки соответствующих инструкций для пользователей, а также контроль за соблюдением требований.

5.2. Решением руководителя организации определяется список лиц, допущенных к работе с СКЗИ. Правом доступа к рабочим местам с установленными СКЗИ должны обладать только определенные лица, прошедшие соответствующую подготовку. Ответственный пользователь криптосредств должен ознакомить каждого пользователя, применяющего СКЗИ, с документацией на СКЗИ и правилами пользования СКЗИ.

5.3. Вопросы обеспечения функционирования и безопасности СКЗИ должны быть отражены в инструкциях, утвержденных руководителем организации, с учетом эксплуатационной документации на СКЗИ.

5.4. Пользователь СКЗИ должен принять на себя обязательства по нераспространению доверенных ему конфиденциальных сведений (в частности, ключевой информации). Такие обязательства могут включаться непосредственно в текст контракта (договора).

5.5. К установке общесистемного и специального программного обеспечения, а также СКЗИ, допускаются лица, прошедшие соответствующую подготовку и изучившие документацию на соответствующее ПО и на СКЗИ.

5.6. Должны быть предусмотрены меры, исключающие возможность несанкционированного изменения аппаратной части технических средств, на которых установлено СКЗИ (например, путем опечатывания системного блока и разъемов ПЭВМ). Место для опечатывания (опломбирования) выбирается таким, чтобы его можно было визуально контролировать.

5.7. На абонентском пункте не должны устанавливаться средства разработки ПО и отладчики. Запрещается вносить какие-либо изменения в программное обеспечение СКЗИ.

5.8. На абонентском пункте должны использоваться сертифицированные средства антивирусной защиты, средства защиты от несанкционированного доступа.

5.9. Должно быть обеспечено регулярное обновление ПО, операционных систем и антивирусных баз.

5.10. Ответственный пользователь криптосредств периодически должен проводить контроль сохранности входящего в состав СКЗИ оборудования, а также всего используемого программного обеспечения для предотвращения несанкционированных изменений.

5.11. Должен осуществляться периодический (не реже раза в неделю) контроль целостности установленного ПО СКЗИ, а также его окружения. Контроль целостности обеспечивается программными средствами путем вычисления хэш-векторов файлов и сравнения вычисленных хэш-векторов с эталонными значениями в соответствии с документацией на СКЗИ.

6. Требования по размещению абонентского пункта

6.1. При размещении абонентского пункта с установленным СКЗИ должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых размещен абонентский пункт, посторонних лиц, не являющихся персоналом, допущенным к работе в этих помещениях.

6.2. Размещение, охрана и режим в помещениях, в которых размещен абонентский пункт с установленными СКЗИ (далее – помещения), должны обеспечивать безопасность информации, средств криптографической защиты информации, ключей шифрования, сведение к минимуму возможности неконтролируемого доступа к СКЗИ, просмотра процедур работы посторонними лицами.

6.3. Порядок доступа в помещения определяется внутренней инструкцией, которая разрабатывается с учетом специфики и условий функционирования организации.

6.4. Размещение компьютера, на котором установлено СКЗИ, должно исключать возможность визуального просмотра экрана монитора через окна. В случае, когда разместить таким образом монитор нет возможности, окна в помещении при работе со СКЗИ закрываются жалюзи.

6.5. По окончании рабочего дня помещения должны быть закрыты.

6.6. Порядок охраны помещений должен предусматривать периодический контроль технического состояния средств охранной и пожарной сигнализации и соблюдения режима охраны.

7. Ответственность за соблюдение порядка работы с порталом

7.1. Владелец абонентского пункта несет ответственность за использование информации в соответствии с законодательством Российской Федерации.

7.2. В случае нарушения Владельцем абонентского пункта установленных правил по работе с порталом, Оператор оставляет за собой право приостановить доступ к порталу до устранения нарушений.