УТВЕРЖДАЮ

Директор ГАУЗ «ПК МИАЦ»

_____ М.В. Волкова

«26» сентября 2017 года

РЕГЛАМЕНТ

ПОДКЛЮЧЕНИЯ МЕДИЦИНСКИХ ОРГАНИЗАЦИЙ ПРИМОРСКОГО КРАЯ К РЕГИОНАЛЬНОМУ СЕГМЕНТУ ЕДИНОЙ ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ЗДРАВООХРАНЕНИЯ ПРИМОРСКОГО КРАЯ

Владивосток, 2017 г.

СОДЕРЖАНИЕ

1.Список сокращений и обозначений

АИС - автоматизированная информационная система
АПК «ЦАМИ»- аппаратно-программный комплекс «Центральный архив медицинских изображений
АРМ - автоматизированное рабочее место
ЕИАС - единая информационно-аналитическая система
ИС - информационная система
ИСПДн - информационная система персональных данных
МО - медицинские организации Приморского края
НСД - несанкционированный доступ
ОС - операционная система
ПДн - персональные данные
ПО - программное обеспечение
РЕГИСЗ ПК - региональный сегмент единой государственной информационной системы здравоохранения Приморского края
РИИСЗ ПК - региональная интегрированная информационная система в сфере здравоохранения Приморского края
СКЗИ - средство криптографической защиты информации
ТЗКИ - техническая защита конфиденциальной информации
ФСТЭК - Федеральная служба по техническому и экспортному контролю
Оператор - ГАУЗ «Приморский краевой медицинский информационно-аналитический центр»

2.Цели и назначение документа

РЕГИСЗ ПК включает в себя следующие подсистемы:

- ЕИАС «Демография»;
- АПК «ЦАМИ»;
- РИИСЗ ПК;
- иные информационные системы, созданные в Приморском крае с целью централизации и автоматизации оказания медицинских услуг (в случае если для их функционирования необходимо обеспечить не выше второго уровня защищенности персональных данных) или обеспечения деятельности медицинских организаций ПК.

Описанные в настоящем документе организационно-технические условия могут применяться как для РЕГИСЗ ПК в целом, так и для одной из подсистем или нескольких подсистем, если иное не установлено отдельными нормативными актами Оператора системы. Для унификации понятий далее под РЕГИСЗ ПК может пониматься как система в целом так и отдельная ее подсистема или набор подсистем.

Оператором РЕГИСЗ ПК и ее подсистем является ГАУЗ «Приморский краевой медицинский информационно-аналитический центр» (далее – Оператор). Пользователями системы, подключающимися к ней в соответствии с настоящим Регламентом, являются медицинские организации Приморского края (далее - МО).

В РЕГИСЗ ПК и ее подсистемах подлежат обработке персональные данные граждан специальных категорий, а также с соответствии с иными классификационными признаками, установленными правительством РФ и уполномоченными органами исполнительной сласти, установлена необходимость обеспечения как минимум второго уровня защищенности персональных данных.

В соответствии с пунктом 6 приказа ФСТЭК № 17 Оператором РЕГИСЗ ПК и ее подсистем принято решение о реализации мер по защите информации в соответствии с положениями Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных Приказом ФСТЭК России №17 от 11.02.2013. Назначением настоящего документа является выработка организационно-технических

требований к клиентской части РЕГИСЗ ПК на стороне МО, а также формирование последовательности действий МО по реализации требований по защите информации в системе.

Требования к мерам по защите информации в сегментах РЕГИСЗ ПК и ее подсистем сформированы в Техническом (Частном техническом) задании на систему (подсистему) защиты информации в РЕГИСЗ ПК (далее – ТЗ, ЧТЗ). Выписка из указанный документации предоставляется МО на основании запроса.

3.Порядок подключения МО к РЕГИСЗ ПК

3.1 Заявление на подключение

Для начала взаимодействия МО и Оператора с целью подключения к РЕГИСЗ ПК, МО направляет в адрес Оператора заявление на подключение по форме, приведенной в Приложении № 1 к настоящему документу.

3.2 Назначение ответственных лиц и внедрение комплекта организационно-распорядительной документации по защите информации

В ответ на заявку, МО получает от оператора выписки из документов «Модель угроз безопасности информации в РЕГИСЗ ПК» и «Частное техническое задание на создание системы защиты информации в РЕГИСЗ ПК» в электронном виде, а также образцы внутренних организационно-распорядительных документов по защите информации.

В соответствии с ПП 1119 в МО назначает ответственное лицо обеспечение безопасности персональных данных при их обработке в МО.

Образцы внутренних документов по защите информации включают следующие формы:

- приказ «О назначении ответственного за организацию обработки персональных данных и администратора безопасности в сегменте МО РЕГИСЗ ПК»;
- инструкция администратора безопасности в сегменте МО РЕГИСЗ ПК;
- инструкция ответственного за организацию обработки персональных данных в МО;
- приказ «О назначении группы реагирования на инциденты информационной безопасности и о правилах регистрации инцидентов информационной безопасности и реагирования на них в сегменте МО РЕГИСЗ ПК»;
- инструкция по реагированию на инциденты информационной безопасности в сегменте МО РЕГИСЗ ПК;
- об утверждении внутренних нормативных актов МО по защите информации;
- инструкция пользователя сегмента МО РЕГИСЗ ПК;
- политика информационной безопасности сегмента МО РЕГИСЗ ПК;
- приказ «Об организации контролируемой зоны»;
- положение о контролируемой зоне в МО;
- план мероприятий по обеспечению безопасности защищаемой информации, выполнению требований законодательства по защите информации, а также по контролю уровня защищенности и выполнения мер по защите информации сегменте МО РЕГИСЗ ПК;
- журнал учета машинных носителей информации сегмента РЕГИСЗ ПК;
- приказ «О порядке хранения и эксплуатации средств криптографической защиты информации в МО»;
- инструкция по обеспечению безопасности эксплуатации СКЗИ в МО;
- журнал поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов;

- технический паспорт на сегмент МО РЕГИСЗ ПК;

МО адаптирует под собственную организационную структуру полученные документы по защите информации и утверждает их.

3.3 Внедрение системы защиты информации

МО осуществляет закупку или использует уже имеющиеся средства защиты информации (далее - СЗИ). Необходимый набор должен включать:

- средство защиты информации от несанкционированного доступа (Dallas Lock 8.0-K или эквивалент);
- Средство антивирусной защиты (Kaspersky Endpoint Security 10 или эквивалент);
- сетевой сканер безопасности (Сканер ВС, XSpider 7 или эквивалент);
- средство защиты сетевого трафика и межсетевой экран ViPNet Client 4.x класса КС3 в сеть № 1652 (эквивалент недопустим, поскольку защищенная сеть оператора серверная часть РЕГИСЗ ПК организована с применением средств криптографической защиты информации семейства ViPNet, другие средства защиты сетевого трафика с технологией ViPNet несовместимы).

Все средства защиты должны иметь действующие сертификаты ФСТЭК и (или) ФСБ России, позволяющий использовать СЗИ в государственных информационных системах второго класса защищенности.

Средства криптографической защиты информации должны применяться согласно эксплуатационной документации.

МО самостоятельно или с привлечением лицензиата ФСТЭК России на проведение работ по технической защите конфиденциальной информации в соответствии с требованиями настоящего документа осуществляет установку и настройку средств защиты информации.

Сетевой сканер устанавливается на ежемесячное сканирование защищаемых АРМ по заданным профилям. В профиле указывается проверка уязвимостей Windows, сканирование баз данных, FTP, LDAP, NetBIOS, а также подбор учетных записей по словарям. Сканирование проводится в нерабочее время.

В случае если антивирусное средство имеет встроенные функции межсетевого экрана, их необходимо отключить по возможности на этапе установки продукта, либо после установки в настройках антивирусного средства. Межсетевой экран антивируса может конфликтовать со встроенным межсетевым экраном средства ViPNet Client.

Средство защиты информации от несанкционированного доступа устанавливается на каждый АРМ пользователей РЕГИСЗ ПК. После установки добавляются пользователи, которым разрешен вход в систему и обработка конфиденциальной информации в панели «учетные записи». В том числе пользователи, создаваемые средствами защиты информации (например, vipnet_user). В панели «контроль доступа» все настройки остаются без изменения.

Для СЗИ от НСД устанавливаются следующие параметры безопасности:

- Вход: запрет смены пользователя без перезагрузки – Выкл.;
- Вход: отображать имя последнего пользователя – Да;
- Вход: максимальное количество ошибок ввода пароля – 8;
- Вход: время блокировки учетной записи в случае ввода неправильных паролей (минут) - 10;
- Вход: отображать время последнего успешного входа – Нет;
- Вход: запрет одновременной работы пользователей с различными уровнями конфиденциальности – Выкл.;
- Сервер безопасности – Не задан;

- Пароли: максимальный срок действия пароля -90 дн.;
- Пароли: минимальный срок действия пароля – 10 дн.;
- Пароли: напоминать о смене пароля за – 14 дн.;
- Пароли: минимальная длина – 6 симв.;
- Пароли: необходимо наличие цифр – Да;
- Пароли: необходимо наличие спец. символов – Да;
- Пароли: необходимо наличие строчных и прописных букв – Да;
- Пароли: необходимо отсутствие цифры в первом и последнем символе – Нет;
- Пароли: необходимо изменение пароля не меньше чем в – 2 симв.;
- Сеть: Ключ удаленного доступа – оставить по умолчанию;
- Сеть: Время хранения сетевого кэша – оставить по умолчанию;
- Сеть: Список незащищенных серверов – оставить по умолчанию;
- Блокировать компьютер при отключении аппаратного идентификатора – нет.

Для СЗИ от НСД устанавливаются следующие параметры аудита:

- Аудит входа в систему – Вкл.;
- Аудит доступа к ресурсам – Вкл.;
- Аудит управления политиками безопасности – Вкл.;
- Аудит управления учетными записями – Вкл.;
- Аудит печати – Выкл.;
- Аудит запуска/завершения процессов – Вкл.;
- Фиксировать в журнале входов неправильные пароли – Да;
- Аудит доступа: Заносить в журналы ошибки Windows – Да;
- Аудит доступа: Заносить в журналы все ошибки при включенном «мягком» режиме – Да;
- Заносить в журнал события запуска и остановки ОС – Да;
- Заносить в журнал события запуска и остановки модулей администрирования DL – Да;
- Аудит доступа/запуска: Вести аудит системных пользователей – Да;
- Печать штампа – Нет;
- Создавать теневые копии распечатываемых документов – Нет;
- Разрешить печать из под уровней доступа – Все уровни;
- Добавлять штамп при печати под уровнями – Все уровни;

На подготовительном этапе средство защиты сетевого трафика и межсетевой экран ViPNet Client устанавливается только в качестве межсетевого экрана. Ключевую информацию для шифрования сетевого трафика МО получает от Оператора только после предъявления аттестата соответствия.

В случае подключения к РЕГИСЗ ПК локальных сетей Оператора от 5 АРМ и более, допускается использование вместо хостового решения ViPNet Client использовать шлюзовое решение ViPNet Coordinator. При таком варианте подключения МО должна гарантировать физическую сепарацию локальной сети, подключаемой к РЕГИСЗ ПК от остальной сети МО.

3.4 Аттестация информационной системы по требованиям защиты информации

Оператором РЕГИСЗ ПК принято решение осуществлять построение системы защиты информации в соответствии с положениями Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных Приказом ФСТЭК России №17 от 11.02.2013 (пункт 6 приказа ФСТЭК № 17: «По решению обладателя информации (заказчика) или оператора настоящие Требования могут применяться для защиты информации, содержащейся в негосударственных информационных системах»).

Подсистемы РЕГИСЗ ПК аттестованы по принципу типовых сегментов. На сегменты МО могут быть распространены результаты аттестационных испытаний центрального сегмента РЕГИСЗ ПК (или одной из подсистем) в случае выполнения на них организационных и технических мер по защите информации в соответствии с установленным классом защищенности РЕГИСЗ ПК или одной из подсистем.

Оформление заключения о соответствии сегмента РЕГИСЗ ПК требованиям по защите информации осуществляется организацией-лицензиатом ФСТЭК России на работы по ТЗКИ после внедрения системы защиты информации, и утверждения внутренних организационно-распорядительных документов по защите информации.

В случае решения МО о самостоятельной организации построения системы защиты информации сегмента РЕГИСЗ ПК, МО подтверждает Оператору выполнение мер по защите информации путем предоставления любых запрашиваемых документов в виде скан-копий (приказы, инструкции, журналы, скриншоты с настройками средств защиты информации, отчеты по результатам сканирования на наличие уязвимостей и т. д.).

В случае получения отрицательного заключения или несоответствия системы защиты информации сегмента РЕГИСЗ ПК установленным требованиям, МО оперативно устраняет выявленные аттестующим органом или Оператором нарушения и проводит дополнительные испытания сегмента РЕГИСЗ ПК на соответствие требованиям по защите информации.

3.5 Ввод сегмента РЕГИСЗ ПК в эксплуатацию и заключение соглашения о подключении к РЕГИСЗ ПК

МО направляет Оператору скан-копию заключения о соответствии сегмента РЕГИСЗ ПК требованиям по защите информации, скан-копию акта о вводе сегмента РЕГИСЗ ПК в эксплуатацию и список пользователей системы со стороны МО с указанием ФИО и необходимых полномочий в системе для каждого пользователя.

Оператор в ответ направляет в МО проект соглашения о подключении к РЕГИСЗ ПК, приведенном в Приложении № 2 настоящего документа (далее - Соглашение), а также проект регламента работы с ресурсами РЕГИСЗ ПК, приведенном в Приложении № 3 настоящего документа (далее - Регламент). Соглашение и Регламент согласовываются и подписываются с обеих сторон.

3.6 Подключение к РЕГИСЗ ПК

На основании подписанных Соглашения и Регламента Оператор выдает МО:

- логины и первичные пароли для каждого пользователя для доступа к подсистемам РЕГИСЗ ПК;
- ключевую информацию в виде dst-файла, для подключения ViPNet Client или ViPNet Coordinator к защищенной сети Оператора;
- парольную фразу к dst-файлу.

Dst-файл передается МО ответственным лицом Оператора на машинном носителе лично или иным доверенным способом (например, спецпочтой или по уже функционирующему защищенному каналу связи).

После установки dst-файла МО может приступать к работе с ресурсами РЕГИСЗ ПК.

Приложение № 1

к Регламенту подключения к РЕГИСЗ ПК

Директору

ГАУЗ «ПК МИАЦ»

Волковой М. В.

ЗАЯВКА

на подключение к РЕГИСЗ ПК

Просим Вас с целью организации подключения автоматизированных рабочих мест «Название МО» к РЕГИСЗ ПК предоставить нам следующую документацию:

- выписку из документа «Модель угроз безопасности информации в РЕГИСЗ ПК»;
- выписку из документа «Частное техническое задание на создание системы защиты информации РЕГИСЗ ПК»;
- комплект шаблонов внутренних организационно-распорядительных документов по защите информации.

Руководитель МО Дата

Приложение № 2

к Регламенту подключения к РЕГИСЗ ПК

СОГЛАШЕНИЕ

о подключении к РЕГИСЗ ПК

ГАУЗ «ПК МИАЦ» (далее - Оператор) и «Название МО» (далее - МО) заключили настоящее соглашение о нижеследующем.

Оператор на основании аттестата соответствия требованиям по защите информации сегмента РЕГИСЗ ПК № ___ от _____ предоставляет доступ к ресурсам РЕГИСЗ ПК через сеть интернет по защищенным каналам связи.

Оператор предоставляет МО методическую и консультационную поддержку по подключению к РЕГИСЗ ПК и по вопросам, связанным с эксплуатацией системы.

МО обязуется выполнять в процессе эксплуатации РЕГИСЗ ПК требования по защите информации.

МО обязуется обеспечить продление аттестата соответствия требованиям по защите информации по окончании срока его действия или уведомить Оператора о невозможности продления срока действия аттестата соответствия.

МО обязуется выполнять требования Регламента работы с ресурсами РЕГИСЗ ПК.

Директор	Руководитель
ГАУЗ «ПК МИАЦ»	Название МО
М. В. Волкова	И. И. Иванов

Приложение № 3

к Регламенту подключения к РЕГИСЗ ПК

РЕГЛАМЕНТ

работы с ресурсами РЕГИСЗ ПК

1. Общие положения

Настоящий Регламент определяет порядок работы МО с ресурсами РЕГИСЗ ПК.

Подключение МО к РЕГИСЗ ПК возможно только при выполнении ими требований законодательства по защите информации, получения аттестата соответствия, соответствия подключаемых АРМ пункту 4 Технических требований на подключение к РЕГИСЗ ПК.

Подключение МО к РЕГИСЗ ПК осуществляется в порядке, описанном в пункте 3 Технических требований на подключение к РЕГИСЗ ПК.

2. Функции Оператора

Оператор обеспечивает:

- непрерывное функционирование и техническое обслуживание серверной части РЕГИСЗ ПК;
- технологическое сопровождение, эксплуатацию и развитие программно-аппаратных средств системы и телекоммуникационной инфраструктуры, обеспечивающей ее функционирование;
- консультационную поддержку участников информационного взаимодействия по вопросам работы с системой;
- взаимодействие с разработчиками системы по вопросам совершенствования РЕГИСЗ ПК;
- формирование аутентификационной и ключевой информации для Пользователей системы;
- соблюдение требований информационной безопасности в центральном сегменте информационной системы, в том числе защиту от несанкционированного доступа;
- защиту персональных данных, обрабатываемых в РЕГИСЗ ПК.

3. Функции и обязанности МО

МО обеспечивают:

- актуальность перечня уполномоченных сотрудников, допущенных к работе с РЕГИСЗ ПК;
- назначение лиц, ответственных за защиту информации;

- выполнение требований по защите информации в РЕГИСЗ ПК;
- актуальность и корректность сведений, вносимых в систему;
- предоставление информации по запросу Оператора.

4. Порядок осуществления авторизованного доступа к РЕГИСЗ ПК участников информационного взаимодействия

При обращении МО с целью обеспечения авторизованного доступа к РЕГИСЗ ПК Оператор обеспечивает рассмотрение поступивших от них заявок и актуализацию перечня МО, подключенных к РЕГИСЗ ПК, в соответствии с результатами рассмотрения поступивших заявок.

При обращении МО с целью обеспечения средствами авторизованного доступа и ключевой информации для защиты сетевого трафика уполномоченных сотрудников МО, Оператор обеспечивает: регистрацию пользователей в системе и назначение им прав доступа к системе на основе ролевой системы разграничения доступа, направление аутентификационных данных в МО, ведение перечня пользователей РЕГИСЗ ПК, консультационную поддержку по первоначальному входу в систему.

Для подключения к РЕГИСЗ ПК МО направляют заявку за подписью руководителя Оператору.

Оператор принимает решение о возможности подключения МО к РЕГИСЗ ПК и в течение 3 рабочих дней со дня получения запроса направляет МО необходимые для подключения документы и инструкции.

Доступ к РЕГИСЗ ПК предоставляется на основании заключения о соответствии требованиям по защите информации сегмента РЕГИСЗ ПК МО.

В случае реорганизации МО или ликвидации МО, Оператору направляется уведомление о реорганизации МО (ликвидации) за подписью руководителя МО. На основании такого уведомления Оператор блокирует учетные записи пользователей реорганизуемой или ликвидируемой МО, а также вносит изменения в перечень МО, подключенных к РЕГИСЗ ПК.

Все участники информационного взаимодействия несут ответственность за полноту, корректность и достоверность размещаемых ими в РЕГИСЗ ПК сведений.