ПРАВИТЕЛЬСТВО САХАЛИНСКОЙ ОБЛАСТИ

П О С Т А Н О В Л Е Н И Е

от 11 июля 2019 г. № 300

г. Южно-Сахалинск

Об организации функционирования единой централизованной информационной системы бухгалтерского учета и отчетности Сахалинской области

В соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Концепцией создания и развития государственной интегрированной информационной системы управления общественными финансами «Электронный бюджет», утвержденной распоряжением Правительства Российской Федерации от 20.07.2011 № 1275-р, а также в целях построения эффективной системы централизованного ведения бухгалтерского учета и составления отчетности Правительство Сахалинской области **п о с т а н о в л я е т:**

1. Создать и внедрить в практику деятельности органов исполнительной власти Сахалинской области и государственных учреждений Сахалинской области Государственную информационную систему «Единая централизованная информационная система бухгалтерского учета и отчетности Сахалинской области» (далее - ЕЦИС).

2. Утвердить Положение о Государственной информационной системе «Единая централизованная информационная система бухгалтерского учета и отчетности Сахалинской области» (далее - Положение) (прилагается).

3. Определить министерство финансов Сахалинской области органом, уполномоченным на создание и эксплуатацию ЕЦИС.

4. Определить оператором ЕЦИС подведомственное учреждение министерства финансов Сахалинской области - государственное казенное учреждение «Межведомственный центр бухгалтерского обслуживания» (далее - ГКУ МЦБО).

5. Оператору ЕЦИС:

5.1. В соответствии с приказом Федеральной службы по техническому и экспортному контролю от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» разработать и внедрить систему защиты информации в ЕЦИС, аттестовать ЕЦИС по требованиям безопасности информации.

5.2. Для исполнения функций по ведению бюджетного (бухгалтерского) учета, составлению бюджетной, налоговой отчетности, отчетности в государственные внебюджетные фонды при обслуживании органов исполнительной власти Сахалинской области использовать ЕЦИС, руководствуясь Положением.

5.3. В соответствии с разделом 4 Положения обеспечить регистрацию пользователей в ЕЦИС.

6. Органам исполнительной власти Сахалинской области и государственным учреждениям Сахалинской области, заключившим соглашение с ГКУ МЦБО о передаче функций по ведению бюджетного (бухгалтерского) учета, составлению бюджетной, налоговой отчетности, отчетности в государственные внебюджетные фонды в условиях электронного документооборота, использовать ЕЦИС, руководствуясь Положением.

7. Опубликовать настоящее постановление в газете «Губернские ведомости», на официальном сайте Губернатора и Правительства Сахалинской области, на «Официальном интернет-портале правовой информации».

Председатель Правительства
Сахалинской области А.В.Белик

УТВЕРЖДЕНО

постановлением Правительства
Сахалинской области
от 11 июля 2019 г. № 300

ПОЛОЖЕНИЕ
о Государственной информационной системе «Единая централизованная информационная система бухгалтерского учета и отчетности Сахалинской области»

1. Общие положения

1.1. Настоящее Положение определяет цель создания, назначение и основные функции Государственной информационной системы «Единая централизованная информационная система бухгалтерского учета и отчетности Сахалинской области» (далее - ЕЦИС), участников информационного взаимодействия, их полномочия, порядок подключения к информационным ресурсам ЕЦИС.

1.2. Цель создания ЕЦИС - построение эффективной системы централизованного ведения бухгалтерского учета и составления отчетности органов исполнительной власти Сахалинской области и государственных учреждений Сахалинской области (с возможностью ее дальнейшего развития).

1.3. Основными задачами создания ЕЦИС являются:

а) соблюдение единой методологии бухгалтерского учета для органов исполнительной власти Сахалинской области и государственных учреждений Сахалинской области;

б) снижение трудозатрат и повышение производительности при ведении учета финансово-хозяйственной деятельности органов исполнительной

власти Сахалинской области и государственных учреждений Сахалинской области;

в) поддержка электронного юридически значимого документооборота с применением электронной подписи в рамках соглашений о передаче функций по ведению бюджетного (бухгалтерского) учета, составлению бюджетной, налоговой отчетности, отчетности в государственные внебюджетные фонды;

г) обеспечение единства и однократности ввода нормативной и справочной информации при ведении бухгалтерского учета и составлении отчетности;

д) обеспечение возможности удаленной работы в ЕЦИС;

е) обеспечение возможности поэтапного наращивания функциональности ЕЦИС при централизации ведения бухгалтерского учета и составления отчетности органов исполнительной государственной власти Сахалинской области, государственных учреждений Сахалинской области;

ж) оперативное получение достоверной информации и необходимой аналитической отчетности.

1.4. Основным назначением ЕЦИС является выполнение функций по ведению бухгалтерского учета, составлению бухгалтерской, налоговой, статистической и кадровой отчетности, отчетности в государственные внебюджетные фонды в соответствии с требованиями действующего законодательства.

1.5. ЕЦИС обеспечивает реализацию следующих функций:

а) ведение бухгалтерского учета;

б) ведение складского учета и учета товарно-материальных ценностей материально ответственными лицами;

в) осуществление бюджетного планирования и финансирования;

г) ведение кадрового учета;

д) составление отчетности.

2. Основные принципы построения ЕЦИС

Основными принципами, на основе которых формируется и функционирует ЕЦИС, являются:

а) полнота, актуальность и достоверность информации, обрабатываемой в ЕЦИС;

б) адаптируемость состава информационных ресурсов ЕЦИС к изменяющимся требованиям законодательства;

в) единство используемых терминов, нормативно-справочной информации, системы показателей, регламентов отчетности;

г) единство стандартов технологий, форматов, протоколов взаимодействия участников создания и эксплуатации ЕЦИС;

д) информационная безопасность ЕЦИС.

3. Полномочия и обязанности участников информационного взаимодействия

3.1. Участниками информационного взаимодействия являются:

а) Оператор ЕЦИС;

б) поставщики информации - органы исполнительной власти Сахалинской области, государственные учреждения Сахалинской области.

3.2. Оператор ЕЦИС осуществляет:

а) организацию ведения в ЕЦИС бухгалтерского учета, составления бухгалтерской и налоговой отчетности, отчетности в государственные внебюджетные фонды в соответствии с требованиями действующего законодательства;

б) разработку и принятие в пределах своей компетенции правовых актов, регламентирующих вопросы организации, функционирования и развития ЕЦИС, в том числе определения количества и условий согласования заявок поставщиков информации на предоставление доступа к ЕЦИС сотрудникам органов исполнительной власти Сахалинской области, государственных учреждений Сахалинской области, выполняющих обработку информации в ЕЦИС (далее - внешние пользователи);

в) организационно-методическое обеспечение функционирования ЕЦИС, в том числе организационные меры по защите информации в пределах своей компетенции;

г) в рамках своей компетенции функции поставщика информации в ЕЦИС;

д) заключение с поставщиками информации соглашений о передаче функций по ведению бюджетного (бухгалтерского) учета, составлению бюджетной, налоговой отчетности, отчетности в государственные внебюджетные фонды в условиях электронного документооборота (далее - Соглашение);

е) в отношении поставщиков информации, с которыми заключено Соглашение, ведение в ЕЦИС бюджетного (бухгалтерского) учета, составление бюджетной, налоговой отчетности, отчетности в государственные внебюджетные фонды поставщиков информации в соответствии с требованиями действующего законодательства;

ж) согласование заявок поставщиков информации на предоставление доступа к ЕЦИС внешним пользователям, предоставление доступа поставщикам информации к ЕЦИС на основании соответствующей заявки;

з) обеспечение эффективного и бесперебойного функционирования ЕЦИС, техническую поддержку ЕЦИС с соблюдением требований законодательства в сфере информационных технологий;

и) консультирование внешних пользователей поставщиков информации по вопросам технической поддержки функционирования ЕЦИС;

к) выполнение организационных и технических мер по защите информации, размещаемой в ЕЦИС, в соответствии с требованиями действующего законодательства;

л) принятие своевременных мер по совершенствованию и развитию технических средств, на которых размещен ЕЦИС, и обновлению программного обеспечения, используемого для функционирования ЕЦИС;

м) резервное копирование данных и хранение резервных копий данных ЕЦИС.

3.3. Оператор имеет право на договорной основе привлекать подрядчиков для осуществления сопровождения ЕЦИС и обеспечения информационной безопасности (администрирование, обновление программного обеспечения, используемого для функционирования ЕЦИС, а также для выполнения других работ и предоставления услуг, связанных с функционированием ЕЦИС).

3.4 Поставщики информации ЕЦИС осуществляют занесение информации внешними пользователями в ЕЦИС в соответствии с предоставленным доступом к интерфейсам в ЕЦИС.

4. Порядок взаимодействия и организации доступа к ресурсам ЕЦИС

4.1. Механизм информационного взаимодействия Оператора ЕЦИС с поставщиками информации устанавливается Соглашением.

4.2. Доступ к системе предоставляется на основании регламента подключения внешних пользователей к ЕЦИС (приложение к настоящему Положению).

5. Обеспечение информационной безопасности

5.1. Политика режима информационной безопасности ЕЦИС направлена на обеспечение доступности информации, ее целостности и в отдельных случаях конфиденциальности, которая базируется на Федеральном законе от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 05.12.2016 № 646, и на региональных нормативных правовых актах.

5.2. Предотвращение хищения и повреждения средств вычислительной техники, на которых хранятся информационные ресурсы ЕЦИС, обеспечивается особым режимом доступа в помещения с находящейся в них техникой, исключающим нахождение в нем посторонних лиц, оснащением помещений с вычислительной и коммутационной техникой охранной и пожарной сигна-

лизацией. Обязанности внешних пользователей ЕЦИС по безопасной работе в ЕЦИС и их действия в нестандартных ситуациях описаны в руководствах для пользователей ЕЦИС.

5.3. Исключение возможности несанкционированного доступа к информационным ресурсам с целью предотвращения утечки, хищения, утраты, искажения, подделки, уничтожения информации обеспечивается штатными средствами и методами, предусмотренными используемыми операционными системами. Каждый внешний пользователь ЕЦИС проходит аутентификацию на сервере ЕЦИС. Права доступа внешних пользователей ЕЦИС к информационным ресурсам разграничены в соответствии с выполняемыми функциями.

5.4. Для обеспечения своевременности обнаружения фактов несанкционированного доступа к информации в ЕЦИС ведутся системные электронные журналы.

5.5. Средства ЕЦИС обеспечивают ежедневное резервное копирование и возможность восстановления актуального состояния ЕЦИС при нарушении безопасности информации.

ПРИЛОЖЕНИЕ

к Положению о Государственной информационной системе «Единая централизованная информационная система бухгалтерского учета и отчетности Сахалинской области», утвержденному постановлением Правительства Сахалинской области

от 11 июля 2019 г. № 300

РЕГЛАМЕНТ

подключения внешних пользователей к Государственной информационной системе «Единая централизованная информационная система бухгалтерского учета и отчетности Сахалинской области»

1. Общие положения

Регламент подключения внешних пользователей к Государственной информационной системе «Единая централизованная информационная система бухгалтерского учета и отчетности Сахалинской области» (далее - Регламент) определяет общий состав, содержание и порядок выполнения участниками информационного взаимодействия работ по защите информации при их подключении к защищенной сети Государственной информационной системы «Единая централизованная информационная система бухгалтерского учета и отчетности Сахалинской области» (далее - ЕЦИС) Оператором.

Защищенная сеть предназначена для обеспечения информационной безопасности ЕЦИС.

Регламент разработан в соответствии со следующими нормативно-правовыми актами:

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- приказ Федеральной службы по техническому и экспортному контролю от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

- приказ Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

В Регламенте используются следующие понятия и сокращения:

ViPNet Administrator	-	программное обеспечение, предназначенное для конфигурирования и управления виртуальной защищённой сетью ViPNet
ViPNet Client 4	-	программное обеспечение, реализующее на рабочем месте внешнего пользователя или сервере функцию VPN-клиента, персонального экрана и клиента защищённой почтовой службы
ViPNet Coordinator	-	программное обеспечение, выполняющее функции универсального сервера виртуальной защищённой сети ViPNet
VPN (Virtual Private Network)	-	обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети
СЗИ от НСД	-	средство защиты информации от несанкционированного доступа

ЕЦИС, Система	-	Государственная информационная система «Единая централизованная информационная система бухгалтерского учета и отчетности Сахалинской области»
Оператор	-	государственное казенное учреждение «Межведомственный центр бухгалтерского обслуживания»
Внешние пользователи	-	внешние пользователи Государственной информационной системы «Единая централизованная информационная система бухгалтерского учета и отчетности Сахалинской области»
ПКИ	-	парольно-ключевая информация
Абонентский пункт	-	узел сети по ViPNet
Абонент	-	внешний пользователь сети ViPNet

Основной целью Регламента является определение обязательного плана работ при подключении в защищенную сеть внешних пользователей, необходимых для выполнения требований по обеспечению информационной безопасности в ЕЦИС.

В соответствии с приказом Федеральной службы по техническому и экспортному контролю от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и другими нормативными актами, применяемыми для ЕЦИС Оператора, информационное взаимодействие с ЕЦИС, осуществляемое внешними пользователями ЕЦИС, должно осуществляться по защищенному каналу связи, а на рабочих местах должны быть установлены и корректно настроены сертифицированные средства защиты информации.

В целях реализации технических требований разработана типовая схема подключения внешних пользователей ЕЦИС и регламентирован способ организации защищенного исполнения автоматизированных рабочих мест (далее - АРМ) внешних пользователей.

Данный Регламент определяет:

- порядок организации и подключения участников информационного взаимодействия к защищенной сети Оператора;

- порядок предоставления доступа к ЕЦИС Оператора;

- порядок организации безопасного межсетевого взаимодействия с ЕЦИС.

2. Технологическое решение по защите ЕЦИС

ЕЦИС обеспечивает информационную поддержку процедур подготовки и принятия управленческих решений в сфере финансово-хозяйственной деятельности органов исполнительной власти и государственных учреждений Сахалинской области, повышает эффективность контроля расходов органов исполнительной власти и государственных учреждений Сахалинской области.

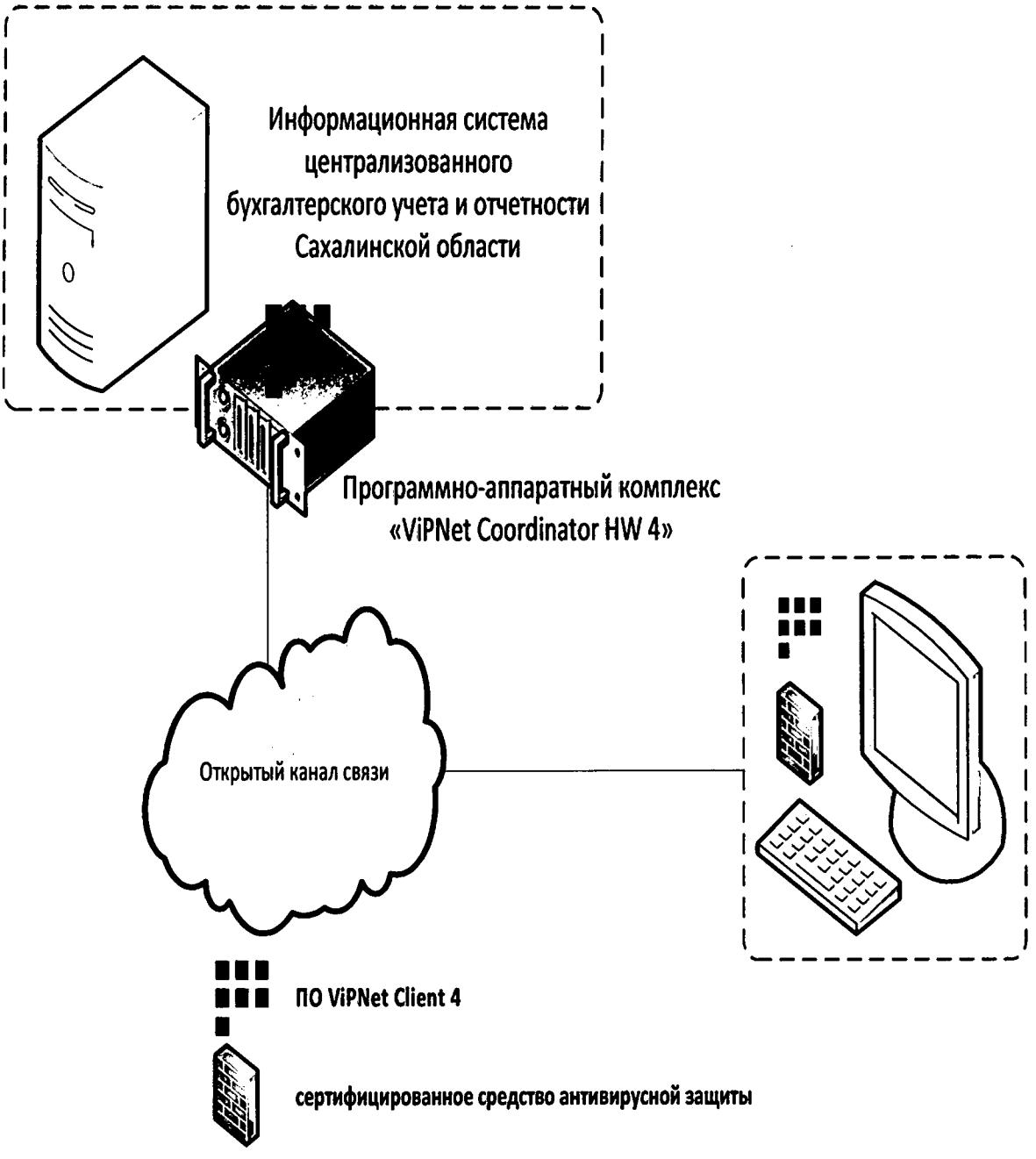
Базы данных ЕЦИС функционируют на аттестованных по требованиям безопасности серверах, расположенных по адресу: 693009, Сахалинская область, г. Южно-Сахалинск, Коммунистический проспект, д. 32, серверная.

Подсистема обеспечения информационной безопасности серверов в части обеспечения криптографической защиты информации реализована на основе сертифицированных программно-аппаратных комплексов «ViPNet Coordinator HW 4» (ViPNet Coordinator HW2000).

На основе решений на базе ПАК «ViPNet Coordinator HW2000» организована защищенная виртуальная сеть. Номер защищенной сети ViPNet - 3735. Программный комплекс «ViPNet Administrator 4» выполняет функции администрирования защищенной сети.

Обобщенная схема информационного взаимодействия ЕЦИС с АРМ внешних пользователей ЕЦИС представлена на схеме.

Схема


Информационная система
централизованного
бухгалтерского учета и отчетности
Сахалинской области
Программно-аппаратный комплекс
«ViPNet Coordinator HW 4»
Открытый канал связи
ПО ViPNet Client 4
сертифицированное средство антивирусной защиты

3. Требования к реализации системы защиты информации и защищенного взаимодействия

Для организации защищенного взаимодействия с ЕЦИС внешние пользователи должны использовать АРМ, на котором установлено сертифицированное по требованиям безопасности информации:

- средство криптографической защиты информации для организации сертифицированного VPN;

- средство антивирусной защиты.

Для возможности реализации защищенного взаимодействия АРМ внешних пользователей с ЕЦИС и обеспечения требований по защите информации участники информационного взаимодействия должны обеспечить реализацию организационных и технических мероприятий.

Технические мероприятия включают:

- установку и настройку тонкого клиента приложения системы «1С: Бухгалтерия»;

- обеспечение безопасного межсетевого взаимодействия;

- обеспечение защиты конфиденциальности и целостности передаваемой по каналам связи информации.

Организационные мероприятия включают:

- разработку документации, регламентирующей меры по защите информации;

- разработку документации, регламентирующей работу ответственных лиц по защите информации.

Не допускается взаимодействие АРМ внешних пользователей с ЕЦИС 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 АРМ внешних пользователей ЕЦИС для возможности включения их в ЕЦИС

Организация подключения внешних пользователей к защищенной сети включает в себя следующие стадии:

1. Заявительная стадия.

2. Стадия рассмотрения заявления.

3. Закупка и установка необходимых программных средств защиты информации (далее - СЗИ) потенциальным участником информационного взаимодействия (далее - Претендент):

- сертифицированного ФСБ России средства криптографический защиты информации «ViPNet Client 4»;

- сертифицированного средства антивирусной защиты.

4. Формирование и передача ключевой информации, формирование и передача учетных записей для доступа к информационным системам.

5. Организационные мероприятия.

4.1. Заявительная стадия

Претендент, желающий подключиться к защищенной сети, направляет в адрес Оператора заявление о намерении подключиться к защищенной сети (форма № 1).

В заявлении, изготовленном на бланке организации, должна содержаться следующая информация:

- наименование Абонентских пунктов, состоящее из названия организации и подразделения;

- количество подключаемых Абонентских пунктов;

- перечень информационных систем, к которым необходимо организовать доступ Претендента;

- Ф.И.О. и контактный телефон лица, ответственного за подключение Претендента.

4.2. Стадия рассмотрения заявления

В ГКУ «Межведомственный центр бухгалтерского обслуживания» заявление рассматривает рабочая группа, назначенная приказом руководителя ГКУ «Межведомственный центр бухгалтерского обслуживания». В состав рабочей группы входит председатель, члены и секретарь рабочей группы.

Рабочая группа проводит заседания в течение 5 рабочих дней со дня получения заявления о намерении подключиться к защищенной сети по каждому поступившему заявлению или, при наличии нескольких заявлений, одно заседание по рассмотрению всех поступивших заявлений.

На заседании оцениваются основания для подключения Претендента к защищенной сети и техническая возможность организации связи и доступа к информационным системам.

Итог заседания - протокол, отражающий принятое решение.

Решение о подключении Претендента к защищенной сети направляется в письменной форме в адрес Претендента или по электронной почте, указанной в заявке Претендента, в течение 3 рабочих дней со дня принятия указанного решения.

4.3. Закупка и установка необходимых программных СЗИ Претендентом

В случае принятия положительного решения о подключении к защищенной сети, Претендент самостоятельно приобретает программное обеспечение «ViPNet Client 4» и сертифицированное антивирусное обеспечение.

При заключении договора о покупке программного обеспечения ViPNet «ViPNet Client 4» Претендент указывает в договоре номер защищенной сети для подключения - 3735.

Подключение Претендента к защищенной сети осуществляется администратором защищенной сети ГКУ «Межведомственный центр бухгалтерского обслуживания» после получения регистрационных файлов (парольно-ключевой информации).

Администратор защищенной сети уведомляет Претендента о получении регистрационных файлов.

Установка СЗИ производится организацией, обладающей лицензией на проведение соответствующих работ. По итогу установки СЗИ составляется и подписывается акт установки и ввода в эксплуатацию средств защиты информации.

4.4. Формирование и передача ключевой информации

Претендент после получения информации о поступлении регистрационных файлов формирует и направляет в ГКУ «Межведомственный центр бухгалтерского обслуживания» заявку на подключение (форма № 2).

В течение 3 рабочих дней со дня получения от Претендента заявки на подключение администратор защищенной сети:

- производит регистрацию Абонентских пунктов и Абонентов в центре управления сетью;

- устанавливает со своей стороны во взаимодействии с Претендентом связь между Абонентскими пунктами в соответствии с заявкой на подключение;

- формирует дистрибутивы ключей для Абонентских пунктов вместе с паролем доступа к нему;

- по завершении обозначенных работ уведомляет об этом Претендента.

Претендент для получения дистрибутива ключей и пароля доступа к нему должен:

1. Предоставить в адрес ГКУ «Межведомственный центр бухгалтерского обслуживания»:

- копию правового акта о назначении Абонентов защищенной сети по форме № 3;

- копию договора на приобретенное программное обеспечение «ViPNet Client 4»;

- носитель информации для записи дистрибутивов ключей.

2. Направить в ГКУ «Межведомственный центр бухгалтерского обслуживания» доверенное лицо на получение дистрибутива ключей с предъявлением доверенности по форме № 4.

Факт выдачи дистрибутива ключей заносится в журнал учета выдачи ключевых документов (форма № 5).

Администратор защищенной сети ГКУ «Межведомственный центр бухгалтерского обслуживания» формирует учетные записи для доступа и передает их доверенному лицу Претендента на условиях и в сроки по взаимному согласованию.

4.5. Организационные мероприятия

Организационные мероприятия включают в себя разработку Претендентом необходимой документации по эксплуатации криптографических средств в соответствии с приказами ФСБ России от 09.02.2005 № 66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)», от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» - правового акта об утверждении перечня мер, направленных на выполнение требований законодательства Российской Федерации в области защиты информации с использованием средств криптографической защиты, включающего в себя следующие мероприятия:

- назначение ответственного пользователя криптосредств;

- утверждение инструкции ответственного пользователя криптосредств;

- утверждение перечня сотрудников, допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности информации;

- утверждение инструкции пользователей криптосредств;

- утверждение перечня помещений, где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств;

- утверждение перечня лиц, имеющих доступ в помещения, где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств;

- утверждение порядка доступа в помещения, где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств;

- утверждение формы журнала поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов;

- утверждение формы лицевого счета пользователя криптосредств.

ФОРМА № 1

к Регламенту подключения внешних пользователей к Государственной информационной системе «Единая централизованная информационная система бухгалтерского учета и отчетности Сахалинской области»

Руководителю ГКУ «Межведомственный центр бухгалтерского обслуживания»

693009, Сахалинская область,
г. Южно-Сахалинск,
Коммунистический проспект, д. 32

ЗАЯВЛЕНИЕ
о подключении к Государственной информационной системе «Единая централизованная информационная система бухгалтерского учета и отчетности Сахалинской области»

Прошу подключить _____ к Государственной информационной системе «Единая централизованная информационная система бухгалтерского учета и отчетности Сахалинской области» для обмена информацией.

Предполагаемое число подключаемых Абонентских пунктов – _____.

Перечень информационных систем, к которым необходим доступ:

- 1С: Бухгалтерия государственного учреждения.
- 1С: Зарплата и кадры для государственного учреждения.
- 1С: Документооборот государственного учреждения.

Лицо, ответственное за подключение, контактный телефон: _____ _____.

Руководитель органа исполнительной власти (государственного учреждения) Сахалинской области _____ _____
(подпись) (Ф.И.О.)

М.П.

_____

ФОРМА № 2

к Регламенту подключения внешних пользователей к Государственной информационной системе «Единая централизованная информационная система бухгалтерского учета и отчетности Сахалинской области»

ЗАЯВКА

администратору защищенной сети на подключение к защищенной виртуальной сети ViPNet 3735

1. Полное наименование организации
2. Сокращенное название организации
3. Юридический адрес организации
4. Фактический (почтовый) адрес организации
5. Ф.И.О. руководителя
6. Должность руководителя
7. Количество необходимых для регистрации Абонентских пунктов
8. Наименование Абонентских пунктов
9. Ф.И.О. доверенного лица
10. Контактные телефоны доверенного лица
11. Контактный E-mail доверенного лица
12. Наименование поставщика и реквизиты договора на приобретенное программное обеспечение «ViPNet Client 4» к защищенной виртуальной сети ViPNet 3735 с приложением копии данного договора, который остается в ГКУ «Межведомственный центр бухгалтерского обслуживания»

ФОРМА № 3

к Регламенту подключения внешних пользователей к Государственной информационной системе «Единая централизованная информационная система бухгалтерского учета и отчетности Сахалинской области»

ПРАВОВОЙ АКТ

о назначении Абонентов защищенной виртуальной сети ViPNet 3735 ГКУ «Межведомственный центр бухгалтерского обслуживания»

Для выполнения служебных обязанностей с использованием сервисов и информационных систем защищенной виртуальной сети ViPNet 3735 ГКУ «Межведомственный центр бухгалтерского обслуживания»:

1. Назначить Абонентами защищенной виртуальной сети ViPNet 3735 ГКУ «Межведомственный центр бухгалтерского обслуживания»:

- пользователя: _____;
- пользователя: _____.

2. В своей работе Абонентам защищенной виртуальной сети ViPNet 3735 ГКУ «Межведомственный центр бухгалтерского обслуживания» руководствоваться Регламентом подключения внешних пользователей к Государственной информационной системе «Единая централизованная информационная система бухгалтерского учета и отчетности Сахалинской области».

3. Контроль за исполнением настоящего правового акта оставляю за собой.

Руководитель органа исполнительной власти (государственного учреждения) Сахалинской области _____ _____

(подпись) (Ф.И.О.)

М.П.

ФОРМА № 4

к Регламенту подключения внешних пользователей к Государственной информационной системе «Единая централизованная информационная система бухгалтерского учета и отчетности Сахалинской области»

ДОВЕРЕННОСТЬ

на получение дистрибутива ключей к защищенной виртуальной сети ViPNet 3735 ГКУ «Межведомственный центр бухгалтерского обслуживания»

_____ «___» _____ 20___ г.

(наименование населенного пункта)

_____

(наименование Абонента)

в лице руководителя _____,

действующего на основании _____

уполномочивает: _____

(ФИО, паспортные данные доверенного лица)

получить в ГКУ «Межведомственный центр бухгалтерского обслуживания» дистрибутив ключей для первичного запуска прикладной программы сети ViPNet 3735 ГКУ «Межведомственный центр бухгалтерского обслуживания».

Настоящая доверенность действительна до «___» _____ 20___ г.

Руководитель органа исполнительной власти (государственного учреждения) Сахалинской области _____ _____

(подпись) (Ф.И.О.)

М.П.

_____

ФОРМА № 5

к Регламенту подключения внешних пользователей к Государственной информационной системе «Единая централизованная информационная система бухгалтерского учета и отчетности Сахалинской области»

ЖУРНАЛ
учета выдачи ключевых документов

№ пп.	Дата выдачи	Организация	Идентификатор дистрибутива	Тип носителя	Ф.И.О. получателя	Роспись получателя