ПРИЛОЖЕНИЕ № 1

Утверждено приказом

№ 790

от

РЕГЛАМЕНТ

подключения внешних информационных систем и автоматизированных рабочих мест

1. Общие положения

1.1 Настоящий Регламент разработан с целью регламентирования подключения внешних пользователей к Государственной информационной системе в сфере здравоохранения Республики Адыгея «Региональный фрагмент Единой государственной информационной системы в сфере здравоохранения Республики Адыгея» (далее – РФ ЕГИСЗ РА) Министерства здравоохранения Республики Адыгея (далее – Министерство).

1.2 Настоящий регламент определяет общий состав, содержание и порядок выполнения участниками информационного взаимодействия работ по защите информации при их подключении к РФ ЕГИСЗ РА.

2. Организация информационного взаимодействия с ГИС «РФ ЕГИСЗ РА»

2.1 Для обеспечения безопасности информации, обрабатываемой и передаваемой через информационные ресурсы Министерства, была создана и эксплуатируется защищенная сеть передачи данных ViPNet № 2285. Подключение организаций к информационным ресурсам Министерства осуществляются исключительно через защищённую сеть передачи данных № 2285; любые другие методы подключения являются недопустимыми.

2.2 РФ ЕГИСЗ РА представляет собой распределенную ГИС с обработкой персональных данных (далее – ПДн) и включает:

– серверный сегмент (УЗ2), который располагается в пределах локально-вычислительной сети регионального ЦОД Министерства цифрового развития, информационных и телекоммуникационных технологий Республики Адыгея по услуге Co-location;

– пользовательские сегменты (УЗ2, УЗ3), осуществляющие доступ к серверному сегменту РФ ЕГИСЗ РА, расположенные непосредственно в

Министерстве, ГАУЗ РА «МИАЦ МЗ РА» (далее – Оператор) и медицинских организациях (далее – МО) Республики Адыгея.

2.3 Организацию информационного взаимодействия, а также подключение организаций к информационным ресурсам Министерства осуществляет ГАУЗ РА «МИАЦ МЗ РА», которое является Оператором РФ ЕГИСЗ РА.

2.4 Возможны следующие варианты организации информационного взаимодействия:

– подключение автоматизированных рабочих мест (далее – АРМ) внешних пользователей с использованием ViPNet Client;

– подключение информационных систем (далее – ИС) внешних пользователей с использованием программно-аппаратного комплекса ViPNet Coordinator HW 4;

– подключение ИС внешних пользователей с установлением межсетевого взаимодействия.

3. Требования к организации подключения

3.1 Организация подключения информационных систем и автоматизированных рабочих мест (далее – ИС/АРМ) внешних пользователей (далее – Претендент) к РФ ЕГИСЗ РА осуществляется в соответствии с:

– требованиями нормативно-правовых актов Российской Федерации в сфере защиты информации;

– требованиями нормативно-технических и методических документов уполномоченных органов исполнительной власти Российской Федерации в сфере обеспечения безопасности информации (федеральная служба по техническому и экспортному контролю России (далее – ФСТЭК России), федеральная служба безопасности России (далее – ФСБ России);

– настоящими Требованиями.

3.2 Для организации взаимодействия ИС/АРМ внешних пользователей с РФ ЕГИСЗ РА (в т.ч. пользовательский сегмент (УЗ2), подключаемые ИС/АРМ Претендентов должны соответствовать требованиям приказа ФСТЭК России от 11 февраля 2013г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» в соответствии с установленным вторым классом защищенности информационных систем (К2) и требования Постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» в соответствии с установленным вторым уровнем защищенности информационных систем персональных данных (УЗ2).

При этом для организации взаимодействия ИС/АРМ внешних пользователей с пользовательским сегментом РФ ЕГИСЗ РА (УЗ3)

подключаемые ИС/АРМ Претендентов должны соответствовать требованиям приказа ФСТЭК России от 11 февраля 2013г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» в соответствии с установленным третьим классом защищенности информационных систем (К3) и требования Постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» в соответствии с установленным третьим уровнем защищенности информационных систем персональных данных (УЗ3).

3.3 Для организации взаимодействия ИС/АРМ внешних пользователей с РФ ЕГИСЗ РА, подключаемая ИС должна иметь действующий аттестат (результаты оценки эффективности), подтверждающий ее соответствие требованиям безопасности информации, предъявляемым к государственным информационным системам 2 класса защищенности, а также действующий аттестат, подтверждающий соответствие требованиям безопасности информации, предъявляемым к информационным системам персональных данных 2 уровня защищенности.

Фактическое определение уровня защищенности персональных данных при их обработке во внешних информационных системах, на АРМ и в иных информационных системах устанавливается МО с учетом количества субъектов персональных данных, персональные данные которых доступны для обработки при информационном взаимодействии внешних информационных систем, АРМ и иных ИС.

3.4 Для реализации комплекса организационных и технических мероприятий по защите информации, установленных для 2 класса защищенности государственных информационных систем в соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11 февраля 2013 года № 17, а также мероприятий в соответствии с требованиями настоящего Регламента, должны применяться средства защиты информации не ниже 5 класса.

Для реализации комплекса организационных и технических мероприятий по защите информации, установленных для 3 класса защищенности государственных информационных систем в соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11 февраля 2013 года № 17, а также мероприятий в соответствии с требованиями настоящего Регламента, должны применяться средства защиты информации не ниже 6 класса.

В информационных системах 2 класса защищенности применяются сертифицированные средства защиты информации, соответствующие 5 или более высокому уровню доверия.

В информационных системах 3 класса защищенности применяются сертифицированные средства защиты информации, соответствующие 6 или более высокому уровню доверия.

3.5 В ИС/АРМ внешних пользователей применяются средства защиты информации, сертифицированные на соответствие обязательным требованиям по безопасности информации, установленным ФСТЭК и ФСБ России, или на соответствие требованиям, указанным в технических условиях (заданиях по безопасности).

К базовому составу средств защиты информации для нейтрализации актуальных угроз безопасности информации при подключении ИС Претендентов к РФ ЕГИСЗ РА относятся:

– средства защиты от несанкционированного доступа;

– средства антивирусной защиты;

– средства обнаружения вторжений;

– средства межсетевого экранирования;

– средства анализа (контроля) защищенности;

– средства криптографической защиты информации.

При взаимодействии с РФ ЕГИСЗ РА АРМ Претендентов должны быть оснащены базовым составом средств защиты информации, необходимым для обеспечения информационной безопасности:

– средства антивирусной защиты;

– средства криптографической защиты информации.

Класс применяемых средств криптографической защиты в ИС внешних пользователей при подключении к РФ ЕГИСЗ РА в соответствии с требованиями ФСБ России должен быть не ниже КС3.

Данный набор средств минимально необходим, но в отдельных случаях может быть дополнен в соответствии с принятыми внешними пользователями моделями угроз и нарушителя безопасности информации, а также по решению владельца РФ ЕГИСЗ РА.

3.6 При организации подключения ИС/АРМ внешних пользователей к РФ ЕГИСЗ РА Претендентом на подключение должно быть обеспечено выполнение организационных мер защиты информации, которые включают:

– назначение ответственного за организацию обработки защищаемой информации;

– назначение ответственного за обеспечение безопасности защищаемой информации;

– определение перечней сотрудников, осуществляющих обработку защищаемой информации и имеющих доступ к обрабатываемой защищаемой информации;

– определение перечня мер по обеспечению безопасности помещений, в которых размещены государственные информационные системы защищаемой информации и сохранности носителей защищаемой информации;

– определение перечня мер, направленных на выполнение требований законодательства Российской Федерации в области защиты информации с использованием средств криптографической защиты;

– определение политики в отношении обработки защищаемой информации.

Не допускается взаимодействие ИС/АРМ внешних пользователей с государственной информационной системой Министерства при неполной или некорректной реализации защищенного подключения, невыполнении всех необходимых требований по обеспечению информационной безопасности, отсутствию или некорректной настройке технических средств защиты информации.

4. Порядок организации подключения

4.1 Порядок подключения ИС/АРМ внешних пользователей к РФ ЕГИСЗ РА различается в зависимости от варианта организации информационного взаимодействия. Организацию подключения осуществляет Оператор, поскольку несет ответственность за защиту информации.

4.1.1 Подключение АРМ внешних пользователей с использованием ViPNet Client и подключение ИС внешних пользователей с использованием программно-аппаратного комплекса ViPNet Coordinator HW 4 осуществляется в следующем порядке.

1) Претендент может направить заявку на подключение по форме, приведенной в Приложении № 1:

– на электронный адрес Министерства(minzdrav@adygheya.gov.ru);

– посредством системы электронного документооборота СЭД «Дело-WEB»;

– почтовым отправлением.

2) Министерство в течение пяти рабочих дней со дня получения заявки от Претендента проводит оценку оснований для подключения его к сети № 2285, а также оценку технической возможности подключения.

3) По результатам рассмотрения заявки Министерство направляет Претенденту уведомление о предварительном согласовании схемы подключения, либо о несогласовании схемы с указанием причин.

4) После получения Претендентом уведомления о предварительном согласовании схемы подключения, Претендент закупает необходимое оборудование. Далее Претендент направляет в адрес Министерства заявление на получение dst-файла – парольно-ключевой информации – (далее – ПКИ) по форме, приведенной в Приложении № 2.

5) Претендент проводит необходимые работы по защите информации:

– для осуществления работы в РФ ЕГИСЗ РА Претендент обязан провести мероприятия по аттестации пользовательского сегмента «РФ ЕГИСЗ РА» по требованиям безопасности информации и выслать в адрес Оператора(miac@adygheya.gov.ru); заверенные скан-копии первых страниц

аттестата соответствия в ту же ветку переписки, что и на согласование схемы подключения и получение ПКИ, а в случае наличия ранее проведенных мероприятий по аттестации пользовательского сегмента «РФ ЕГИСЗ РА» по требованиям безопасности информации требуется выслать в адрес Оператора заверенные скан-копии первых страниц аттестата соответствия в ту же ветку переписки, что и на согласование схемы подключения и получение ПКИ.

6) Оператор проводит проверку полученных от Претендента данных и по результатам направляет официальный ответ о согласовании схемы подключения.

7) Министерство в течении 1 месяца изготавливает ПКИ. По факту готовности ПКИ, Оператор уведомляет об этом Претендента по электронной почте.

8) Получение ПКИ:

Претендент получает ПКИ одним из следующих способов:

1) Претендент направляет лицо, указанное в заявке на получение ПКИ в Министерство по адресу г. Майкоп, ул. Советская, д.176. При себе лицо, прибывшее получать ПКИ, должно иметь паспорт, CD-диск для записи ПКИ и сейф-пакет (Претенденту необходимо самостоятельно приобрести электронный носитель (CD/DVD-диск) и сейф-пакет).

2) После этого Министерство записывает ПКИ на электронный носитель, предоставленный Претендентом, упаковывает электронный носитель с записанной ПКИ в сейф-пакет и передает лицу, указанному в заявке на получение ПКИ. Выдача ПКИ производится в заранее согласованное сторонами время. Факт получения ПКИ фиксируется в Журнале учета выдачи ключевых документов, где должно расписаться лицо, ответственное за получение ПКИ.

9) Вскрытие сейф-пакета производится на территории Претендента в присутствии руководителя, при этом, перед вскрытием проверяется его целостность, оформляется находящийся внутри сейф-пакета акт передачи ПКИ, который высылается в адрес Министерства (оригинал по почте и скан-копия по электронной почте minzdrav@adygheya.gov.ru). В случае обнаружения нарушения целостности сейф-пакета перед его вскрытием, с целью исключения компрометации ПКИ, необходимо незамедлительно оповестить об этом Министерства по электронной почте (minzdrav@adygheya.gov.ru).

4.1.2 Подключение ИС/АРМ внешних пользователей с установлением межсетевого взаимодействия осуществляется в следующем порядке.

1) Претендент может направить заявку на подключение по форме, приведенной в Приложении № 1:

– на электронный адрес Министерство (minzdrav@adygheya.gov.ru);

– посредством системы электронного документооборота СЭД «Дело-WEB»;

почтовым отправлением.

2) Министерство в течение пяти рабочих дней со дня получения заявки от Претендента проводит оценку оснований для подключения его к сети № 2285, а также оценку технической возможности подключения.

3) По результатам рассмотрения заявки Оператор направляет Претенденту уведомление о предварительном согласовании схемы подключения, либо о несогласовании схемы с указанием причин.

4) После получения Претендентом уведомления о предварительном согласовании схемы подключения, Претендент закупает необходимое оборудование и направляет в адрес Оператора скан-копию заявки на установление межсетевого взаимодействия согласно Приложению № 3 к настоящему регламенту и скан-копию лицензии на использование ViPNet Administrator.

5) Претендент формирует первичный экспорт своей сети ViPNet и нарочно передает или доставляет курьерской службой, упакованный в сейф-пакет CD-диск, содержащий первичный экспорт по адресу: 385000, г. Майкоп, ул. Советская, 176, а также подписанное со стороны Претендента соглашение об организации межсетевого взаимодействия в двух экземплярах. Форма соглашения об организации межсетевого взаимодействия приведена в Приложении № 4 к настоящему регламенту.

6) В зависимости от целей подключения Претендент проводит необходимые работы по защите информации:

– для осуществления работы в ГИС «РФ ЕГИСЗ РА» Претендент обязан провести мероприятия по аттестации пользовательского сегмента «РФ ЕГИСЗ РА» по требованиям безопасности информации и выслать в адрес Оператора заверенные скан-копии первых страниц аттестата соответствия в ту же ветку переписки, что и на согласование схемы подключения и получение ПКИ.

7) Оператор проводит проверку полученных от Претендента материалов, по результатам которой направляет официальный ответ о согласовании схемы подключения.

8) Министерство в течении 1 месяца изготавливает ПКИ. По факту готовности ПКИ, Министерство уведомляет об этом Претендента тем же способом, которым поступила заявка на подключение.

9) Претендент получает ПКИ одним из способов, указанных в п.4.1.1 настоящего регламента, одновременно с ПКИ Претенденту передается подписанный со стороны Министерства экземпляр соглашения об установлении межсетевого взаимодействия (приложение 4) и протокол установления межсетевого взаимодействия (приложение 5) в двух экземплярах.

После получения ПКИ, Претендент проводит действия, описанные в п.4.1.1 настоящего регламента и высылает в адрес Министерства (оригинал по почте и скан-копии по электронной почте (minzdrav@adygheya.gov.ru), либо посредством системы электронного документооборота СЭД «Дело-WEB») следующие подписанные со стороны Претендента документы:

– Акт передачи ПКИ (приложение 6);

– Экземпляр протокола об установлении межсетевого взаимодействия.

По окончании работ по подключению Претендент переходит в статус

Абонента.

5. Ответственность

5.1 Ответственность за соблюдение требований настоящего регламента, обеспечение защиты информации, в ходе эксплуатации информационных ресурсов Оператора на стороне Абонента, а также ответственность за соблюдение требований к эксплуатации СЗИ и СКЗИ в составе системы защиты Абонента лежит исключительно на Абоненте.

Оператор имеет право проводить проверки реализации схем подключения.

В некоторых случаях Оператор имеет право произвести отключение Абонента от защищенной сети Оператора (сеть № 2285). К таким случаям относятся:

- выявление факта нарушения требований Регламента;
- ликвидация юридического лица;
- компрометация парольно-ключевой информации;

окончание договора с обслуживающей организацией.

В случае приобретения Претендентом без согласования Министерства программного комплекса ViPNet Client для защиты рабочих мест из защищенной сети передачи данных Министерства не гарантирует успешное установление информационного взаимодействия.

ПРИЛОЖЕНИЕ № 1

к Регламенту подключения внешних

информационных систем и

автоматизированных рабочих мест

Образец Заявки на подключение к Государственной информационной системе в сфере здравоохранения Республики Адыгея «Региональный фрагмент Единой государственной информационной системы в сфере здравоохранения Республики Адыгея»

(оформляется на бланке учреждения)

Прошу подключить _____ (указывается полное наименование организации) к защищённой виртуальной сети ViPNet (сеть ViPNet № 2285) Министерства здравоохранения Республики Адыгея (далее - Министерство) в соответствии с нижеуказанной информацией и на условиях согласно Регламенту.

Сведения об организации		
1.	Полное наименование организации	
2.	Фактический адрес	
3.	Сайт филиала или головной организации	
4.	Должность руководителя организации	
5.	Ф. И. О. руководителя организации	
6.	Телефон организации	
Ответственное за подключение лицо		
7.	ФИО (полностью)	
8.	Должность	
9.	Телефон (рабочий)	
10.	Телефон (мобильный)	
11.	E-mail	
Общая информация		

12.	Цель подключения	
13.	Тип подключения	
14.	Есть ли у Вас согласованные ранее схемы с Министерством? (Если есть, указать наименование схемы).	

15.	Цель согласования схемы с Министерством (Новое подключение/Переход на новую схему подключения/Актуализация данных)	
16.	Планируемое кол-во автоматизированных рабочих мест, подключаемых к сети № 2285, шт.	
Используемое оборудование		
17.	Полное наименование используемого программного или программно-аппаратного решения	
18.	Номер сети ViPNet	

Достоверность предоставленных данных гарантируем. Обязуемся не нарушать согласованную схему подключения и производить изменения только по согласованию с Министерством.

Руководитель учреждения _____ ФИО

подпись М.П.

ПРИЛОЖЕНИЕ № 2

к Регламенту подключения внешних

информационных систем и

автоматизированных рабочих мест

Запрос
на получение парольно-ключевой информации

г._____ «___» _____ 20__г.

В соответствии с регламентом подключения внешних информационных систем и автоматизированных рабочих мест к Государственной информационной системе в сфере здравоохранения Республики Адыгея «Региональный фрагмент Единой государственной информационной системы в сфере здравоохранения Республики Адыгея» (далее – ГИС «РФ ЕГИСЗ РА»)

_____

(наименование учреждения)

провело мероприятия по выполнению организационных и технических требований для подключения к ГИС «РФ ЕГИСЗ РА».

В соответствии с регламентом регламентом подключения внешних информационных систем и автоматизированных рабочих мест, прошу предоставить парольно-ключевую информацию для подключения к защищенной сети передачи данных с номером 2285.

Руководитель учреждения _____ ФИО

подпись М.П.

ПРИЛОЖЕНИЕ № 3

к Регламенту подключения внешних

информационных систем и

автоматизированных рабочих мест

Образец Заявки на установление межсетевого взаимодействия

(оформляется на бланке учреждения)

В соответствии с Регламентом подключения к информационным ресурсам Министерства здравоохранения Республики Адыгея (далее - Регламент, _____ (указывается полное наименование организации) провела мероприятия по закупке оборудования и разворачивания сети ViPNet для подключения к сети ViPNet № 2285.

При организации защищенного взаимодействия с сетью ViPNet № 2285 выполняются требования нормативно-правовых и руководящих документов уполномоченных органов в сфере защиты информации, а также требования Регламента.

Перечень абонентских пунктов, напрямую участвующих во взаимодействии с ViPNet сетью № 2285:

- _____ (указывается наименование АП)**;**

Все вышеперечисленные абонентские пункты входят в состав пользовательского сегмента РФ ЕГИСЗ РА.

Копии документов, подтверждающие статус владельца сети:

- лицензия на право пользования ViPNet Администратор.

Прошу предоставить парольно-ключевую и всю необходимую справочную информацию ViPNet для организации межсетевого взаимодействия между сетью ViPNet № 2285 и сетью _____ (указывается полное наименование организации) под номером _____ (указывается номер сети).

_____(указывается вариант передачи Министерством здравоохранения Республики Адыгея справочной информации и мастер-ключа сети VIPNet)

_____(указывается вариант получения справочной информации для установления межсетевого взаимодействия ViPNet сетей)

Руководитель учреждения _____ ФИО

подпись М.П.

ПРИЛОЖЕНИЕ № 4

к Регламенту подключения внешних

информационных систем и

автоматизированных рабочих мест

ТИПОВОЕ СОГЛАШЕНИЕ
об установлении межсетевого взаимодействия

г. Майкоп «___» _____ 20__г.

ы

Министерство здравоохранения Республики Адыгея, именуемое в дальнейшем «Министерство», в лице Министра здравоохранения Республики Адыгея Меретукова Рустема Батырбиевича, действующего на основании _____, с одной стороны, и _____, именуемое в дальнейшем _____, в лице _____, действующего на основании _____, с другой стороны, (вместе именуемые «Стороны») заключили настоящее соглашение о нижеследующем:

1. ПРЕДМЕТ СОГЛАШЕНИЯ

1.1. Стороны договорились об установлении межсетевого взаимодействия и доверия между ViPNet сетями № 2285 и № ____. Межсетевое взаимодействие должно обеспечивать создание защищенной, доверенной среды передачи информации ограниченного доступа между ViPNet сетями Сторон.

1.2. Создание и модификация межсетевого взаимодействия осуществляется в соответствии с эксплуатационной документацией на программный комплекс ViPNet Administrator актуальной версии.

1.3. Отношения между Сторонами регулируются следующими нормативными документами:

- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
- Приказом ФСБ РФ от 9.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
- Приказом ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

1.4. Взаимодействие Сторон осуществляется на безвозмездной основе.

2. ПРАВА И ОБЯЗАННОСТИ СТОРОН

2.1. При организации межсетевого взаимодействия Министерство принимает на себя следующие права и обязанности:

2.1.1. Обеспечивает поддержание в работоспособном состоянии программных и программно-аппаратных комплексов ViPNet №2285 в границах своей зоны ответственности.

2.1.2. Обеспечивает установку и сопровождение средств криптографической защиты информации абонентам сети ViPNet № 2285, а также организацию взаимосвязи с сетевыми узлами ViPNet.

2.2. При организации межсетевого взаимодействия «_____» принимает на себя следующие права и обязанности:

2.2.1. Обеспечивает поддержание в работоспособном состоянии программных и

программно-аппаратных комплексов ViPNet №_____ в границах своей зоны ответственности.

2.2.2. Обеспечивает организацию взаимосвязи с сетевыми узлами ViPNet № 2285 в соответствии с разделом 3 настоящего соглашения.

2.3. Стороны обеспечивают контроль за проведением процедуры обмена данными экспорта между центрами управления сетью (далее - ЦУС) ViPNet сетей. Экспортированные данные импортируются в ЦУС соответствующей сети.

2.4. Стороны обеспечивают контроль за соблюдением абонентами правил использования средств криптографической защиты информации.

2.5. Установка взаимосвязи с абонентами сетей ViPNet производится по взаимному согласию Сторон.

3. ОРГАНИЗАЦИЯ МЕЖСЕТЕВОГО ВЗАИМОДЕЙСТВИЯ

3.1. Ответственными лицами Сторон для организации межсетевого взаимодействия являются Администраторы ЦУС.

3.2. Организация межсетевого взаимодействия (установление доверительных отношений) между ViPNet сетями Сторон осуществляется в соответствии с технической документацией на программное обеспечение (ПО) ViPNet Administrator.

3.3. По завершении процедуры организации межсетевого взаимодействия между ViPNet сетями Сторон подписывается Протокол установления межсетевого взаимодействия.

3.4. Для установления взаимодействия между сетевыми узлами пользователей ViPNet сетей Сторон, Стороны согласовывают списки таких сетевых узлов, и устанавливают данное взаимодействие в рабочем порядке, руководствуясь технической документацией на ПО ViPNet Administrator.

4. ПРОВЕДЕНИЕ ПРОФИЛАКТИЧЕСКИХ МЕРОПРИЯТИЙ

4.1. Проведение профилактических мероприятий по поддержанию работоспособности программных и программно-аппаратных комплексов ViPNet в границах своей зоны ответственности Стороны осуществляют при соблюдении следующих условий:

- о сроках проведения профилактических мероприятий другая Сторона должна быть оповещена заблаговременно, не позднее, чем за 3 рабочих дня до дня проведения профилактических мероприятий.

4.2. В случае возникновения необходимости проведения технических работ, следствием которых может быть временное прекращение работоспособности программных и программного аппаратных комплексов ViPNet, Сторона-инициатор должна уведомить другую Сторону любым удобным способом.

5. ОТВЕТСТВЕННОСТЬ СТОРОН

5.1. Стороны несут ответственность за обеспечение безопасности информации, передаваемой по средствам программных и программно-аппаратных комплексов ViPNet в границах своей зоны ответственности согласно законодательству Российской Федерации.

5.2. Стороны не несут ответственность за содержание информации, передаваемой абонентами друг другу.

6. СРОК ДЕЙСТВИЯ СОГЛАШЕНИЯ

6.1. Настоящее Соглашение вступает в силу с момента его подписания, и действует бессрочно.

6.2. Настоящее Соглашение может быть расторгнуто по инициативе любой из Сторон, о чем необходимо письменно уведомить другую Сторону не позднее, чем за два месяца до дня его расторжения.

7. ФОРС-МАЖОР

7.1. При возникновении обстоятельств, которые делают полностью или частично невозможным выполнение настоящего Соглашения одной из Сторон, таких как стихийные бедствия, военные действия и другие обстоятельства непреодолимой силы, не зависящие от сторон, сроки исполнения обязательств продлеваются на время, в течение которого действуют эти обстоятельства.

7.2. Сторона, подвергшаяся действию форс-мажорных обстоятельств, обязуется уведомить

письменно другую Сторону в течение 3 (трех) рабочих дней с предоставлением документов, подтверждающих наличие данных обстоятельств.

7.3. Если обстоятельства непреодолимой силы действуют более одного месяца, Соглашение может быть досрочно расторгнуто в одностороннем порядке, путем заключения дополнительного соглашения.

8. ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ

8.1. В случае возникновения между Сторонами споров или разногласий, вытекающих из настоящего Соглашения или связанных с ним, Стороны примут все меры к разрешению их путем переговоров.

8.2. Если Сторонам не удается разрешить споры и/или разногласия путем переговоров, то такие споры и/или разногласия передаются на рассмотрение в Арбитражный суд Республики Адыгея.

9. ПРОЧИЕ УСЛОВИЯ

9.1. В случае возникновения споров и разногласий Стороны прилагают все усилия, чтобы устранить их путём переговоров.

9.2. При возникновении обстоятельств, которые не позволяют обеспечить межсетевое взаимодействие между ViPNet сетями № 2285 и № ____ Стороны прилагают совместные усилия по устранению этих обстоятельств.

9.3. Настоящее Соглашение составлено в двух экземплярах, каждый из которых имеет одинаковую юридическую силу.

9.4. Изменения и дополнения в настоящее Соглашение могут вноситься только в письменном виде по взаимному согласию Сторон и действительны с момента подписания Сторонами.

10. ЮРИДИЧЕСКИЕ АДРЕСА И РЕКВИЗИТЫ СТОРОН

Министерство здравоохранения Республики Адыгея	_____
Юридический адрес: 385000, Республика Адыгея, г. Майкоп, ул. Советская, 176 ИНН 0105023439 КПП 010501001 Тел./факс +7 (8772) 210-234	Юридический адрес: _____ ИНН/КПП _____/_____ ОГРН _____ Тел./факс _____
Министр	_____
/ Р.Б. Меретуков/	/ _____/
М.П.	М.П.

ПРИЛОЖЕНИЕ № 5

к Регламенту подключения внешних

информационных систем и

автоматизированных рабочих мест

ПРОТОКОЛ

установления межсетевого взаимодействия

г. Майкоп 20_г.

1. Межсетевое взаимодействие устанавливается между сетями:

Номер ViPNet сети	**Наименование организации**
№ 2285	*Министерство здравоохранения Республики Адыгея*

2. Целью установления межсетевого взаимодействия является межведомственное информационное взаимодействие ViPNet - сети *№2285* и ViPNet - сети № ____.

3. Процедуру установления межсетевого взаимодействия осуществляли:

Номер сети	**Должность**	**ФИО**

4. Передача начального и ответного экспорта между сетями ViPNet *№ 2285* и ViPNet — сети № осуществлялась согласно Регламенту подключения к защищенной сети передачи данных № 2285 доверенным способом.

5. Для установления межсетевого взаимодействия использовался индивидуальный симметричный межсетевой мастер-ключ, созданный в сети ViPNet №.

6. Для установления межсетевого взаимодействия были назначены серверы маршрутизаторы для организации шлюза:

- в сети ViPNet *№ 2285 — « _____»;*
- в сети ViPNet №— «».

7. При установлении межсетевого взаимодействия в части создания связей между сетевыми узлами были произведены импорты справочников из сети ViPNet *№ 2285* и сети ViPNet №____.

8. Смена межсетевых ключей, изменение состава сетевых узлов, участвующих в межсетевом взаимодействии, производится после предварительного согласования средствами взаимного экспорта/импорта, о чем Администраторы ViPNet - сетей Сторон уведомляют друг друга с помощью ПО ViPNet Client [Деловая почта] с указанием производимых изменений.

9. Стороны обязуются производить изменения в настройках и структуре защищенных сетей, которые могут привести к нарушению межсетевого взаимодействия, только после предварительного согласования.

ПРИЛОЖЕНИЕ № 6

к Регламенту подключения внешних

информационных систем и

автоматизированных рабочих мест

АКТ

приема-передачи парольной и справочно-ключевой информации для узлов защищенной сети ViPNet № 2285

Экз № _

город Майкоп «___»_____202__ г.

Настоящий акт составлен о том, что Министерство здравоохранения Республики Адыгеи передало, а (наименование лица-заявителя) приняло парольную и справочно-ключевую информацию для работы в защищенной сети ViPNet № 2285.

1) Парольная и справочно-ключевая информация передана в сейф-пакете № ____(далее - сейф-пакет)

2) Сейф-пакет был вскрыт в присутствии руководителя организации.

3) Целостность сейф-пакета не нарушена, количество и состав переданной в соответствии с настоящим актом парольной и справочно-ключевой информации соответствует составу и количеству парольной и справочно-ключевой информации, указанной ниже:

Тип и серийный номер носителя	Наименование dst-файлов

Передал	**Принял**
Министерство здравоохранения Республики Адыгея	*(Наименование юридического лица)*
(полное наименование должности уполномоченного работника)	(полное наименование должности уполномоченного работника или руководителя)
_____/ _____/ (подпись) (Ф.И.О)	_____/ _____/ (подпись) (Ф.И.О)
«__»_____202__г.	«__»_____202__г.

ПРИЛОЖЕНИЕ № 7

к Регламенту подключения внешних информационных систем и автоматизированных рабочих мест

Памятка
«Классификация подсистем РФ ЕГИСЗ РА в соответствии с пользовательскими сегментами»

Пользовательский сегмент (УЗ 2) ГИС «РФ ЕГИСЗ РА»	**Пользовательский сегмент (УЗ 3) ГИС «РФ ЕГИСЗ РА»**
Интегрированная электронная медицинская карта	Подсистема обеспечения отдельных категорий граждан, в том числе граждан, имеющих право на получение государственной социальной помощи, лекарственными препаратами, специализированными продуктами лечебного питания, медицинскими изделиями
Централизованная подсистема управления лабораторными исследованиями	Телемедицинские консультации
Централизованная подсистема хранения и обработки результатов диагностических исследований (медицинских изображений)	Организация оказания профилактической медицинской помощи (диспансеризация, диспансерное наблюдение, профилактические осмотры)
Организации оказания медицинской помощи больным онкологическими заболеваниями	Компонент «Вакцинопрофилактика»
Организация оказания медицинской помощи по профилям «Акушерство и гинекология» и «Неонатология» (мониторинг беременных)	
Организация оказания медицинской помощи больным сердечно-сосудистыми заболеваниями	
Региональный регистр пациентов	
Региональный реестр электронных медицинских документов	
BI. Система аналитики и мониторинга исполнения показателей	