Приложение № 2

Утверждено

приказом АУ «ЦИТ»
Минцифры Чувашии

от 21.06.2023 № 74

**Регламент**

**подключения к единой централизованной информационной системе бюджетного (бухгалтерского) учета и отчетности**

1. Общие положения

Регламент подключения к единой централизованной информационной системе бюджетного (бухгалтерского) учета и отчетности (далее соответственно – Регламент) определяет общий состав, содержание и порядок выполнения мероприятий, необходимых для подключения к единой централизованной информационной системе бюджетного (бухгалтерского) учета и отчетности.

В настоящем Регламенте используются следующие понятия:

единая централизованная информационная система бюджетного (бухгалтерского) учета и отчетности (далее – ЕЦИС) – информационная система, обеспечивающая построение эффективной системы централизованного бюджетного (бухгалтерского) учета и отчетности в государственных органах Чувашской Республики, государственных учреждениях Чувашской Республики, подведомственных органам государственной власти Чувашской Республики, а в муниципальных учреждениях - в соответствии с соглашениями между муниципальными районами и городскими округами и оператором инфраструктуры ЕЦИС о взаимодействии;

инфраструктура ЕЦИС – технологически и территориально обособленные серверные комплексы, размещенные в Республиканском центре обработки данных, включающие в себя серверное и коммуникационное оборудование, системы хранения и резервного копирования данных и иные вспомогательные системы;

оператор ЕЦИС – казенное учреждение Чувашской Республики «Республиканский центр бухгалтерского учета», государственный орган Чувашской Республики, государственное учреждение Чувашской Республики, подведомственное органу государственной власти Чувашской Республики, функции по бюджетному (бухгалтерскому) учету и отчетности которого не переданы казенному учреждению Чувашской Республики «Республиканский центр бухгалтерского учета» либо централизованной бухгалтерии подведомственной органу исполнительной власти Чувашской Республики, централизованная бухгалтерия подведомственных органу исполнительной власти Чувашской Республики учреждений, находящаяся в его ведении, централизованная бухгалтерия муниципального района (городского округа) в соответствии с соглашением.

пользователь ЕЦИС – уполномоченное оператором ЕЦИС должностное лицо, получившее в установленном порядке доступ к ЕЦИС и выполняющее обработку информации в ЕЦИС;

технический оператор инфраструктуры ЕЦИС – автономное учреждение Чувашской Республики «Центр информационных технологий» Министерства цифрового развития, информационной политики и массовых коммуникаций Чувашской Республики.

Иные понятия и термины, используемые в настоящем Регламенте, применяются в значениях, определенных федеральными законами «Об информации, информационных технологиях и о защите информации», «О персональных данных», «Об электронной подписи» и принимаемыми в соответствии с ними нормативными правовыми актами, а также постановлением Кабинета Министров Чувашской Республики от 28 декабря 2018 года № 583 «Об утверждении Положения об инфраструктуре единой централизованной информационной системы бюджетного (бухгалтерского) учета и отчетности».

Основной целью Регламента является определение необходимых мероприятий по обеспечению информационной безопасности, проводимых оператором ЕЦИС при организации подключения автоматизированных рабочих мест, предназначенных для обеспечения информационного взаимодействия с ЕЦИС (далее – АРМ оператора ЕЦИС) по защищенным с использованием шифровальных (криптографических) средств каналам передачи данных (далее также – защищенное информационное взаимодействие), регистрации должностных лиц оператора ЕЦИС в качестве пользователей ЕЦИС и получении ими необходимых прав доступа для работы в ЕЦИС.

Принимаемые оператором ЕЦИС меры по защите информации при её обработке в ЕЦИС, в том числе при подключении АРМ оператора ЕЦИС к ЕЦИС и организации доступа должностных лиц оператора ЕЦИС для работы в ЕЦИС, должны соответствовать требованиям федеральных законов «Об информации, информационных технологиях и о защите информации», «О персональных данных», принимаемым в соответствии с ними нормативным правовым актам, методическим и руководящим документов Федеральной службы по техническому и экспортному контролю (далее – ФСТЭК России) и Федеральной службы безопасности Российской Федерации (далее – ФСБ России) в области защиты информации и настоящим Регламентом.

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, Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом ФСТЭК России от 18 февраля 2013 года № 21, Составом и содержанием 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, утвержденных приказом ФСБ России от 10 июля 2014 года № 378, при обработке информации в информационных системах персональных данных и её передаче по сетям связи общего пользования, в том числе информационно-телекоммуникационной сети Интернет (далее – сеть Интернет), должны применятся сертифицированные по требованиям безопасности информации средства защиты информации и средства криптографической защиты информации (далее также – СКЗИ).

Применяемые организационные и технические меры защиты информации должны удовлетворять требованиям, установленным для 3 класса защищенности государственных информационных систем и требованиям, установленным для 4 уровня защищенности персональных данных.

1. Требования к реализации организационных и технических мероприятий по обеспечению защиты информации

В целях организации защищенного информационного взаимодействия с ЕЦИС оператор ЕЦИС обеспечивает реализацию организационных и технических мероприятий по обеспечению безопасности персональных данных и иной информации ограниченного доступа (далее – защищаемая информация) при её обработке на АРМ оператора ЕЦИС.

Организационные мероприятия по обеспечению защиты информации должны включать:

назначение должностных лиц, ответственных за обеспечение информационного взаимодействия с ЕЦИС (пользователей ЕЦИС);

организацию режима обеспечения безопасности помещений, в которых размещены технические и программные средства, участвующие в обработке защищаемой информации, а также помещений, где используются или хранятся средства защиты информации и СКЗИ, носители защищаемой информации, в том числе носители персональных данных, носители ключевой, аутентифицирующей и парольной информации (далее – защищаемое помещение);

обеспечение сохранности носителей персональных данных и иной защищаемой информации;

принятие мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами;

принятие мер, направленных на обеспечение защиты информации и безопасности персональных данных при их обработке в информационных системах.

* + 1. Обеспечиваемый режим безопасности защищаемых помещений должен исключать возможность неконтролируемого проникновения или пребывания в данных помещениях, лиц, не имеющих права доступа в защищаемые помещения. Организация обеспечения режима безопасности защищаемых помещений достигается путем:

оснащения защищаемых помещений входными дверьми с замками, обеспечения постоянного закрытия дверей защищаемых помещений на замок и их открытия только для санкционированного прохода, а также опечатывания защищаемых помещений по окончании рабочего дня или оборудование защищаемых помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии защищаемых помещений;

утверждения правил доступа в защищаемые помещения в рабочее и нерабочее время, а также в нештатных ситуациях;

утверждения перечня лиц, имеющих право доступа в защищаемые помещения.

В целях организации режима обеспечения безопасности помещений рекомендуется разработать и утвердить соответствующий документ, определяющий меры по обеспечению безопасности защищаемых помещений.

* + 1. В целях обеспечения сохранности носителей персональных данных и иной защищаемой информации необходимо:

осуществлять хранение съемных машинных носителей, содержащих защищаемую информацию, в сейфах (металлических шкафах), оборудованных внутренними замками с двумя или более дубликатами ключей и приспособлениями для опечатывания замочных скважин или кодовыми замками. В случае если на съемном машинном носителе хранятся только персональные данные в зашифрованном с использованием СКЗИ виде, допускается хранение таких носителей вне сейфов (металлических шкафов);

осуществлять поэкземплярный учет машинных носителей, содержащих защищаемую информацию, который достигается путем ведения соответствующего журнала учета носителей с использованием регистрационных (заводских) номеров.

Рекомендуется разработать и утвердить документ, определяющий порядок использования носителей защищаемой информации и меры по обеспечению их сохранности.

* + 1. В целях принятия мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, необходимо разработать, утвердить и поддерживать в актуальном состоянии документы, определяющие:

ответственного за организацию обработки персональных данных;

регламент (инструкцию) ответственного за организацию обработки персональных данных;

политику в отношении обработки персональных данных;

формы документов, необходимых в целях выполнения требований законодательства Российской Федерации в области обработки персональных данных;

перечень лиц, доступ которых к персональным данным и иной защищаемой информации, обрабатываемой в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей.

* + 1. В целях принятия мер, направленных на обеспечение защиты информации и безопасности персональных данных при их обработке в информационных системах, необходимо разработать, утвердить и поддерживать в актуальном состоянии документы, определяющие:

ответственного за обеспечение безопасности защищаемой информации при её обработке в информационных системах;

регламент (инструкцию) ответственного за обеспечение безопасности защищаемой информации при её обработке в информационных системах;

перечень мер, направленных на выполнение требований законодательства Российской Федерации в области защиты персональных данных с использованием средств криптографической защиты

Технические мероприятия по обеспечению защиты информации должны включать:

установку и настройку средства антивирусной защиты;

установку и настройку СКЗИ и средств электронной подписи;

получение и установку ключей электронной подписи и сертификатов ключей проверки электронной подписи, используемых для обеспечения защищенного информационного взаимодействия АРМ оператора ЕЦИС с ЕЦИС.

В целях предотвращения несанкционированного доступа к информации рекомендуется установить и настроить одно из средств защиты информации от несанкционированного доступа, приведенное в пункте 2.3. приложения № 1 к настоящему Регламенту.

1. Требования к автоматизированным рабочим местам оператора ЕЦИС

На АРМ оператора ЕЦИС, предназначенного для обеспечения защищенного информационного взаимодействия с ЕЦИС, должны быть установлены и настроены сертифицированные на соответствие требованиям по безопасности информации средства антивирусной защиты и СКЗИ.

В целях выполнения пункта 10 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11 февраля 2013 года № 17, и пункта 8 Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом ФСТЭК России от 18 февраля 2013 года № 21, на АРМ оператора ЕЦИС рекомендуется установить и настроить средство защиты информации от несанкционированного доступа, удовлетворяющее требованиям, установленными для 3 класса защищенности государственных информационных систем и требованиями, установленными для 4 уровня защищенности персональных данных.

В случае, если АРМ оператора ЕЦИС имеет непосредственное подключение к сети Интернет или имеет подключение к информационно-телекоммуникационной сети, оператор которой не обеспечивают фильтрацию и блокирование неразрешенного сетевого трафика между АРМ оператора ЕЦИС и сетью Интернет, оператором ЕЦИС должны быть приняты меры по фильтрации и блокированию сетевого трафика с использованием сертифицированных средств межсетевого экранирования, которые обеспечивают фильтрацию и блокирование неразрешенного сетевого трафика между внешней информационно-телекоммуникационной сетью и АРМ оператора ЕЦИС или информационно-телекоммуникационной сетью оператора ЕЦИС, при этом рекомендуется на АРМ оператора ЕЦИС установить и настроить средство защиты информации, имеющее сертификат соответствия по профилю защиты межсетевых экранов типа «В» не ниже 6 класса защиты, либо на логической границе (периметре) информационно-телекоммуникационной сети оператора ЕЦИС установить и настроить межсетевой экран, имеющий сертификат соответствия по профилю защиты межсетевых экранов типа «А» или «Б» не ниже 5 класса защиты в соответствии с Требованиями к межсетевым экранам, утвержденными приказом ФСТЭК России от 09 февраля 2016 года № 9.

СКЗИ, используемые для обеспечения защищенного информационного взаимодействия с ЕЦИС, должны соответствовать требованиям ФСБ России к шифровальным (криптографическим) средствам класса КС2.

При 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, и для 4 уровня защищенности персональных данных в соответствии Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом ФСТЭК России от 18 февраля 2013 года № 21, Составом и содержанием 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, утвержденных приказом ФСБ России от 10 июля 2014 года № 378, а также мероприятий в соответствии с требованиями настоящего Регламента, допускается использование СКЗИ класса КС1.

Реализация антивирусной защиты на АРМ оператора ЕЦИС должна предусматривать:

применение средства антивирусной защиты;

установку, конфигурирование и управление средством антивирусной защиты;

проведение периодических проверок на наличие вредоносных компьютерных программ;

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 об обнаружении вредоносных компьютерных программ;

определение и выполнение действий по реагированию на обнаружение объектов, подвергшихся заражению вредоносными компьютерными программами;

регулярное, не реже 1 раза в день, обновление антивирусных баз;

обновление средства антивирусной защиты по мере выпуска производителем новых сертифицированных версий средств антивирусной защиты;

периодическую проверку работоспособности средств антивирусной защиты.

Перечень рекомендуемых средств защиты информации и СКЗИ приведен в приложении № 1 к настоящему Регламенту.

1. Порядок подключения к ЕЦИС

Установка и настройка программного обеспечения, средств защиты информации и СКЗИ осуществляется операторами ЕЦИС в соответствии с эксплуатационной документацией на используемые средства защиты информации и СКЗИ.

Используемые для организации защищенного информационного взаимодействия с ЕЦИС ключи электронной подписи и сертификаты ключей проверки электронной подписи должны соответствовать требованиям Федерального закона «Об электронной подписи» и стандарту ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».

Изготовление и выдача квалифицированного сертификата ключей проверки электронной подписи (далее – квалифицированный сертификат) осуществляется в соответствии с Порядком реализации функций аккредитованного удостоверяющего центра БУ «Центр информационных технологий» Мининформполитики Чувашии и исполнения его обязанностей, который размещен в информационно-телекоммуникационной сети Интернет по адресу <http://uc-cit.cap.ru>.

Изготовление сертификата ключа проверки электронной подписи, который не являются квалифицированным сертификатом и может использоваться только для организации защищенного информационного взаимодействия с ЕЦИС, осуществляется техническим оператором инфраструктуры ЕЦИС в течение пяти рабочих дней со дня предоставления оператором ЕЦИС заявки на изготовление сертификата ключа проверки электронной подписи по форме согласно Приложению № 5 к настоящему Регламенту.

Проверка возможности подключения к ЕЦИС осуществляется путем открытия веб-ресурса по адресу <https://cb.cap.ru> с использованием веб-браузера или специализированного прикладного программного обеспечения, установленного на АРМ оператора ЕЦИС.

Доступ пользователя ЕЦИС для обработки информации в ЕЦИС, в том числе его регистрация в ЕЦИС в качестве пользователя ЕЦИС и назначение ему прав для работы в ЕЦИС, осуществляется техническим оператором инфраструктуры ЕЦИС на основании заявки оператора ЕЦИС на предоставление доступа пользователю к ЕЦИС по форме согласно Приложению № 3 к настоящему Регламенту.

Доступ должностного лица оператора ЕЦИС для обработки информации в ЕЦИС осуществляется только после выполнения оператором ЕЦИС организационных и технических мероприятий в соответствии с требованиями настоящего Регламента.

Выполнение вышеуказанных мероприятий подтверждается соответствующим актом о готовности оператора ЕЦИС, который оформляется по форме согласно Приложению № 2 к настоящему Регламенту и предоставляется техническому оператору инфраструктуры ЕЦИС.

Прекращение доступа пользователя ЕЦИС к ЕЦИС осуществляется на основании заявки на прекращение доступа пользователя к ЕЦИС по форме согласно Приложению № 4 к настоящему Регламенту.

Заявка, указанная в пункте 4.4 настоящего Положения, представляется техническому оператору инфраструктуры ЕЦИС в течение десяти рабочих дней со дня принятия оператором ЕЦИС решения о прекращении доступа пользователя ЕЦИС к ЕЦИС.

В случае принятия оператором ЕЦИС решения о прекращении доступа пользователя ЕЦИС к ЕЦИС оператор ЕЦИС не позднее трех рабочих дней со дня принятия данного решения представляет техническому оператору инфраструктуры ЕЦИС заявку на прекращение действия (отзыв) сертификата ключа проверки электронной подписи, используемого для организации защищенного информационного взаимодействия с ЕЦИС, по форме согласно Приложению № 6 к настоящему Регламенту.

В случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи, в том числе при утере или хищении носителя ключа электронной подписи, соответствующего сертификату ключа проверки электронной подписи, используемого для организации защищенного информационного взаимодействия с ЕЦИС, оператор ЕЦИС обязан немедленно уведомить технического оператора инфраструктуры ЕЦИС и в течение одного рабочего дня предоставить заявку на прекращение действия (отзыв) сертификата ключа проверки электронной подписи по форме согласно Приложению № 6 к настоящему Регламенту.

Предоставление (прекращение) доступа пользователя ЕЦИС к ЕЦИС осуществляется техническим оператором инфраструктуры ЕЦИС в течение трех рабочих дней со дня получения заявок, указанных в пунктах 4.4, 4.5 настоящего Регламента.

Прекращение действия (отзыв) сертификата ключа проверки электронной подписи осуществляется техническим оператором инфраструктуры ЕЦИС в течение одного рабочего дня со дня получения заявок, указанных в пунктах 4.6, 4.7 настоящего Регламента. Уведомление о прекращении действия (отзыве) сертификата ключа проверки электронной подписи осуществляется посредством публикации списка отозванных сертификатов. Адреса точек распространения списка отозванных сертификатов указываются в сертификате ключа проверки электронной подписи.

Приложение № 1
к Регламенту подключения к единой централизованной информационной системе бюджетного (бухгалтерского) учета и отчетности

Перечень рекомендуемых сертифицированных средств защиты информации и средств криптографической защиты информации

Технические меры защиты информации должны реализовываться посредством применения средств защиты информации, в том числе программных (программно-аппаратных) средств, в которых они реализованы, имеющих необходимые функции безопасности.

В с соответствии с требованиями к составу и содержанию организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденными приказом Федеральной службой по техническому и экспортному контролю (далее – ФСТЭК России) от 18.02.2013 № 21, для обеспечения 4 уровня защищенности персональных данных должны применяться средства защиты информации не ниже 6 класса, а также средства вычислительной техники не ниже 6 класса.

1. Перечень рекомендуемых средств защиты информации и средств криптографической защиты информации, совместимых с операционными системами Microsoft Windows.
	1. Средства криптографической защиты информации (далее – СКЗИ) и средства электронной подписи:

СКЗИ «КриптоПро CSP» версии 4.0 или выше, либо СКЗИ «ViPNet CSP 4.2» (варианты исполнения 1, 2, 3), либо ViPNet PKI Client (варианты исполнения 1, 2, 3);

СКЗИ «Континент TLS VPN Клиент» (при необходимости).

СКЗИ «Континент TLS VPN Клиент» рекомендуется устанавливать для организации защищенного информационного взаимодействия с единой централизованной информационной системе бюджетного (бухгалтерского) учета и отчетности (далее – ЕЦИС) в случаях:

применения на АРМ оператора ЕЦИС специализированного прикладного программного обеспечения для работы в ЕЦИС;

применения СКЗИ «Континент TLS VPN Клиент» без стороннего криптопровайдера (СКЗИ «КриптоПро CSP» версии 4.0). В данном варианте СКЗИ «Континент TLS VPN Клиент» используется с криптопровайдером «Код Безопасности CSP», входящим в состав СКЗИ «Континент TLS VPN Клиент».

* 1. Средства антивирусной защиты информации:
1. программное изделие «Kaspersky Endpoint Security 10 для Windows» или «Kaspersky Endpoint Security 11 для Windows»;
2. программное обеспечение «Dr.Web Enterprise Security Suite».
	1. Средства защиты информации от несанкционированного доступа:
3. средство защиты информации Secret Net Studio 8;
4. система защиты информации от несанкционированного доступа «Dallas Lock 8.0-К».
5. Перечень рекомендуемых средств защиты информации и средств криптографической защиты информации, совместимых с операционными системами Linux.
	1. СКЗИ и средства электронной подписи: СКЗИ «КриптоПро CSP» версии 4.0 или выше, либо СКЗИ «ViPNet CSP 4.2» (варианты исполнения 4, 5), либо ViPNet PKI Client (вариант исполнения 6).
	2. Средства антивирусной защиты информации:
6. программное изделие «Kaspersky Endpoint Security 10 для Linux»;
7. программное обеспечение «Dr.Web Enterprise Security Suite».
	1. Средства защиты информации от несанкционированного доступа:
8. средство защиты информации «Secret Net LSP»;
9. система защиты информации от несанкционированного доступа «Dallas Lock Linux».

В случае отсутствия технической возможности применения на АРМ оператора ЕЦИС сертифицированных средств защиты информации от несанкционированного доступа, рекомендуется использовать операционные системы, соответствующие требованиям к профилю защиты операционных систем типа «А» не ниже 5 класса защиты в соответствии с методическими документами, утвержденными Федеральной службой по техническому и экспортному контролю.

Приложение № 2
к Регламенту подключения к единой централизованной информационной системе бюджетного (бухгалтерского) учета и отчетности

УТВЕРЖДАЮ

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ г. *Руководитель \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

 Акт № \_\_\_\_\_
о готовности подключения к единой централизованной информационной системе бюджетного (бухгалтерского) учета и отчетности

Комиссия \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(наименование организации)

в составе:

|  |  |  |
| --- | --- | --- |
| Председатель комиссии:  | - |  |
| Члены комиссии:  | - |  |
|  |  |  |
|  |  |  |

составила настоящий акт о том, что проведена проверка выполнения требований в соответствии с Регламентом подключения к единой централизованной информационной системе бюджетного (бухгалтерского) учета и отчетности, утвержденным приказом АУ «ЦИТ» Минцифры Чувашии от \_\_\_\_\_\_\_\_\_\_ № \_\_\_\_\_\_ (далее – Регламент), в том числе проверка:

1. Наличия разработанных и принятых организационных документов по вопросам информационной безопасности и обеспечения защиты персональных данных в соответствии с федеральными законами «Об информации, информационных технологиях и о защите информации», «О персональных данных» и принимаемыми в соответствии с ними нормативными правовыми актами, методическими и руководящими документами в области защиты информации.
2. Организации режима обеспечения безопасности помещений, в которых размещены автоматизированные рабочие места, предназначенные для обеспечения информационного взаимодействия с единой централизованной информационной системой бюджетного (бухгалтерского) учета и отчетности (далее соответственно – АРМ оператора ЕЦИС, ЕЦИС), технические и программные средства, участвующие в обработке информации при взаимодействии с ЕЦИС, а также помещений, где используются или хранятся средства защиты информации, средства криптографической защиты информации, носители защищаемой информации, персональных данных, ключевой, аутентифицирующей и парольной информации.
3. Подготовленности лиц, ответственных за обеспечение информационного взаимодействия с ЕЦИС, знания ими основных положений законодательства в области защиты информации и обеспечения безопасности персональных данных, требований 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, утвержденной приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 года № 152.
4. Готовности АРМ оператора ЕЦИС, технических и программных средств, участвующих в обработке информации при взаимодействии с ЕЦИС, а также проверка настроек и корректности функционирования следующих средств защиты информации и средств криптографической защиты информации, установленных на АРМ оператора ЕЦИС:

средства криптографической защиты информации:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;

наименование СКЗИ (например, СКЗИ «КриптоПро CSP» версии 4.0, СКЗИ «Континент TLS VPN Клиент» версии 2)

средства антивирусной защиты информации:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;

наименование средства антивирусной защиты (например, Kaspersky Endpoint Security 11 для Windows)

средства защиты информации от несанкционированного доступа:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;

наименование средства защиты информации (например, Secret Net Studio)

**Заключение комиссии:**

принятые организационные и технические меры по обеспечению информационной безопасности \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(наименование организации)

соответствуют требованиям Регламента, автоматизированные рабочие места для подключения и обработки информации в единой централизованной информационной системе бюджетного (бухгалтерского) учета и отчетности готовы.

Представители комиссии:

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (подпись члена комиссии) (Ф.И.О. члена комиссии)

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (подпись члена комиссии) (Ф.И.О. члена комиссии)

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (подпись члена комиссии) (Ф.И.О. члена комиссии)

Приложение № 3
к Регламенту подключения к единой централизованной информационной системе бюджетного (бухгалтерского) учета и отчетности

|  |  |
| --- | --- |
| *На бланке оператора единой централизованной информационной системы бюджетного (бухгалтерского) учета и отчетности* | В автономное учреждение Чувашской Республики «Центр информационных технологий» Министерства цифрового развития, информационной политики и массовых коммуникаций Чувашской Республики |

**ЗАЯВКА**

**на предоставление доступа к единой централизованной информационной системе бюджетного (бухгалтерского) учета и отчетности**

|  |  |
| --- | --- |
| Фамилия, имя, отчество (последнее – при наличии) пользователя |  |
| Наименование государственного (муниципального) учреждения |  |
| Адрес |  |
| Должность |  |
| № кабинета |  |
| Контактный телефон |  |
| Основание для предоставления доступа |  |
| Дата предоставления доступа |  |
| Наименование интерфейса (рабочего места) |  |
| Назначенные права |  |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| «\_\_\_» \_\_\_\_\_\_\_ 20\_\_ года  | / | / |
|  | (подпись) | (расшифровка) |

Приложение № 4
к Регламенту подключения к единой централизованной информационной системе бюджетного (бухгалтерского) учета и отчетности

|  |  |
| --- | --- |
| *На бланке оператора единой централизованной информационной системы бюджетного (бухгалтерского) учета и отчетности* | В автономное учреждение Чувашской Республики «Центр информационных технологий» Министерства цифрового развития, информационной политики и массовых коммуникаций Чувашской Республики |

**ЗАЯВКА**

**на прекращение доступа к единой централизованной информационной системе бюджетного (бухгалтерского) учета и отчетности**

|  |  |
| --- | --- |
| Фамилия, имя, отчество (последнее – при наличии) пользователя |  |
| Наименование государственного (муниципального) учреждения |  |
| Должность |  |
| Основания для прекращения доступа |  |
| Дата отключения |  |

|  |  |  |
| --- | --- | --- |
| «\_\_\_» \_\_\_\_\_\_\_ 20\_\_ года  | / | / |
|  | (подпись) | (расшифровка) |

Приложение № 5
к Регламенту подключения к единой централизованной информационной системе бюджетного (бухгалтерского) учета и отчетности

|  |  |
| --- | --- |
| *На бланке оператора единой централизованной информационной системы бюджетного (бухгалтерского) учета и отчетности* | АУ «ЦИТ» Минцифры Чувашии  |

**ЗАЯВКА**

**на изготовление сертификата ключа проверки электронной подписи**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(наименование организации)

в целях организации защищенного информационного взаимодействия при подключении к единой централизованной информационной системе бюджетного (бухгалтерского) учета и отчетности просит изготовить сертификат ключа проверки электронной подписи, содержащий следующие данные[[1]](#footnote-1):

|  |  |
| --- | --- |
| Наименование организации (сокращенное) |  |
| Наименование населенного пункта |  |
| Название улицы, номер дома |  |
| Область | 21 Чувашская Республика – Чувашия |
| Страна | RU |
| ИНН организации |  |
| ОГРН организации  |  |
| Фамилия |  |
| Имя Отчество |  |
| Должность |  |
| Подразделение организации |  |
| СНИЛС |  |
| Адрес электронной почты |  |
| Используемое средство электронной подписи (установленное на АРМ) | □ СКЗИ «КриптоПро CSP»;□ СКЗИ «ViPNet CSP»□ СКЗИ «Континент TLS VPN Клиент» |

Приложение: запрос на изготовление сертификата в электронном виде[[2]](#footnote-2).

|  |  |
| --- | --- |
|  |  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (должность руководителя) | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / \_\_\_\_\_\_\_\_\_\_\_\_\_ / (подпись) (расшифровка) |
|  |  |

Приложение № 6
к Регламенту подключения к единой централизованной информационной системе бюджетного (бухгалтерского) учета и отчетности

|  |  |
| --- | --- |
| *На бланке оператора единой централизованной информационной системы бюджетного (бухгалтерского) учета и отчетности* | АУ «ЦИТ» Минцифры Чувашии  |

**ЗАЯВКА**

**на прекращение действия (отзыв) сертификата ключа проверки электронной подписи**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(наименование организации)

в связи с \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(причина прекращения действия сертификата)

просит прекратить действие сертификата ключа проверки электронной подписи, используемого для организации защищенного информационного взаимодействия с единой централизованной информационной системой бюджетного (бухгалтерского) учета и отчетности, содержащего следующие данные[[3]](#footnote-3):

|  |  |
| --- | --- |
| Серийный номер сертификата |  |
| ОГРН организации  |  |
| Фамилия |  |
| Имя Отчество |  |
| СНИЛС |  |

|  |  |
| --- | --- |
|  |  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (должность руководителя) | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / \_\_\_\_\_\_\_\_\_\_\_\_\_ / (подпись) (расшифровка) |

1. В издаваемый неквалифицированный сертификат, исходя из технических возможностей программного обеспечения и (или) СКЗИ, используемого для формирования запроса на изготовление сертификата, будут включены только данные, присутствующие в запросе на изготовление сертификата. [↑](#footnote-ref-1)
2. Указывается только в случае, если запрос на изготовление сертификата формируется на АРМ пользователя ЕЦИС. [↑](#footnote-ref-2)
3. Серийный номер сертификата указывается в обязательном порядке, иные данные указываются, если они присутствуют в сертификате. [↑](#footnote-ref-3)