|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **«УТВЕРЖДено»** | |  |  | |
| Начальник управления здравоохранения Липецкой области | |  |  | |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |  |  |
| «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_2017 г. | |  |  | |

ГОСУДАРСТВЕННАЯ ИНФОРМАЦИОННАЯ СИСТЕМА

РЕГИОНАЛЬНАЯ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКАЯ МЕДИЦИНСКАЯ СИСТЕМА В СФЕРЕ ЗДРАВООХРАНЕНИЯ ЛИПЕЦКОЙ ОБЛАСТИ

(ГИС РИАМС)

ТЕХНИЧЕСКИЕ УСЛОВИЯ   
по подключению к ГИС РИАМС объектов (сегментов, АРМ) негосударственных медицинских организаций

*РДМТ-УЗО48-СЗИ.17 – НМО ТУ*

**2017**

**Список сокращений**

|  |  |  |
| --- | --- | --- |
| АРМ |  | Автоматизированное рабочее место |
| АС |  | Автоматизированная система |
| АПКШ |  | Аппаратно-программный комплекс шифрования |
| ГИС |  | Государственная информационная система |
| ИС |  | Информационная система |
| КШ |  | Криптографический шлюз |
| ЛВС |  | Локально-вычислительная сеть |
| МЭ |  | Межсетевой экран |
| НСД |  | Несанкционированный доступ |
| ОС |  | Операционная система |
| ОИ |  | Объект информатизации |
| ПК |  | Программный комплекс |
| ПО |  | Программное обеспечение |
| ПТС |  | Программно-техническое средство |
| ПЭВМ |  | Персональная электронно-вычислительная машина |
| САВЗ |  | Средство антивирусной защиты |
| СЗИ |  | Система защита информации |
| СКЗИ |  | Система криптографической защиты информации |
| СрЗИ |  | Средства защиты информации |
| ТУ |  | Технические условия |
| ФСБ |  | Федеральная служба безопасности |
| ФСТЭК |  | Федеральная служба по техническому и экспортному контролю |

ПОРЯДОК

подключения негосударственных медицинских организаций к государственной региональной информационно-аналитической медицинской системы в сфере здравоохранения Липецкой области (РИАМС)

**1. Этап «Организация подключения к РИАМС через ЗСПД РИАМС в тестовом режиме»**

1.1. Этап выполняется на период подготовки и реализации (выполнения) медицинской организацией (МО) требований по работе пользователейв РИАМСв защищенном режиме.

1.2. На этапе **«Организация подключения к РИАМС … в тестовом режиме»** выполняются:

а) подачаМОзаявки на организацию защищенного подключенияксерверу РИАМС (ПО КВАЗАР) через защищенную сеть передачи данных (ЗСПД) РИАМС;

Форма заявки приведена в Приложении А.

Заявка формируется в зависимости от следующих исходных данных (условий) МО:

- номера ViPNet сети, к которой уже подключена МО;

- типа ViPNet средств (программный или программно-аппаратный комплекс средств криптографической защиты информации (СКЗИ) и средств межсетевого экранирования (МЭ)), которые имеются в МО (или отсутствуют и будут закуплены), подключаемых к ЗСПД РИАМС;

- количества автоматизированных рабочих местах (АРМ) сотрудников МО, подключаемых к РИАМС (ПО КВАЗАР).

б) анализ заявки МО, включая: определение подключаемых АРМ пользователей РИАМС (АРМ пользователей ПО КВАЗАР), определение задействованных в подключенииViPNet средств, определение задействованных в подключенииViPNet сетей;

в) подключение АРМ пользователей – сотрудников МО к серверу РИАМС (сервер ПО КВАЗАР) по защищенным каналам связи в тестовом режиме.

Варианты реализации подключения АРМ пользователей к ГИС РИАМС по защищенным каналам связи приведены в Приложении Б.

в) уточнение сведений по составу АРМ (сегментаЛВС) МО, на которых будет осуществляться работа в РИАМС, в том числе обработка защищаемой в РИАМС информации (персональные данные, врачебная тайна). Далее данные АРМ МО именуются: «АРМ РИАМС». При работе с РИАМС отдельных сетевых сегментов ЛВС МО, выделенных в сегмент виртуально или физически: «Удаленный сегмент РИАМС».

Сведения по АРМ, на которых разворачивается клиентское ПО РИАМС(ПО КВАЗАР) ибудет осуществляться работа в РИАМС, в том числе обработка защищаемой в РИАМС информации, – сообщаются в первичной заявке МО (Приложение А).

г) настройка в РИАМС прав (полномочий) пользователям РИАМС– сотрудникам МО по обработке информации, в том числе персональных данных в РИАМС.

Работа с пользователям РИАМС– сотрудникам МО, их правам (полномочиям) по обработке информации в РИАМС, – производитсяв порядке, указанном в Приложении В.

При отсутствии в МО кадровой и/или технической возможности выполнить работы по установке на АРМ сотрудников МО клиентское ПО РИАМС (ПО КВАЗАР), – МО может привлекать к данным услугам организации, имеющие соответствующий опыт работы с ПО РИАМС (ПО КВАЗАР).

д) уточнение версионности СКЗИ и средств МЭ МОк версиям СКЗИ/МЭв ЗСПД РИАМС;

Для анализа версионности МО должны будут представить копии документов, подтверждающих легитимность приобретения и использования СКЗИ и средств МЭ(средств ViPNet). Форма сведений (скан-копия листов Формуляра на СКЗИ и средства МЭ) приведена в Приложении А (приложениеА1 Заявки).

Анализ совместимостиверсионности СКЗИ и средств МЭ (средства ViPNet) МО с применяемыми в ЗСПД РИАМС версиями СКЗИ/МЭ осуществляется в процессе работы МО с РИАМС в тестовом режиме по защищенным каналам связи ЗСПД РИАМС.

**2. Этап «Выполнение (реализация) на АРМ РИАМС (в удаленном сегменте РИАМС) МОправил работы в РИАМС, в том числе мер по защите информации, оценка соответствия установленным в РИАМС правилам работы с информацией (персональными данными), правилам (требованиям) безопасностиинформации»**

2.1. Выполняется в период работы МО в РИАМСв тестовом режиме, в целях выполнения (реализации) на АРМ РИАМС (в сегменте РИАМС) правил работы в РИАМС, в том числе мер по защите информации.

2.2. Данный этап завершаетсямероприятиями по оценке соответствия установленным в РИАМС правиламработы с информацией (персональными данными), правилам (требованиям) безопасности информации.

2.3. На данном этапе, до мероприятий по оценке соответствия, должны быть завершены и выполнены:

а) реализована схема защищенного режима подключения и взаимодействия с РИАМС (в соответствии с приложением Б);

б) СКЗИ и средств МЭ МОприведены к версиям СКЗИ/МЭв ЗСПД РИАМС.

При необходимости «поднятия» версионности МО должна будет закупить пакет обновлений (модернизации) для своих СКЗИ и средств МЭ и выполнить работы по обновлению СКЗИ и средств МЭ. Закупка пакетов обновлений (модернизации) для СКЗИ и средств МЭ осуществляется через организацию-производителя средств ViPNet или ее партнеров.

При отсутствии в МО кадровой и/или технической возможности выполнить работы по обновлению СКЗИ и средств МЭ, – МО может привлекать к данным услугам организацию – лицензиата ФСТЭК и ФСБ России, имеющего соответствующий опыт работы со средствами защиты информации ViPNet;

в) внедрены организационные мероприятия по обработке и защите информации для удаленныхсегментов РИАМС (перечень необходимых организационных мер защиты информации приведен в Приложении Г).

В целях внедрения организационных мероприятий по обработке и защите информации, по запросу МО могут быть предоставлены шаблоны отдельных документов.

При отсутствии в МО кадровой и/или иной возможности подготовки к внедрению организационных мероприятий по обработке изащите информации – МО может привлекать к данным услугам организацию-лицензиата ФСТЭК и ФСБ России, имеющего соответствующий опыт работы;

г) реализованы технические меры защиты информации для удаленныхсегментов РИАМС (перечень необходимых технических мер защиты информации и частные технические требования по защите информации АРМ и сегментов РИАМС приведены в Приложении Д).

В целях реализации технических мер по защите информации на АРМ РИАМС (в сегменте РИАМС) подготовлены частные технические решения, – в зависимости от варианта защищенного подключения к РИАМС, порядка организации удаленного сегмента РИАМС в МО,состава АРМ.

При отсутствии в Организации кадровой и/или технической возможности представить к контролю выполнение (реализацию) вышеперечисленных задач – Организация может привлекать к работам по внедрению (установка, настройка конфигураций) средств защиты информации лицензиата ФСТЭК и ФСБ России, имеющего опыт работы с СКЗИ, средствами МЭ, средствами антивирусной защиты (АВЗ), средствами защиты от несанкционированного доступа (НСД), опыт подготовки и проведения аттестационных испытаний.

2.4. Оценка соответствия включает следующие контрольные мероприятия:

а) проверкуналичия в МО лиц, ответственных за обработку, защиту информации и эксплуатацию средств защиты информации, назначенных приказом Руководителя МО;

б) проверку наличия актуальных списков пользователей РИАМС – сотрудников МО, утвержденных приказом Руководителя МО;

в) анализ реализациив МОорганизационных мер по обработке и защите информации (прим. в части контроля доступа к средствам обработки информации, а также в помещенияМО, в которых размещены АРМ РИАМС);

г) проверку наличия в МОактуальной эксплуатационной документации (формуляры) на используемые СКЗИ и средства защиты информации;

д) анализ реализации в МОтехнических мер по защите информации (прим. в частипроверки наличия и контроля настроекСКЗИ и средств защиты информации на АРМ РИАМС,в удаленном сегменте РИАМС);

е) вывод о соответствии медицинской организации установленным в РИАМС правилам обработки информации (персональных данных), правилам (требованиям) безопасности информации.

**В целях проведения оценки соответствия**МО должна будет предоставить сканы (копии) следующих документов:

а) копия приказа Руководителя МОо назначении сотрудника (сотрудников) МО, ответственного за обработку персональных данных, за защиту информации и за эксплуатацию средств защиты информации МО;

б) копия актуального списка сотрудников МО, допущенных к работе в РИАМС, – пользователей РИАМС;

в) копия приказа Руководителя МОо выполнении мероприятий поорганизации защиты информации в удаленном сегменте РИАМС МО;

г) копия листа ознакомления сотрудников МО – пользователей РИАМС с документами по организации защиты информации в удаленном сегменте РИАМС;

д) копии формуляров на средства защиты информации:

- копия титульного листа с указанием типа средства защиты информации;

- копия листов с указанием серийных/заводских номеров средства защиты информации;

- копия листов «Свидетельство о приемке», «Свидетельство об упаковке и маркировке»;

е) копия лицензии (право обладания) средством зашиты информации;

ж) копия дистрибутивного комплекта на средство зашиты информации;

з) копия технического паспортаудаленного сегмента РИАМС (или технических паспортов отдельных АРМ пользователей РИАМС):

- копия титульного листа с указанием объекта информатизации;

- копии листов с общими сведениями об объекте информатизации, листов со сведениями об основных технических средствах и системах (ОТСС), программном обеспечении и средствах защиты информацииобъекта информатизации(с указанием серийных/заводских номеров), листов со схемами размещения относительно границ контролируемой зоны организации, листов со сведениями об аттестации на соответствие требованиям безопасности информации (при наличии);

д) скриншоты (снимки экрана), подтверждающие выполнение необходимых конфигурационных настроек средств защиты информации, установленных на АРМ РИАМС, в удаленном сегменте РИАМС.

По запросу МО могут быть предоставлены инструкции по предоставлению скриншотов (снимки экрана), подтверждающих выполнение необходимых конфигурационных настроек средств защиты информации.

**По результатам анализа предоставленных материалов** – копий документов МО, – будет выполнена оценка соответствия медицинской организации установленным в РИАМС правилам работы с информацией (персональными данными), правилам (требованиям) безопасности информации.

Приложение А

**Заявка**

**на подключение медицинской организации (МО) к государственной информационной системе (ГИС) региональной информационно-аналитической медицинской системы в сфере здравоохранения Липецкой области (РИАМС)**

1. **Общие сведения об организации**

|  |  |  |  |
| --- | --- | --- | --- |
| **Полное наименование организации без сокращений (на основании учредительных документов)** |  | | |
| **Почтовый адрес организации** |  | | |
| **Юр. адрес организации** |  | | |
| **Руководитель организации (ФИО, должность)** |  | | |
| **Данные об сотрудниках** | ФИО | Должность | Контактные данные |
| Должностные лица, ответственные за подключение к РИАМС (ПО КВАЗАР) |  |  | *Рабочий телефон*  *Мобильный телефон*  *Е-mail* |
| Должностное лицо, ответственное за защиту информации |  |  | *Рабочий телефон*  *Мобильный телефон*  *Е-mail* |

1. **Техническая спецификация на доступ к ресурсам РИАМС:**

Номер ViPNet сети, к которой уже подключена Организация

|  |  |  |  |
| --- | --- | --- | --- |
| ViPNet сеть ТФОМС (№641) | ViPNet сеть УЗО (№1702) | ViPNet сеть самой Организации (№\_\_\_) | Отсутствует подключение к перечисленным ViPNet сетям |
|  |  |  |  |

Тип ViPNetсредства (программный комплекс (ПК) или программно-аппаратный комплекс средств криптографической защиты информации (СКЗИ) и средств межсетевого экранирования (МЭ)), имеющийся у Организации

|  |  |  |  |
| --- | --- | --- | --- |
| ViPNetClient (указать наименование абонентского пункта/узла) | ViPNetCoordinator аппаратный (HW\_\_\_\_) | ViPNetCoordinator программный | Нет ViPNetсредства (не приобретены) |
|  |  |  |  |

Сведения о ViPNetсредствах, имеющихся в Организации

|  |  |  |  |
| --- | --- | --- | --- |
| Регистрационный номер СКЗИ/МЭ  (номер ViPNet средства) | Серийный номер дистрибутива  СКЗИ/средства МЭ | Серийный/заводской номер СКЗИ и средств МЭ (прим. указано в формуляре на СКЗИ или в наклейке на устройстве) | Версия СКЗИ/МЭ (версия ViPNet средства) |
|  |  |  |  |

Сведения об автоматизированных рабочих местах (АРМ) сотрудников МО, подключаемых к РИАМС

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Порядковый номер  (или наименование) АРМ МО | Серийный или инвентарный номер системного блока АРМ | Версия операционной системы (ОС) (указать полностью, включая разрядность 32/64) | Название абонентского пункта  (если установлен ViPNetClient) | Ответственный за АРМ с правами администратора ОС  (ФИО, должность, контакты) | Пользователи АРМ  (ФИО, должность, контакты) |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

|  |  |  |
| --- | --- | --- |
|  |  |  |
| *Должность* | *подпись\** | *Фамилия. Инициалы* |

м.п.

*\*прим. Подпись и печать ставятся на 1 экз. заявки.*

*2-й экз. заявки отправляется в электронном виде.*

**Приложение А1**

**Скан-копия листов Формуляра на СКЗИ и средства МЭ**

*- титульный лист с указанием типа средства криптографии;*

*- листы с указанием серийных/заводских номеров средства криптографии и средства межсетевого экранирования (МЭ)\*\*;*

*- раздел №5 формуляра «Свидетельство о приемке и маркировке».*

*\*\*прим. для устаревших ViPNetсредств возможно наличие двух отдельных формуляров. В таком случае выслать необходимо скан-копии с обоих документов.*

Приложение Б

**Варианты схем реализации защищенного подключения   
и взаимодействия АРМ пользователей с ГИС РИАМС**

**Вариант 1 реализации защищенного взаимодействия с ГИС РИАМС**



Рисунок 1. Схема реализации защищенного взаимодействия с ГИС РИАМС (вариант 1)

Схема по варианту 1 предполагает следующее защищенное подключение АРМ пользователей:

– к ГИС РИАМС по криптозащищенному каналу СЗИ ГИС РИАМС через VipNetсеть №641 (VipNetсеть территориального фонда обязательного медицинского страхования Липецкой области (далее – ТФОМС ЛО)).

Шаги по реализации варианта 1 защищенного взаимодействия:

1. Для доступа к ГИС РИАМС на АРМ пользователя устанавливается клиент средств криптографической защиты информации (СКЗИ) и средств МЭ (далее – СКЗИ/МЭ) «ViPNetClient» сети № 641ТФОМС ЛО, подключаемый к КШ СЗИ ГИС РИАМС через межсетевое взаимодействие между VipNetсетью 641 и VipNetсеть 1702 (VipNetсеть Управления).

Указанные требования и порядок защищенного подключения уточняются и согласовываются с администратором информационной безопасностиУправления.

**Вариант 2 реализации защищенного взаимодействия с ГИС РИАМС**



Рисунок 2. Схема реализации защищенного взаимодействия с ГИС РИАМС (вариант 2)

Схема по варианту 2 предполагает следующее защищенное подключение АРМ пользователей:

– к ГИС РИАМС по криптозащищенному каналу СЗИ ГИС РИАМС через VipNetсеть № 1702 (VipNetсеть Управления).

Шаги по реализации варианта 2 защищенного взаимодействия:

1. Для доступа кГИС РИАМС на АРМ пользователя устанавливается клиент средств СКЗИ ViPNetClient» сети № 1702Управления, подключаемый к КШ СЗИ ГИС РИАМС.

Указанные требования и порядок защищенного подключения уточняются и согласовываются с администратором информационной безопасностиУправления.

**Вариант 3 реализации защищенного взаимодействия с ГИС РИАМС при подключении к ГИС РИАМС через криптошлюз VipNet сети Управления или собственную VipNet сеть**



Рисунок 3. Схема реализации защищенного взаимодействия с ГИС РИАМС (вариант 3)

Схема по варианту 3 предполагает следующие возможные защищенные подключения АРМ пользователей к ГИС РИАМС:

– путем установки КШ ViPNet сети № 1702 сети Управления;

– путем использования КШ собственной ViPNet сети Учреждения, с настройкой межсетевого взаимодействия c криптографической сетью ЗСПД РИАМС (с ViPNet сетью № 1702).

При этом, подключение АРМ пользователей к указанным КШ должно производиться:

– по криптозащищенному каналу ViPNet сети (прим. сети № 1702ЗСПД РИАМС или собственной ViPNet сети) – от АРМ пользователя к КШ своего объекта (прим. сети № 1702 ЗСПД РИАМС или – собственной ViPNet сети) через открытые каналы ЛВС своего объекта – к СЗИ ИС РИАМС.

Шаги по реализации варианта 4 защищенного взаимодействия:

1. Организация доверенного канала внутри объекта. Реализуется тремя возможными способами:
   1. Для организации криптозащищенного канала внутри ЛВС объекта на АРМ пользователя устанавливается клиент СКЗИ/МЭ «ViPNetClient» ViPNet сети № 1702Управления, подключаемый к КШ СЗИ ГИС РИАМС.
   2. Для организации криптозащищенного канала внутри ЛВС объекта на АРМ пользователя устанавливается клиент СКЗИ/МЭ «ViPNetClient» собственной ViPNet сети объекта, подключаемый к КШ своей ViPNet сети и, далее, через межсетевое взаимодействие – к ViPNet сети № 1702 ЗСПД РИАМС.
   3. Для организации доверенного канала в ЛВС объекта, АРМ пользователя должен входить (должен быть подключен) в существующий или создаваемый в ЛВС объекта выделенный сегмент сети. Периметр указанного выделенного сетевого сегмента должен быть защищен средствами МЭ с реализацией правил безопасности (политик безопасности) согласованной с Управлением разрешительной системы доступа.
2. Организация защищенного межсетевого взаимодействия между криптографической сетью Управления (ViPNet сеть № 1702) и ViPNet сетью объекта (прим. пункт выполняется в случае использования КШ собственной ViPNet сети):

– должно быть организовано защищенное межсетевое взаимодействие криптографических сетей, по согласованию с Управлением, между собственной сетью и сетью ЗСПД РИАМС;

– должно быть обеспечено, по согласованию с Управлением, соответствие версионности и класса защиты СКЗИ собственной ViPNet сети и СКЗИ ЗСПД РИАМС, в целях правильного и корректного взаимодействия криптозащищенных сетей.

1. По завершении реализации п. 1-2, по согласованию с Управлением производится настройка защищенного взаимодействия указанных АРМ пользователей путем корректировки разрешительной системы доступа СЗИ ГИС РИАМС.

Указанные требования и порядок защищенного подключения уточняются и согласовываются с администратором информационной безопасности ГИС РИАМС.

Приложение В

**Получение доступа к РИАМС – сотрудникам МО, их правам (полномочиям) по обработке информации в РИАМС**

Шаги дляполучения доступа к РИАМС:

1. Завести физических лиц в ПО КВАЗАР, службу поддержки формы сведений:

| **№**  **п/п** | **Фамилия Имя Отчество** | **Дата рождения** | **СНИЛС** | **Примечание** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |

1. Дождаться ответа от службы поддержки о заведении указанных физических лиц;
2. В кадровом модуле ПО КВАЗАР завести физических как сотрудников;
3. Для создания пользователей и наделения их правами предоставить путем отсылки в службу поддержки следующие данные:

| **№**  **п/п** | **ФИО пользователя** | **Должность** | **Подразделение** | **Необходимые права** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |

1. Дождаться ответа службы поддержки с присвоенными пользователям учетными данными (логины и пароли) для работы в системе.

Приложение Г

**Перечень организационных мер обработки и защиты информации на объектах, подключаемых к ГИС РИАМС (для всех типов подключения)**

На объектах, подключаемых к ГИС РИАМС, необходимо выполнить следующие организационные мероприятия, направленные на реализацию правил обработки и на защиту информации ограниченного доступа, не являющейся государственной тайной, обрабатываемой в ГИС РИАМС:

1. назначить администратора информационной безопасности, подключаемого к ГИС РИАМС объекта (ОИ или Учреждения) (форма приказа приведена в Приложении Г2);
2. определить перечень лиц, допущенных к работе с ГИС РИАСМ;
3. организовать контролируемую зону объекта, системы контроля доступа в помещения, в которых размещены основные технические системы и средства обработки информации (ОТСС) ОИ;
4. организовать контроль доступа пользователей при работе с ГИС РИАМС;
5. организовать управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены;
6. разработать и довести до пользователей ГИС РИАМС (под роспись) положения следующих организационно-распорядительных документов по защите информации, обрабатываемой в ГИС РИАМС:

* Положения по организации работ по обеспечению безопасности информации, обрабатываемой на объектах информатизации, подключаемых к ГИС РИАМС.
* Инструкция администратору информационной безопасности объектов информатизации, подключаемых к ГИС РИАМС;
* Положение об организации режима безопасности помещений, в которых размещены объекты информатизации,подключаемые к ГИС РИАМС.
* Инструкция ответственного пользователя средств криптографической защиты информации, применяемых на объектах информатизации,подключаемых к ГИС РИАМС.
* Инструкция по организации антивирусной защиты на объектах информатизации,подключаемых к ГИС РИАМС.
* Инструкция по организации парольной защиты на объектах информатизации,подключаемых к ГИС РИАМС.
* Инструкция пользователя объектов информатизации на объектах информатизации,подключаемых к ГИС РИАМС.
* Инструкция по организации хранения, учета и работы с материальными носителями информации ограниченного доступа, в том числе с машинными носителями информации.
* Инструкция по регистрации, выявлению и реагированию на инциденты (события безопасности).
* Инструкция по организации учета, хранения и эксплуатации средств защиты информации.
* Инструкция по восстановлению связи в случае компрометации действующих ключей к средствам криптографической защиты информации.
* Инструкция по уничтожению ключевой информации к средствам криптографической защиты информации.

1. назначить ответственных за помещения, в которых расположены АРМ, подключаемые к ГИС РИАМС;
2. разработать следующие эксплуатационные документы на АРМ, подключаемые к ГИС РИАМС:

* Технический паспорт ОИ;
* Журнал учета материальных учета машинных носителей информации ограниченного доступа;
* Журнал учета используемых криптосредств, эксплуатационной и технической документации к ним, ключевых документов;
* Журнал учета лиц, допущенных к средствам криптографической защиты информации (форма);
* Журнал учета мероприятий по обеспечению контроля состояния защиты информации на АРМ, подключаемых к ГИС РИАМС.

1. утвердить План мероприятий по обеспечению контроля состояния обеспечения безопасности информации ОИ, подключаемого к ГИС РИАМС (типовая форма плана представлена в приложение В.1).

Приложение Г1

**Типовая форма приказа «О выполнении мероприятий, направленных на обеспечение защиты информации, обрабатываемой на объектах информатизации, подключаемых к ГИС РИАМС»**

**ПРИКАЗ**

“ \_\_ ” \_\_\_\_2017 г. № \_\_\_\_

г. Липецк

О выполнении мероприятий, направленных на обеспечение защиты информации, обрабатываемой на объектах информатизации, подключаемых к ГИС РИАМС

С целью организации работ по обеспечению безопасности информации ограниченного доступа, не являющейся государственной тайной (в том числе, персональных данных(ПДн)) обрабатываемой на объектах информатизации (ОИ) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(далее – Учреждение), подключаемых к Государственной региональной информационно-аналитической медицинской системы в сфере здравоохранения Липецкой области (далее - ГИС РИАМС) и во исполнение требований Федерального закона Российской Федерации от 27.06.2006 г. № 152-ФЗ «О персональных данных» и Федерального закона Российской Федерации от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и защите информации», нормативных, методических и руководящих документов уполномоченных федеральных органов исполнительной власти,

ПРИКАЗЫВАЮ:

1. Определить следующие ОИ, подключаемые к ГИС РИАМС:

- ОИ «*Типовое АРМ ГИС РИАМС \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*»

2. Назначить администратором безопасности ОИ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. В своей деятельности администратору информационной безопасности руководствоваться «Инструкцией администратору информационной безопасности объектов информатизации, подключаемых к ГИС РИАМС» и «Положением по организации работ по обеспечению безопасности информации, обрабатываемой на объектах информатизации, подключаемых к ГИС РИАМС».

3. Возложить на администратора безопасности функции ответственного пользователя СКЗИ. Ответственному пользователю в своей деятельности руководствоваться «Инструкцией ответственного пользователя средств криптографической защиты информации, применяемых на объектах информатизации, подключаемых к ГИС РИАМС».

4. Допустить к работе на ОИ (в том числе к работе со средствами криптографической защиты информации) следующих сотрудников Учреждения (пользователей ОИ):

*- ФИО, должность*

5. Пользователей ОИ ознакомить под роспись со следующими организационно-распорядительными документами:

- Положение об организации режима безопасности помещений, в которых размещены объекты информатизации, подключаемые к ГИС РИАМС.

- Инструкция ответственного пользователя средств криптографической защиты информации, применяемых на объектах информатизации, подключаемых к ГИС РИАМС.

- Инструкция по организации антивирусной защиты на объектах информатизации, подключаемых к ГИС РИАМС.

- Инструкция по организации парольной защиты на объектах информатизации, подключаемых к ГИС РИАМС.

- Инструкция пользователя объектов информатизации на объектах информатизации, подключаемых к ГИС РИАМС.

- Инструкция по организации хранения, учета и работы с материальными носителями информации ограниченного доступа, в том числе с машинными носителями информации.

- Инструкция по регистрации, выявлению и реагированию на инциденты (события безопасности).

- Инструкция по организации учета, хранения и эксплуатации средств защиты информации.

- Инструкция по восстановлению связи в случае компрометации действующих ключей к средствам криптографической защиты информации.

- Инструкция по уничтожению ключевой информации к средствам криптографической защиты информации.

6. Назначить ответственными за помещения, в которых расположены ОИ, подключаемые к ГИС РИАМС, следующих сотрудников Учреждения:

………………………………………

Ответственный за помещения в своей деятельности руководствоваться «Положением об организации режима безопасности помещений, в которых размещены объекты информатизации, подключаемых к ГИС РИАМС».

7. Утвердить следующие эксплуатационные документы ОИ:

- Технический паспорт - *ОИ «Типовое АРМ ГИС РИАМС \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_»*

- Журнал учета материальных учета машинных носителей информации ограниченного доступа;

- Журнал учета используемых криптосредств, эксплуатационной и технической документации к ним, ключевых документов;

- Журнал учета лиц, допущенных к средствам криптографической защиты информации (форма);

- Журнал учета мероприятий по обеспечению контроля состояния защиты информации на ОИ, подключаемых к ГИС РИАМС.

Ведение и поддержание в актуальном состоянии эксплуатационной документации на ОИ ГИС РИАМС возложить на администратора информационной безопасности ОИ.

8. На автоматизированных рабочих местах ОИ, подключаемых к ГИС РИАМС выполнить организационно-технические мероприятия по защите информации в соответствии с Техническими условиями по подключению типовых объектов (сегментов, АРМ) к ГИС РИАМС в защищенном режиме.

9. Провести мероприятия по контролю реализации мер по защите информации в сегменте РИАМС в Учреждения и оценки соответствия сегмента РИАМС Учреждения установленным в РИАМС правилам безопасности информации.

10. Утвердить План мероприятий по обеспечению контроля состояния обеспечения безопасности информации на ОИ, подключаемых к ГИСРИАМС.

11. Предоставить в управление здравоохранения области следующие документы:

- копию настоящего приказа;

- копии организационно-распорядительных документов по защите информации;

- копии листов ознакомления пользователей с организационно-распорядительными документами;

- копии технических паспортов ОИ;

- копии материалов проверки по п. 9.

12. Контроль за исполнением настоящего приказа оставляю за собой.

Руководитель \_\_\_\_\_\_\_\_\_\_

Приложение Д

**Реализация технических мер защиты информации   
при подключении АРМ и сегментов ЛВС к ГИС РИАМС**

Рекомендуется исключить использование ОС MicrosoftWindowsXP, ввиду окончания технической поддержки разработчиком данной ОС и, как следствие, прекращения выпуска обновлений для блокирования уязвимостей нулевого дня.

Для реализации технических мер защиты на АРМ должны быть установлены и настроены следующие сертифицированные средства защиты информации:

* СрЗИ от несанкционированного доступа (НСД) ПК DallasLock 8.0-K с модулем межсетевого экранирования и средством обнаружения вторжений;
* Средство антивирусной защиты (САВЗ) программный комплекс (ПК) KasperskyEndpointSecurity 10 для Windows(или аналог, имеющий сертифицированный комплект по требованиям безопасности информации);
* Средство криптографической защиты информации с функцией межсетевого экранирования (СКЗИ/МЭ) ПК Vipnet Client 3.2 (или более поздняя сертифицированная версия).
* Средство доверенной загрузки (СДЗ) DallasLock.

СрЗИ должны быть настроены в соответствии с необходимостью обеспечения реализации технических мер защиты информации, предусмотренных для СЗИ ГИС РИАМС.

Установка и настройка СрЗИ НСД DallasLock 8.0-K с модулем межсетевого экранирования и средства обнаружения вторжений должна обеспечивать:

* Идентификацию и аутентификацию пользователей информационной системы;
* идентификацию и аутентификацию устройств, применяемых в информационной системе;
* определение администратора (суперадминистратора), ответственного за создание, присвоение и уничтожение идентификаторов пользователей и устройств;
* присвоение идентификатора пользователю или устройству; предотвращение повторного использования идентификатора пользователя или устройства в течение установленного периода времени;
* установление характеристик пароля (назначение минимальной сложности пароля с определяемыми требованиями к регистру, количеству символов, сочетанию букв верхнего и нижнего регистра, цифр и специальных символов, минимального количества измененных символов при создании новых паролей, назначение минимального и максимального времени действия пароля);
* управление доступом субъектов доступа к объектам доступа на основе идентификационной информации субъекта и для каждого объекта доступа – списка, содержащего набор субъектов доступа (групп субъектов) и ассоциированных с ними типов доступа;
* разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование ИС, в соответствии с их должностными обязанностями (функциями), и санкционирование доступа к объектам доступа в соответствии с разделением полномочий (ролей);
* назначение прав и привилегий пользователям и запускаемым от их имени процессам, администраторам и лицам, обеспечивающим функционирование ИС, минимально необходимых для выполнения ими своих должностных обязанностей (функций), и санкционирование доступа к объектам доступа в соответствии с минимально необходимыми правами и привилегиями;
* блокирование устройства, с которого предпринимаются попытки доступа, или учетной записи пользователя при превышении пользователем ограничения количества неуспешных попыток входа в информационную систему;
* предоставление доступа к машинным носителям информации только тем лицам, которым он необходим для выполнения своих должностных обязанностей (функций) путем разрешения дискреционного и мандатного доступа к этим носителям;
* контроль использования интерфейсов ввода (вывода) информации на машинные носители информации;
* уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания;
* сбор, запись и хранение информации о событиях безопасности;
* обнаружение (предотвращение) вторжений (компьютерных атак), направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней;
* обновление базы решающих правил модуля системы обнаружения вторжений;
* контроль целостности программного обеспечения информационной системы, включая программное обеспечение средств защиты информации.

Установка и настройкаСАВЗ ПКKasperskyEndpointSecurity 10 дляWindowsили его аналога должна обеспечивать:

* обнаружение компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации;
* проведение периодических проверок компонентов ИС (автоматизированных рабочих мест, серверов, других средств вычислительной техники) на наличие вредоносных компьютерных программ (вирусов);
* проверку в масштабе времени, близком к реальному, объектов (файлов) из внешних источников (съемных машинных носителей информации, сетевых подключений, в том числе к сетям общего пользования, и других внешних источников) при загрузке, открытии или исполнении таких файлов;
* оповещение администраторов безопасности в масштабе времени, близком к реальному, об обнаружении вредоносных компьютерных программ (вирусов);
* определение и выполнение действий по реагированию на обнаружение в информационной системе объектов, подвергшихся заражению вредоносными компьютерными программами (вирусами);

# получение уведомлений о необходимости обновлений и непосредственном обновлении базы данных признаков вредоносных компьютерных программ (вирусов);

* получение из доверенных источников и установку обновлений базы данных признаков вредоносных компьютерных программ (вирусов);
* контроль целостности обновлений базы данных признаков вредоносных компьютерных программ (вирусов).
* обнаружение и реагирование на поступление незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию ИС (защита от спама).

Установка и настройка СКЗИ/МЭ ПК Vipnet Client 3.2 должна обеспечивать:

* Предоставление доступа к серверу ГИС РИАМС по шифрованному VPN-каналу связи (ГОСТ 28147-89);

# предоставление доступа к ГИС только авторизованным (уполномоченным) пользователям;

* исключение удаленного доступа к АРМ ГИС РИАМС через сети связи общего пользования;
* настройку правил межсетевого экрана для входящих подключений по принципу «запрещено все, что однозначно не разрешено»;
* защиту персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны.

Установка и настройка СДЗ DallasLock должна обеспечивать выполнение следующих мер защиты информации:

* разрешение действий пользователям до прохождения ими процедур идентификации и аутентификации и запрет действий пользователям, не включенных в перечень разрешенных действий, до прохождения ими процедур идентификации и аутентификации;
* разрешение администраторубезопасности действий в обход установленных процедур идентификации и аутентификации, необходимых только для восстановления функционирования АРМ ГИС РИАМС в случае сбоев в работе или выходе из строя отдельных технических средств (устройств);
* исключение несанкционированного доступа к программным и техническим ресурсам средства вычислительной техники на этапе его загрузки, блокировка попытки несанкционированной загрузки нештатной ОС, контроль доступа пользователей к процессу загрузки ОС, контроль целостностизагружаемой операционной системы и состава компонентов аппаратного обеспечения ПК.