



УТВЕРЖДАЮ
Директор ГКУ «ЦБА при Минздраве
Карелии»
М.В. Шиманская
Утвержден приказом № 618
от «25» кабры 2024 г.

РЕГЛАМЕНТ

информационного взаимодействия ИСПДн обслуживаемых учреждений
с ИСПДн «Бухгалтерский и кадровый учёт»

Государственного казённого учреждения Республики Карелия
«Центр бухгалтерского учёта и организации закупок при Министерстве
здравоохранения Республики Карелия»

г. Петрозаводск

2024 г.

ОГЛАВЛЕНИЕ

ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ	3
АННОТАЦИЯ.....	4
ВВЕДЕНИЕ	4
1. ОСНОВНЫЕ ПОЛОЖЕНИЯ.....	5
2. ТЕХНИЧЕСКИЕ И СПЕЦИАЛЬНЫЕ ТРЕБОВАНИЯ.....	7
3. ПОРЯДОК ПОДКЛЮЧЕНИЯ	8
4. КОНТРОЛЬ РЕАЛИЗАЦИИ ПОДКЛЮЧЕНИЯ	9
Приложение № 1.....	10
Приложение № 2.....	11
Приложение № 3.....	12
Приложение № 4.....	14

ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ

АИС – Автоматизированная информационная система

АРМ – Автоматизированное рабочее место

РМИАЦ – Государственное бюджетное учреждение здравоохранения Республики Карелия
«Республиканский медицинский информационно–аналитический центр»

ИСПДн – Информационная система персональных данных ИСПДн «Бухгалтерский и кадровый учет»

МЭ – Межсетевой экран

РД – Руководящий документ

Регламент – настоящий регламент

Роскомнадзор – Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций

РФ – Российская Федерация

СЗИ – Средство защиты информации

СКЗИ – Средство криптографической защиты информации

ТУ – Технические условия

ФСБ России – Федеральная служба безопасности Российской Федерации.

ФСТЭК России – Федеральная служба по техническому и экспортному контролю

ЦБЗ – Государственное казённое учреждение Республики Карелия «Центр бухгалтерского учёта и организации закупок при Министерстве здравоохранения Республики Карелия»

ЭД – Эксплуатационная документация

АННОТАЦИЯ

Регламент определяет требования, условия и зоны ответственности, а также устанавливает порядок подключения обслуживаемых учреждений к ИСПДн ЦБЗ.

Требования настоящего регламента распространяются на информационные системы персональных данных обслуживаемых учреждений, подключаемые (имеющие подключение) к ИСПДн ЦБЗ.

ВВЕДЕНИЕ

Настоящий регламент устанавливает состав, содержание, порядок выполнения работ по подключению ИСПДн обслуживаемых учреждений, включая необходимые меры по защите информации, порядок применения средств защиты информации, в том числе средств криптографической защиты информации, необходимых для организации защищенного взаимодействия ИСПДн обслуживаемых учреждений с ИСПДн ЦБЗ.

В качестве подключаемой ИСПДн обслуживаемого учреждения рассматривается как группа АРМ, так и отдельные АРМ, имеющие сетевой доступ к ИСПДн ЦБЗ.

1. ОСНОВНЫЕ ПОЛОЖЕНИЯ

1.1. Общее описание информационного обмена

Информационное взаимодействие между ИСПДн ЦБЗ и ИСПДн обслуживаемых учреждений осуществляется в электронном виде через защищенную сеть передачи данных ViPNet № 934 – сеть VPN, функционирующую на базе сертифицированных СКЗИ семейства ViPNet. Организацией, определяющей порядок подключения и работы в сети ViPNet № 934, является РМИАЦ. Порядок подключения к указанной сети и работы в ней в рамках настоящего Регламента не рассматривается.

1.2. Общие требования по защите информации

Для ИСПДн Центра бухучета и закупок определен 4 уровень защищенности.

В соответствии с нормативно–правовыми актами в сфере защиты информации в ИСПДн ЦБЗ и ИСПДн обслуживаемых учреждений должны быть приняты меры по защите содержащейся в них информации, направленные на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации; соблюдение конфиденциальности информации ограниченного доступа; реализацию права на доступ к информации, **в соответствии с нормативными требованиями, установленными для 4 уровня защищенности персональных данных.**

В результате принятия мер по защите информации должно быть обеспечено:

- 1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
- 2) своевременное обнаружение фактов несанкционированного доступа к информации;
- 3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
- 4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
- 5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
- 6) постоянный контроль за обеспечением уровня защищенности информации;
- 7) нахождение на территории Российской Федерации баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление,

хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации.

Обмен защищаемой информацией осуществляется после принятия обоими участниками информационного взаимодействия, каждым в своей ИСПДн, необходимых мер по защите указанной, в соответствии с требованиями, предусмотренными нормативными правовыми актами Российской Федерации в области защиты информации.

Руководители обслуживаемых учреждений назначают лиц, ответственных за внесение сведений в ИСПДн ЦБЗ (пользователей), а также лиц, ответственных за обеспечение мер по защите информации, содержащейся в ИСПДн обслуживаемых учреждений (администраторов).

Ответственность за соблюдение требований настоящего Регламента, обеспечение защиты информации в ходе эксплуатации ИСПДн обслуживаемого учреждения, соблюдение требований к эксплуатации СЗИ и СКЗИ в составе системы защиты информации ИСПДн обслуживаемого учреждения лежит на обслуживаемом учреждении.

Обслуживаемые учреждения несут также предусмотренную законодательством Российской Федерации ответственность за полноту, достоверность и актуальность сведений, внесенных ими в ИСПДн ЦБЗ.

1.3. Нормативные правовые акты в области защиты информации.

Система защиты информации подключаемой ИСПДн обслуживаемого учреждения должна соответствовать требованиям следующих нормативных правовых актов:

- Федеральный закон Российской Федерации «О персональных данных» (от 27.07.2006 № 152–ФЗ);
- Федеральный закон "Об информации, информационных технологиях и о защите информации" (от 27.07.2006 № 149-ФЗ);
- Постановление Правительства Российской Федерации «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (от 01.11.2012г. № 1119);
- Нормативные и методические документы Роскомнадзора, ФСТЭК России, ФСБ России, устанавливающие требования по защите информации в соответствии с указанными Постановлением Правительства Российской Федерации и Федеральными законами.

1.4. Внесение изменений в Регламент

Все изменения к настоящему Регламенту опубликовываются на официальном сайте ЦБЗ <https://cbmz1.ru>. Одновременно с этим обслуживаемые учреждения письменно уведомляются о появлении таких изменений. Если по истечении 30 дней со дня

опубликования изменений на официальном сайте обслуживаемое учреждение не уведомило ЦБЗ о прекращении информационного взаимодействия с его ИСПДн, такое учреждение признается надлежащим образом уведомленным, принявшим изменения в Регламент, и выполнившим все требования новой версии Регламента.

2. ТЕХНИЧЕСКИЕ И СПЕЦИАЛЬНЫЕ ТРЕБОВАНИЯ

2.1. Требования к организации подключения

Для подключения рабочих мест обслуживаемых учреждений к ИСПДн Центра бухучета и закупок может применяться одна из двух типовых схем подключения.

Типовая схема №1 с указанием СЗИ, в том числе СКЗИ, представлена в Приложении №1.

Типовая схема №2 с указанием СЗИ, в том числе СКЗИ, представлена в Приложении №2.

Класс криптозащиты СКЗИ должен быть не ниже КС1.

Помещения для размещения технических средств ИСПДн обслуживаемого учреждения должны удовлетворять требованиям ТУ и ЭД на данные средства. Работы по установке, монтажу, запуску и первоначальной настройке средств защиты информации и СКЗИ должны выполняться в соответствии с требованиями ТУ и ЭД на данные средства.

2.2. Привлечение сторонних организаций к созданию ИСПД подключаемого учреждения

Для проведения работ по защите информации в ходе создания и эксплуатации ИСПДн обслуживаемого учреждения (оператором) в соответствии с законодательством Российской Федерации при необходимости привлекаются организации, имеющие:

- лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации, позволяющую выполнять работы по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации, проведения аттестационных испытаний и аттестации на соответствие требованиям по защите информации, проектирования в защищенном исполнении средств и систем информатизации, установки, монтажа, средств защиты информации;

- лицензию ФСБ России на деятельность по распространению шифровальных/криптографических средств, техническому обслуживанию

шифровальных/криптографических средств, а также оказанию услуг в области шифрования информации.

3. ПОРЯДОК ПОДКЛЮЧЕНИЯ

До подачи заявки на присоединение к Регламенту и подключение к ИСПДн Центра бухучета и закупок обслуживаемое учреждение принимает необходимые меры по защите информации в своей ИСПДн, выделенной для взаимодействия с ИСПДн Центра бухучета и закупок и согласовывает схему подключения с ЦБЗ и РМИАЦ.

Затем обслуживаемое учреждение подаёт заявку в 3-х экземплярах на присоединение к регламенту и подключение к ИСПДн ЦБЗ. Подавая заявку, обслуживаемое учреждение подтверждает, что требования по защите информации, предусмотренные Регламентом, выполнены им в полном объеме.

В заявке указываются пользователи подключаемых рабочих мест, их должности и полномочия. Шаблон заявки представлен в Приложении № 3. Пример заполнения заявки представлен в Приложении № 4.

В течение 2-х рабочих дней ЦБЗ рассматривает заявку.

В случае положительного рассмотрения ЦБЗ утверждает заявку и передаёт 3 (три) экземпляра для согласования и проведения работ в РМИАЦ.

В случае выявления недостатков, ЦБЗ отклоняет заявку и возвращает в обслуживаемое учреждение 1 (один) экземпляр с указанием выявленных недостатков. Обслуживаемому учреждению следует принять исчерпывающие меры для устранения недостатков и подать новую заявку.

В случае невозможности согласования проведения работ РМИАЦ отклоняет заявку: первый экземпляр заявки направляется в централизованную бухгалтерию, второй остаётся на хранении в РМИАЦ, третий экземпляр направляется в обслуживаемое учреждение. Обслуживаемому учреждению следует принять исчерпывающие меры для устранения выявленных РМИАЦ недостатков и подать новую заявку.

В случае повторного отклонения заявки, каждая последующая заявка от данного обслуживаемого учреждения рассматривается Центром бухучета и закупок в течении 10 календарных дней.

После выполнения работ РМИАЦ: первый экземпляр заявки направляется в централизованную бухгалтерию, второй - остаётся на хранении в РМИАЦ, третий экземпляр направляется в обслуживаемое учреждение.

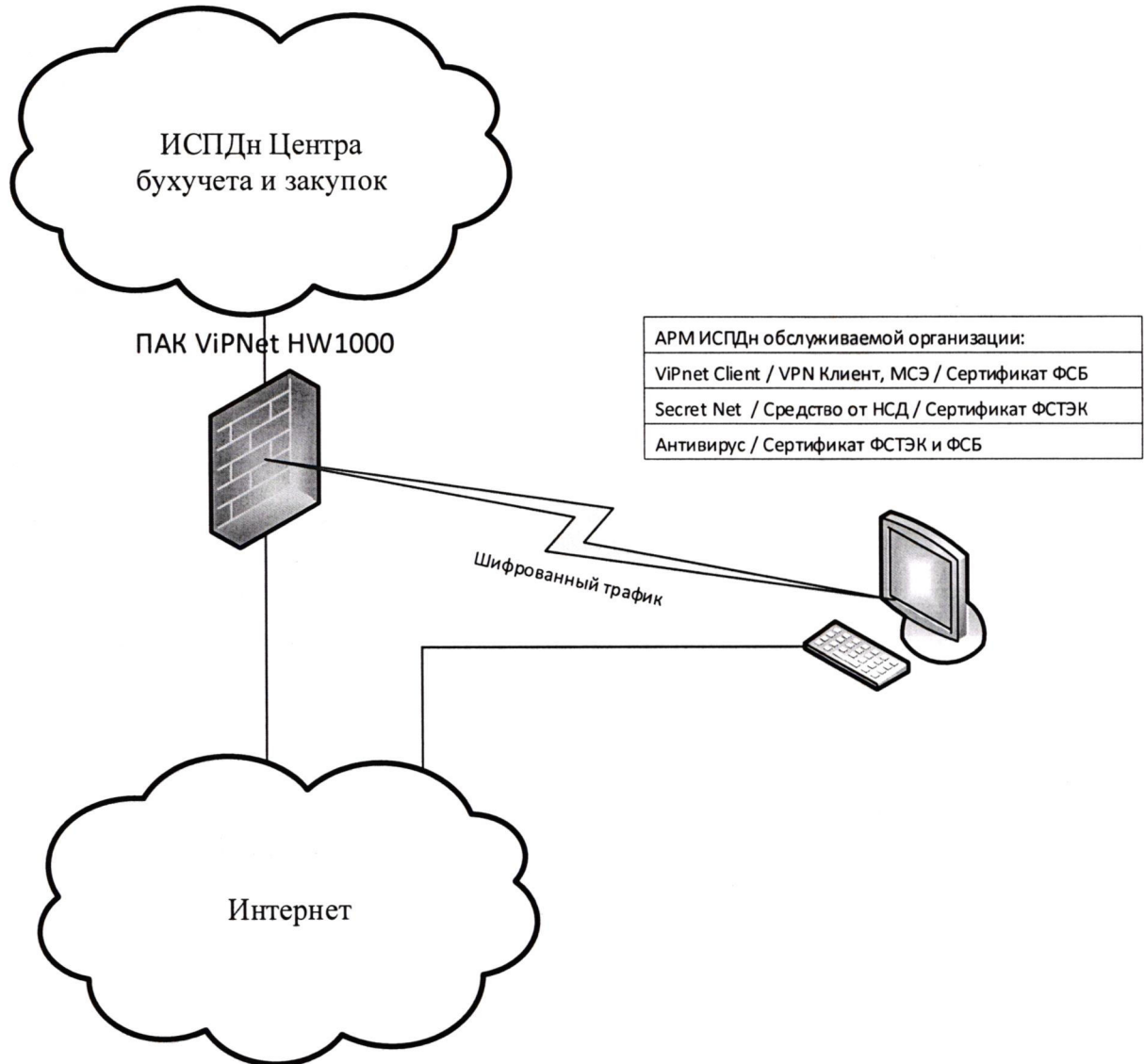
После получения экземпляра заявки с отметкой о подключении в течении 2 (двух) рабочих дней ЦБЗ создаёт идентификаторы и временные пароли для аутентификации в ИСПДн и передаёт их в обслуживаемое учреждение с использованием каналов связи, защищённых с помощью СКЗИ.

4. КОНТРОЛЬ РЕАЛИЗАЦИИ ПОДКЛЮЧЕНИЯ

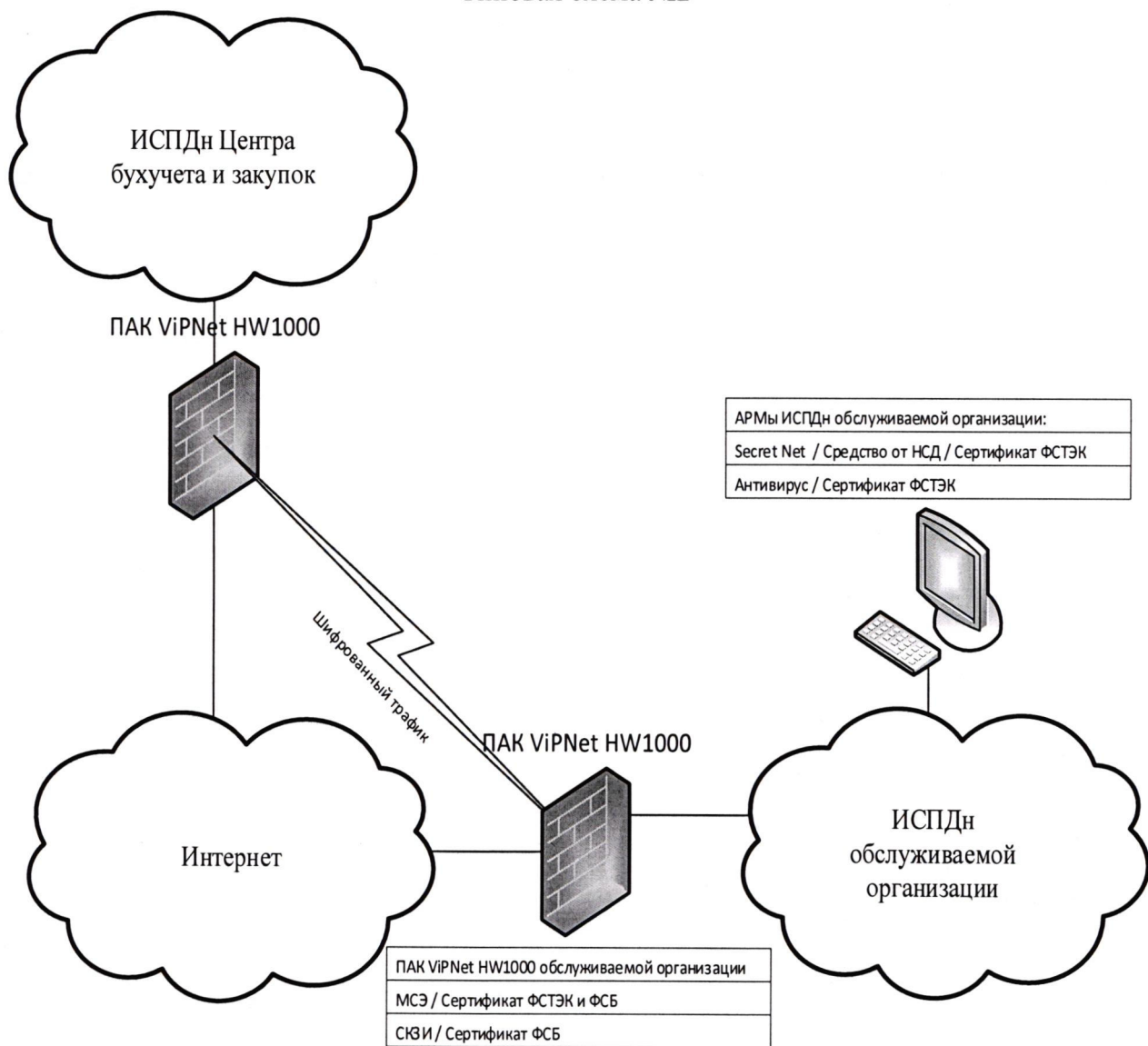
Обслуживаемые учреждения должны поддерживать в актуальном состоянии информацию о лицах, допущенных к внесению сведений в ИСПДн ЦБЗ, лицах, ответственных за защиту информации, и о выполнении требований по защите информации в подключаемой ИСПДн своего учреждения. В случае изменения состава указанных лиц или их полномочий, состояния системы защиты информации в подключаемой ИСПДн, поступления запроса на предоставление указанной информации от ЦБЗ, а также **не реже одного раза в год в срок до 31 января** указанная информация передается в ЦБЗ по форме Приложения №3 Регламента.

ЦБЗ и РМИАЦ имеют право проводить проверки реализации подключения. В случае выявления нарушений требований настоящего Регламента, РМИАЦ немедленно производит отключение VPN-соединений соответствующей ИСПДн обслуживаемого учреждения от ИСПДн ЦБЗ, а ЦБЗ блокирует выданные обслуживаемому учреждению идентификаторы.

Типовая схема №1



Типовая схема №2



Приложение № 3
к РЕГЛАМЕНТУ взаимодействия с ИСПДн
ГКУ «ЦБЗ при Минздраве Карелии»

**Заявка на присоединение к регламенту и подключение к
ИСПДн Центра бухучета и закупок¹**

Наименование организации				
ИНН/ОГРН				
Наименование подключаемой ИСПДн		«Бухгалтерский и кадровый учет»		
Номер используемой схемы подключения (Схема №1 / Схема №2)				
Адрес точки подключения ИСПДн				
ID узла сети VipNet № 934, подлежащего подключению				
IP-адрес АРМ подлежащего подключению				
1	ФИО, должность сотрудника ответственного за внесение сведений в ИСПДн Центра бухучета и закупок		Полномочия (Запись, Просмотр, КЭП, ПЭП...) ⁴	1С:БГУ ²
			Полномочия (Запись, Просмотр, КЭП, ПЭП...) ⁴	1С:ЗиК ³
...
99	ФИО, должность сотрудника ответственного за внесение сведений в ИСПДн Центра бухучета и закупок		Полномочия (Запись, Просмотр, КЭП, ПЭП...) ⁴	1С:БГУ ²
			Полномочия (Запись, Просмотр, КЭП, ПЭП...) ⁴	1С:ЗиК ³
ФИО, должность сотрудника ответственного за обеспечение мер по защите информации, содержащейся в ИСПДн, адрес электронной почты, контактный телефон				
Средство защиты от НСД				
Межсетевой экран				
Средство антивирусной защиты				
СКЗИ				

Прошу подключить к ИСПДн ЦБЗ. ИСПДн организации в соответствии с вышеуказанной информацией и на условиях согласно Регламента взаимодействия с ИСПДн Государственного казённого учреждения Республики Карелия "Центр бухгалтерского учёта и организации закупок при Министерстве здравоохранения Республики Карелия».

Все необходимые меры по обеспечению безопасности ПДн в подключаемой ИСПДн приняты. Работы по установке, монтажу, запуску и первоначальной настройке средств защиты информации и СКЗИ выполнены в соответствии с требованиями ТУ и ЭД на данные средства.

Обязанность по поддержанию системы защиты ИСПДн в актуальном состоянии возложена на ответственного за обеспечение мер по защите информации, содержащейся в ИСПДн. В случае изменения информации указанной в данной заявке организация–заявитель обязуется сообщить об изменениях, путем подачи новой заявки.

Должность: _____

ФИО: _____

Подпись: _____

« ____ » _____ 20 ____ г

МП

Отметка Центра бухучета и закупок

<p><i>Заявка отклонена.</i> <i>Причина отказа:</i></p> <p>_____</p> <p>_____</p>	<p>Заявка Утверждена</p> <p>Должность: Директор</p> <p>ФИО: Шиманская Мария Викторовна</p> <p>Подпись: _____</p> <p>« ____ » _____ 20 ____ г МП</p>
--	--

Отметка РМИАЦ

<p><i>Заявка отклонена.</i> <i>Причина отказа:</i></p> <p>_____</p> <p>_____</p>	<p>Работы по подключению выполнены:</p> <p>Должность: _____</p> <p>ФИО: _____</p> <p>Подпись: _____</p> <p>« ____ » _____ 20 ____ г МП</p>
--	---

1 - Пример заполнения заявки см.в Приложении 4 к Регламенту

2 - 1С:БГУ – 1С:Предприятие. Бухгалтерия государственного учреждения (доступ к финансовым документам, документам по расчетам с подотчетными лицами и т.п.)

3 - 1С:ЗиК – 1С: Предприятие. Зарплата и кадры бюджетного учреждения (доступ к кадровым документам)

4 - Запись – создание/исправление документов ИСПДн

Просмотр – только просмотр без возможности изменения документов

ПЭП – использование простой электронной подписи (логин и пароль)

КЭП – использование квалифицированной электронной подписи

Приложение № 4
к РЕГЛАМЕНТУ взаимодействия с ИСПДн
ГКУ «ЦБЗ при Минздраве Карелии»

Заявка на присоединение к регламенту и подключение к ИСПДн Центра бухучета и закупок (Пример заполнения)

Наименование организации		ГБУЗ РК «ЗДОРОВЬЕ»		
ИНН/ОГРН		1234567890/1234567890123		
Наименование подключаемой ИСПДн		«Бухгалтерский и кадровый учет»		
Номер используемой схемы подключения (Схема №1 / Схема №2)		Схема № 2		
Адрес точки подключения ИСПДн		185000, г.Петрозаводск, ул. Вымышленная, дом 1, серверная		
ID узла ViPnet подлежащего подключению		03A60777 CM ЗДОРОВЬЕ (VPN № 934)		
IP-адрес АРМ подлежащего подключению		172.16.35.77		
1	ФИО, должность сотрудника ответственного за внесение сведений в ИСПДн Центра бухучета и закупок	Иванов Иван Иванович, директор	Полномочия: просмотр, КЭП	1С:БГУ
2	ФИО, должность сотрудника ответственного за внесение сведений в ИСПДн Центра бухучета и закупок	Сидоров Сидр Сидорович, специалист	Полномочия: Запись, ПЭП	1С:БГУ
			Полномочия: Запись	1С:ЗиК
ФИО, должность сотрудника ответственного за обеспечение мер по защите информации, содержащейся в ИСПДн, адрес электронной почты, контактный телефон		Петров Петр Петрович, Администратор безопасности superadminpetrov@bestmail.ru +79990000000		
Средство защиты от НСД		Secret Net 7		
Межсетевой экран		ПАК ViPNet Coordinator HW 3		
Средство антивирусной защиты		Kaspersky Endpoint Security 10 для Windows		
СКЗИ		ПАК ViPNet Coordinator HW 3		

Прошу подключить к ИСПДн ЦБЗ. ИСПДн организации в соответствии с вышеуказанной информацией и на условиях согласно Регламента взаимодействия с ИСПДн Государственного казённого учреждения Республики Карелия "Центр бухгалтерского учёта и организации закупок при Министерстве здравоохранения Республики Карелия».

Все необходимые меры по обеспечению безопасности ПДн в подключаемой ИСПДн приняты. Работы по установке, монтажу, запуску и первоначальной настройке средств защиты информации и СКЗИ выполнены в соответствии с требованиями ТУ и ЭД на данные средства.

