МИНИСТЕРСТВО ЮСТИЦИИ РЕСПУБЛИКИ ТЫВА
ЗАРЕГИСТРИРОВАНО
Регистрационный № 905
от «23» октября 2023 г.

МИНИСТЕРСТВО ФИНАНСОВ РЕСПУБЛИКИ ТЫВА
ТЫВА РЕСПУБЛИ КАНЫҢ САҢ-ХӨӨ ЯАМЫЗЫ

ПРИКАЗ

от «26» октября 2023 г. № 116 о/д

г. Кызыл

Об утверждении Регламента защищенного подключения внешних пользователей к государственной информационной системе «Единая централизованная информационная система бюджетного (бухгалтерского) учета и отчетности Республики Тыва»

В соответствии с Федеральными законами от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и от 27.07.2006 № 152-ФЗ «О персональных данных», Закона Республики Тыва от 17 января 2013 года №1768 ВХ-1 «О государственных информационных системах Республики Тыва», Приказом Министерства финансов Республики Тыва от 05.05.2023 № 56о/д «О создании государственной информационной системы «Единая централизованная информационная система бюджетного (бухгалтерского) учета и отчетности Республики Тыва»,

ПРИКАЗЫВАЮ:

1. Утвердить Регламент защищенного подключения внешних пользователей к государственной информационной системе «Единая централизованная информационная система бюджетного (бухгалтерского) учета и отчетности Республики Тыва» (Далее – Регламент).
2. Государственному казенному учреждению Межотраслевая централизованная бухгалтерия Республики Тыва (Саая А.С.) довести настоящий Регламент до обслуживаемых учреждений и обеспечить его исполнение.
3. Контроль за исполнением настоящего приказа возложить на первого заместителя министра финансов Республики Тыва Зенченко А.В.

Министр О.С. Достай

УТВЕРЖДЕНО
Приказом
Министерства финансов
Республики Тыва
От «20» октября 2023 г.

№ 116 с/д

РЕГЛАМЕНТ
ЗАЩИЩЕННОГО ПОДКЛЮЧЕНИЯ ВНЕШНИХ ПОЛЬЗОВАТЕЛЕЙ К ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ «ЕДИНАЯ ЦЕНТРАЛИЗОВАННАЯ ИНФОРМАЦИОННАЯ СИСТЕМА БЮДЖЕТНОГО (БУХГАЛТЕРСКОГО) УЧЕТА И ОТЧЕТНОСТИ РЕСПУБЛИКИ ТЫВА»

Кызыл– 2023

Принятые сокращения и определения

АРМ	-	автоматизированное рабочее место
Пользователи	-	работники органов государственной власти, государственных органов и государственных учреждений Республики Тыва
Владелец ЕЦИС	-	Министерство финансов Республики Тыва
ЕЦИС	-	Государственная информационная система «Единая централизованная информационная система бухгалтерского учета и отчетности Республики Тыва»
КЗ	-	контролируемая зона
МЭ	-	межсетевой экран
НСД	-	несанкционированный доступ
ОС	-	операционная система
Оператор ЕЦИС	-	Государственное казенное учреждение «Межотраслевая централизованная бухгалтерия Республики Тыва»
ПАК	-	программно-аппаратный комплекс
ПО	-	программное обеспечение
ПОИБ ИС	-	подсистема обеспечения информационной безопасности ЕЦИС
САВЗ	-	средство антивирусной защиты
САНЗ	-	средство анализа защищенности
СВТ	-	средства вычислительной техники
СЗИ	-	средство защиты информации
СКЗИ	-	средства криптографической защиты информации
СОВ	-	средство обнаружения вторжений
СФ	-	среда функционирования СКЗИ
Учреждения	-	органы государственной власти, государственные органы, государственные и муниципальные учреждения Республики Тыва
ГКУ «МЦБ РТ»	-	Государственное казенное учреждение «Межотраслевая централизованная бухгалтерия Республики Тыва»

Нормативно-правовые ссылки

Настоящий регламент защищенного подключения внешних пользователей к государственной информационной системе «Единая централизованная информационная система бюджетного (бухгалтерского) учета и отчетности Республики Тыва» (далее – Регламент) разработан в соответствии со следующими нормативно-правовыми актами Российской Федерации (далее – НПА):

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

[2] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

[3] Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

[4] Приказ ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

[5] Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

[6] Приказ ФСБ России 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»;

Введение

Настоящий Регламент разработан в соответствии с НПА [1]-[6] и регламентирует порядок технологического подключения пользователей к государственной информационной системе «Единая централизованная информационная система бюджетного (бухгалтерского) учета и отчетности Республики Тыва», а также определяет обязательные технические и организационные требования по обеспечению информационной безопасности при подключении.

Порядок подключения пользователей к ЕЦИС

Подсистема обеспечения информационной безопасности серверов в части обеспечения криптографической защиты информации реализована на основе сертифицированных программно-аппаратных комплексов ViPNet.

На основе решений на базе ПАК ViPNet организована защищенная виртуальная сеть. Номер защищенной сети ViPNet – 20510.

Государственная информационная система «Единая централизованная информационная система бухгалтерского учета и отчетности Республики Тыва» министерства финансов Республики Тыва аттестована на соответствие требованиям безопасности информации по 3-му классу защищенности ГИС и 3-му уровню защищенности ПДн. Для подключения пользователей к ЕЦИС информационная система (часть системы) Учреждения должна пройти аттестационные испытания и получить аттестат соответствия требованиям по защите информации.

Порядок действия Учреждения:

1. Выбрать вариант подключения к ЕЦИС, которые представлены в Приложении № 1.
2. Направить с сопроводительным письмом в адрес Министерства финансов Республики Тыва (далее – Министерство) – Владельца ЕЦИС Уведомление о намерении подключения к ЕЦИС (далее – Уведомление) по форме Приложения №2 к настоящему Регламенту, продублировав Уведомление на адрес электронной почты Государственного казенного учреждения «Межотраслевая централизованная бухгалтерия Республики Тыва» (далее – ГКУ «МЦБ РТ») – Оператора ЕЦИС: info@mcbrt.ru.
3. Обеспечить защиту информации, обрабатываемой на АРМ, подключаемых к ЕЦИС. Для обеспечения защиты информации должны использоваться АРМ, оснащенные СЗИ и СКЗИ, прошедшими процедуру оценки соответствия требованием безопасности информации. В Приложении № 3 к настоящему Регламенту приведен Перечень рекомендуемых средств защиты информации.
4. Разработать либо актуализировать организационно-распорядительную и техническую документацию:

– приказ о сотрудниках, осуществляющих обработку защищаемой информации в ЕЦИС (Приложение № 4);

– приказ об обеспечении безопасности помещений, в которых имеется доступ к ЕЦИС (Приложение № 5);

– приказ об утверждении перечня мер, направленных на выполнение требований законодательства Российской Федерации в области защиты информации

с использованием средств криптографической защиты (Приложение № 6).

5. Выполнить организационные и технические меры по защите информации:

– установить пароль администратора на доступ к базовой системе ввода-вывода (BIOS/UEFI). Организовать контроль доступа пользователей к процессу загрузки операционной системы посредством запрета альтернативной загрузки операционной системы (в том числе – с внешних носителей), отключить возможность выбора источников во время загрузки в настройках базовой системы ввода-вывода (BIOS/UEFI);

– провести, при необходимости, дополнительные мероприятия по технической укрепленности помещений, в которых планируется эксплуатация АРМ с СКЗИ (средства охраны (охранной сигнализации), прочные входные двери с надежными замками, устройства для опечатывания помещений по окончании рабочего дня, другие средства, препятствующие неконтролируемому проникновению).

– обеспечить помещение ответственного пользователя криптосредств сейфом (металлическим шкафом).

6. Учреждение привлекает организацию, имеющую право на данный вид работ, в соответствии с Федеральным законом от 04.05.2011 №99-ФЗ «О лицензировании отдельных видов деятельности», для проведения аттестационных испытаний по требованиям безопасности информации для подтверждения обеспечения безопасности информации по необходимому классу защиты. По результатам успешных испытаний Учреждению выдается Аттестат соответствия требованиям по защите информации.

7. По результатам выполнения пунктов 3-6 настоящего Регламента составить Акт готовности к обработке и защите информации, не содержащей сведения, составляющие государственную тайну, в ЕЦИС и направить на адрес электронной почты: info@mcbrt.ru (Приложение № 7).

Приложение № 1
к регламенту

Варианты подключения к государственной информационной системе «Единая централизованная информационная система бухгалтерского учета и отчетности Республики Тыва»

Реализация защищенного подключения к ЕЦИС реализуется двумя схемами подключения:

Вариант №1.

Реализация межсетевого взаимодействия с помощью СКЗИ Учреждения и СКЗИ министерства финансов Республики Тыва (ViPNet-сеть № 20510 Минфина Республики Тыва).

Для реализации подключения к сети № 20510 Минфина Республики Тыва по Варианту № 1 Учреждению необходимо оформить договор (соглашение) о межсетевом взаимодействии с Министерством финансов Республики Тыва, а также иметь сертифицированное ФСТЭК России и ФСБ России СКЗИ ViPNet Client (версия от 4.5.3.65117) или ПАК ViPNet Coordinator HW, установленное силами одного из лицензиатов ФСБ, реестр которых представлен на сайте Центра по лицензированию, сертификации и защите государственной тайны ФСБ России (http://clsz.fsb.ru/clsz/license.htm). Также необходимо приобрести и установить сертифицированные ФСТЭК России СЗИ от НСД, МЭ, САВЗ, САНЗ, СОВ для АРМ, подключаемых к ЕЦИС.

Вариант №2.

Подключение к ЕЦИС путем приобретения клиентского ПО ViPNet Client или ПАК ViPNet Coordinator HW за счет Учреждения в защищенную сеть ViPNet № 20510 Минфина Республики Тыва.

Для реализации подключения по Варианту № 2 Учреждению необходимо приобрести клиентское ПО ViPNet Client (версия от 4.5.3.65117) или ПАК ViPNet Coordinator HW и установить силами одного из лицензиатов ФСБ, реестр которых представлен на сайте Центра по лицензированию, сертификации и защите государственной тайны ФСБ России (http://clsz.fsb.ru/clsz/license.htm), а также приобрести и установить сертифицированные ФСТЭК России СЗИ от НСД, МЭ, СОВ, САВЗ, САНЗ для АРМ, подключаемых к ЕЦИС.

Получить ключевую информацию (DST-файлы) в ГКУ «МЦБ РТ» доверенными способами.

Требования к безопасности информации на АРМ, подключаемых к ЕЦИС, Учреждений обеспечиваются независимо от схемы подключения.

Приложение №2
к Регламенту

Уведомление о намерении подключения к ЕЦИС

_____

(наименование государственного органа/органа государственной власти/ государственного учреждения

уведомляет о намерении подключиться к государственной информационной системе «Единая централизованная информационная система бухгалтерского учета и отчетности Республики Тыва». Необходимое количество автоматизированных рабочих мест (АРМ) пользователей - __.

Перечень АРМ, планируемых к подключению, приведен в таблице.

№ п/п	Фамилия, имя, отчество пользователя	Наименование структурного подразделения пользователя	Должность пользователя	Служебный телефон	Электронная почта пользователя	Подсистема ЕЦИС (БГУ, ЗКГУ)	Месторасположение АРМ (адрес, № кабинета)

Руководитель органа государственной власти/

государственного органа/государственного учреждения

Приложение №3
к Регламенту

Перечень рекомендуемых средств защиты информации

1. Средства антивирусной защиты для ОС Windows:

– сертифицированное ФСТЭК России по требованиям безопасности информации средство антивирусной защиты Kaspersky Endpoint Security для Windows;

– сертифицированное ФСТЭК России по требованиям безопасности информации средство антивирусной защиты Dr.Web Enterprice Security Suite.

2. Средства антивирусной защиты для ОС семейства Linux:

– сертифицированное ФСТЭК России по требованиям безопасности информации средство антивирусной защиты Kaspersky Endpoint Security для Linux;

– сертифицированное ФСТЭК России по требованиям безопасности информации средство антивирусной защиты Dr.Web Enterprice Security Suite.

3. Средства защиты информации от несанкционированного доступа для ОС Windows:

– сертифицированное ФСТЭК России по требованиям безопасности информации средство защиты от НСД Secret Net Studio 8;

– сертифицированное ФСТЭК России по требованиям безопасности информации средство защиты от НСД Dallas Lock 8.0-K.

4. Средства защиты информации от несанкционированного доступа для ОС семейства Linux:

– сертифицированное ФСТЭК России по требованиям безопасности информации средство защиты от НСД Secret Net LSP;

– сертифицированное ФСТЭК России по требованиям безопасности информации средство защиты от НСД Dallas Lock Linux;

– встроенные функции СЗИ от НСД в случае работы с ОС специального назначения Astra Linux Special Edition.

5. Сертифицированные средства межсетевого экранирования для ОС Windows:

– сертифицированное ФСТЭК России средство межсетевого экранирования – ViPNet Client 4 класса КС1 и выше, выполняющее функции средства криптографической защиты информации (сертифицированного ФСБ России);

– сертифицированное ФСТЭК России средство межсетевого экранирования ViPNet Coordinator HW, выполняющее функции средства криптографической защиты информации (сертифицированного ФСБ России).

6. Сертифицированные средства межсетевого экранирования для ОС семейства Linux:

– сертифицированное ФСТЭК России по требованиям безопасности информации средство защиты от НСД Secret Net LSP;

– сертифицированное ФСТЭК России по требованиям безопасности

информации средство защиты от НСД Dallas Lock Linux;

– сертифицированное ФСТЭК России средство межсетевого экранирования ViPNet Coordinator HW, выполняющее функции средства криптографической защиты информации (сертифицированного ФСБ России).

7. Сертифицированные средства обнаружения вторжений:

– сертифицированное ФСТЭК России по требованиям безопасности информации средство обнаружения вторжений ViPNet IDS HS.

8. Сертифицированные средства анализа уязвимостей:

– сертифицированное ФСТЭК России по требованиям безопасности информации средство анализа уязвимостей Сканер-ВС;

– сертифицированное ФСТЭК России по требованиям безопасности информации средство анализа уязвимостей XSpider.

Приложение №4
к Регламенту

П Р И К А З

№ _____ _____

О сотрудниках _____, осуществляющих обработку защищаемой информации, в государственной информационной системе «Единая централизованная информационная система бухгалтерского учета и отчетности Республики Тыва»

В целях выполнения требований Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», 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», ПРИКАЗЫВАЮ:

Утвердить перечень сотрудников _____, осуществляющих обработку защищаемой информации, не содержащей сведения, составляющие государственную тайну, и имеющих доступ к обрабатываемой защищаемой информации, не содержащей сведения, составляющие государственную тайну, содержащейся в государственной информационной системе «Единая централизованная информационная система бухгалтерского учета и отчетности Республики Тыва» (Приложение № 1).

Утвердить перечень сотрудников _____, осуществляющих обработку персональных данных и имеющих доступ к персональным данным, обрабатываемым в государственной информационной системе «Единая централизованная информационная система бухгалтерского учета и отчетности Республики Тыва» (Приложение № 2).

Утвердить инструкцию пользователя государственной информационной системы «Единая централизованная информационная система бухгалтерского учета и отчетности Республики Тыва» (Приложение № 3).

Контроль за исполнением настоящего приказа оставляю за собой.

_____ _____

Приложение № 1
к Приказу

Перечень сотрудников _____, осуществляющих обработку защищаемой информации, не содержащей сведения, составляющие государственную тайну, и имеющих доступ к обрабатываемой защищаемой информации, не содержащей сведения, составляющие государственную тайну, содержащейся в государственной информационной системе «Единая централизованная информационная система бухгалтерского учета и отчетности Республики Тыва»

№ п/п	ФИО сотрудника	Должность

Приложение № 2
к Приказу

Перечень сотрудников _____, осуществляющих обработку персональных данных и имеющих доступ к персональным данным, обрабатываемым в Государственной информационной системе «Единая централизованная информационная система бухгалтерского учета и отчетности Республики Тыва»

№ п/п	ФИО сотрудника	Должность
1.		

Приложение № 3
к Приказу

Инструкция пользователя государственной информационной системы «Единая централизованная информационная система бухгалтерского учета и отчетности Республики Тыва»

1. Общие положения

1.1. Пользователями Государственной информационной системы «Единая централизованная информационная система бухгалтерского учета и отчетности Республики Тыва» (далее – Пользователь) являются уполномоченные сотрудники Министерства финансов Республики Тыва (далее – Министерство), сотрудники органов государственной власти, государственных органов и государственных учреждений Республики Тыва (далее – Учреждения), сотрудники ГКУ «МЦБ РТ», отраслевых централизованных бухгалтерий (далее – ЦБУ (ЦБ).

1.2. Пользователь ЕЦИС должен знать нормы действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну (далее – защищаемая информация).

1.3. В своей деятельности, связанной с обработкой защищаемой информации, Пользователь руководствуется настоящей Инструкцией.

1.4. Пользователи, участвующие в рамках своих функциональных обязанностей в процессах автоматизированной обработки защищаемой информации и имеющие доступ к аппаратным средствам, программному обеспечению и обрабатываемой защищаемой информации, несут персональную ответственность за свои действия.

2. Обязанности и права пользователя информационной системы

2.1. Пользователь обязан:

– выполнять в ЕЦИС только те процедуры, которые необходимы для исполнения его должностных обязанностей;

– использовать для выполнения должностных обязанностей только предоставленное ему автоматизированное рабочее место (далее – АРМ) на базе персонального компьютера (автономной ПЭВМ);

– немедленно сообщать руководителю структурного подразделения _____ и (или) ответственному за защиту информации, не содержащей сведения, составляющие государственную тайну, в ЕЦИС Министерства (далее – Ответственный за защиту информации) о нештатных ситуациях, фактах и попытках несанкционированного доступа к обрабатываемой информации, о блокировании, исчезновении (искажении) защищаемой информации;

– убедиться в том, что во время работы экран монитора располагается таким образом, чтобы исключалась возможность ознакомления с отображаемой на нем информацией посторонними лицами;

– соблюдать установленный режим разграничения доступа к информационным ресурсам: получать пароль, надежно его запоминать и хранить в тайне.

2.2. Пользователям ЕЦИС запрещается:

– записывать и хранить защищаемую информацию, на неучтенных материальных носителях информации;

– оставлять во время работы материальные носители информации без присмотра, несанкционированно передавать материальные носители информации другим лицам и выносить их за пределы помещения, в котором производится обработка защищаемой информации;

– отключать (блокировать) средства защиты информации;

– производить какие-либо изменения в электрических схемах, монтаже и размещении технических средств;

– самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;

– обрабатывать в ЕЦИС информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к информационным ресурсам ЕЦИС;

– сообщать (или передавать) посторонним лицам личные атрибуты доступа к ресурсам в ЕЦИС;

– работать в ЕЦИС при обнаружении каких-либо неисправностей;

– хранить на учтенных носителях информации программы и данные, не относящиеся к рабочей информации;

– вводить в ЕЦИС защищаемую информацию под диктовку или с микрофона;

– привлекать посторонних лиц для производства ремонта технических средств ЕЦИС без согласования с Ответственным за защиту информации.

2.3. Пользователь имеет право знакомиться с внутренними документами, регламентирующими его обязанности по занимаемой должности.

3. Организация парольной защиты в информационной системе

3.1. Пароли доступа к ЕЦИС устанавливаются ответственным за управление (администрирование) системой защиты информации ЕЦИС Министерства (далее – Ответственный за управление (администрирование) или Пользователем.

3.2. При формировании пароля необходимо руководствоваться следующими требованиями:

– длина пароля должна быть не менее 8-и буквенно-цифровых символов;

– пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, дни рождения и другие памятные даты, номера телефонов, автомобилей, адреса места жительства, наименования АРМ, общепринятые сокращения) и другие данные, которые могут быть подобраны злоумышленником путем анализа информации;

– запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

– запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);

– при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;

– в числе символов пароля, обязательно должны присутствовать буквы в верхнем и нижнем регистрах, а также цифры;

– запрещается использовать ранее использованные пароли.

3.3. При организации парольной защиты запрещается:

– записывать свои пароли в очевидных местах, внутренностях ящика стола, на мониторе ПЭВМ, на обратной стороне клавиатуры и т.д.;

– хранить пароли в записанном виде на отдельных листах бумаги;

– сообщать свои пароли посторонним лицам, а также сведения о применяемых средствах защиты от НСД.

4. Порядок применения парольной защиты

4.1. Периодичность плановой смены пароля на доступ в ИС устанавливается Ответственным за управление (администрирование).

4.2. Пользователь обязан незамедлительно сообщить Ответственному за управление (администрирование) факты утраты, компрометации ключевой, парольной и аутентифицирующей информации.

4.3. Внеплановая смена личного пароля должна производиться в обязательном порядке в следующих случаях:

– компрометации (подозрении на компрометацию) пароля;

– в случае прекращения полномочий (увольнение, переход на другую работу внутри организации) Пользователя (в течение 24 часов после окончания последнего сеанса работы, данного с ЕЦИС);

– по инициативе Ответственного за управление (администрирование).

5. Технология обработки защищаемой информации

5.1. При первичном допуске к работе с ЕЦИС Пользователь:

– проходит инструктаж по использованию ЕЦИС;

– знакомится с требованиями нормативно-правовых, руководящих и организационно-распорядительных документов, регламентирующих обработку и обеспечение безопасности защищаемой информации;

– получает у Ответственного за управление (администрирование) идентификатор и личный пароль для входа в ЕЦИС.

5.2. Авторизацию в ЕЦИС (ввод личного идентификатора и пароля) Пользователь осуществляет при отсутствии в помещении посторонних лиц, не являющихся сотрудниками Министерства/ Учреждений/ ЦБУ (ЦБ) и не имеющих права доступа в помещения Министерства/ Учреждений/ ЦБУ (ЦБ).

5.3. Копирование защищаемой информации на электронные носители информации осуществляется только при наличии производственной необходимости и только на учтенные электронные носители информации.

5.4. Печать документов, содержащих защищаемую информацию, осуществляется только при наличии производственной необходимости. Распечатанные черновые бумажные варианты вновь создаваемых документов, содержащих защищаемую информацию, уничтожаются с применением уничтожителей бумаги незамедлительно после подписания (утверждения) окончательного варианта документа.

5.5. В случае возникновения необходимости временно покинуть рабочее помещение во время работы в ЕЦИС, Пользователь обязан выключить компьютер, либо заблокировать его. Разблокирование компьютера производится набором пароля разблокировки, который был создан при настройке системы блокировки АРМ. При отсутствии в покидаемом помещении других сотрудников Министерства/ Учреждений/ ЦБУ (ЦБ), Пользователь обязан закрыть дверь помещения на ключ или другой используемый ограничитель доступа.

5.6. Покидая рабочее помещение в конце рабочего дня, Пользователь обязан выключить все необходимые средства вычислительной техники и закрыть дверь помещения на ключ.

ЛИСТ ОЗНАКОМЛЕНИЯ

с Инструкцией пользователя государственной информационной системы «Единая централизованная информационная система бухгалтерского учета и отчетности Республики Тыва»

№ п/п	Ф.И.О.	Должность	Дата	Подпись

Приложение №5
к Регламенту

П Р И К А З

№ _____ _____

Об обеспечении безопасности помещений_____, в которых размещена государственная информационная система «Единая централизованная информационная система бухгалтерского учета и отчетности Республики Тыва»

В целях выполнения требований 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», приказа Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» ПРИКАЗЫВАЮ:

Утвердить перечень помещений _____, в которых размещена Государственная информационная система «Единая централизованная информационная система бухгалтерского учета и отчетности Республики Тыва» (Приложение № 1).

Утвердить порядок доступа сотрудников _____ в помещения, в которых осуществляется обработка защищаемой информации, не содержащей сведения, составляющие государственную тайну, и размещена Государственная информационная система «Единая централизованная информационная система бухгалтерского учета и отчетности Республики Тыва» (Приложение № 2).

Контроль за исполнением настоящего приказа оставляю за собой.

_____ _____

Приложение №6
к Регламенту

П Р И К А З

№

_____ _____

Об утверждении перечня мер, направленных на выполнение требований законодательства Российской Федерации в области защиты информации с использованием средств криптографической защиты

В целях выполнения требований законодательства Российской Федерации в области защиты информации при ее передаче по открытым каналам связи с использованием средств криптографической защиты, приказа ФАПСИ от 13 июня 2001 г. № 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», приказа ФСБ России от 10 июля 2014 г. № 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» ПРИКАЗЫВАЮ:

Назначить _____
ответственным пользователем криптосредств _____.

1. Утвердить Инструкцию ответственного пользователя криптосредств _____ (Приложение № 1).

2. Утвердить Перечень сотрудников _____, допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, в Государственной информационной системе «Единая централизованная информационная система бухгалтерского учета и отчетности Республики Тыва» (Приложение № 2).

3. Утвердить Инструкцию пользователя криптосредств _____ (Приложение № 3).

4. Утвердить Перечень помещений, где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств (Приложение № 4).

5. Утвердить Перечень лиц, имеющих доступ в помещения, где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств (Приложение № 5).

6. Утвердить Порядок доступа в помещения, где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств (Приложение № 6).

7. Утвердить форму Журнала поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов (Приложение № 7).

8. Утвердить форму Лицевого счета пользователя криптосредств (Приложение № 8).

9. Утвердить форму Журнала учета и выдачи носителей с ключевой информацией (Приложение № 9).

10. Утвердить форму Журнала обучения пользователей правилам работы с криптосредствами (Приложение № 10).

Контроль за исполнением настоящего приказа оставляю за собой.

Приложение № 1
к Приказу

Инструкция ответственного пользователя криптосредств

_____

1. Общие положения

Настоящая Инструкция ответственного пользователя криптосредств _____ (далее – Инструкция) определяет основные обязанности и права ответственного пользователя криптосредств.

Ответственный пользователь криптосредств назначается приказом _____ (далее – _____) и отвечает за организацию, обеспечение функционирования и безопасности криптосредств, предназначенных для защиты информации, не содержащей сведения, составляющие государственную тайну (далее – защищаемая информация), государственной информационной системы «Единая централизованная информационная система бухгалтерского учета и отчетности Республики Тыва» (далее – ИС).

Ответственный пользователь криптосредств должен знать нормы действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности защищаемой информации, а также в области защиты информации при ее передаче по открытым каналам связи с использованием средств криптографической защиты.

В своей деятельности ответственный пользователь криптосредств руководствуется настоящей Инструкцией.

2. Обязанности

Ответственный пользователь криптосредств обязан:

Соблюдать требования нормативных актов _____, устанавливающих порядок работы с защищаемой информацией.

Осуществлять контроль за организацией, обеспечением функционирования и безопасности криптосредств, предназначенных для обеспечения безопасности защищаемой информации при ее обработке в ИС:

– контролировать соблюдение условий использования криптосредств, предусмотренных эксплуатационной и технической документацией к ним;

– обеспечивать надежное хранение эксплуатационной и технической документации к криптосредствам, ключевых документов, носителей информации ограниченного распространения;

– вносить предложения по режиму охраны помещений, в которых установлены криптосредства или хранятся ключевые документы к ним;

– вести Журнал поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов (далее – Журнал);

– выдавать пользователям криптосредств экземпляры криптосредств, эксплуатационной и технической документации к ним, ключевых документов под расписку в соответствующем Журнале;

– вести на каждого пользователя криптосредств Лицевой счет, в котором регистрировать числящиеся за ними криптосредства, эксплуатационную и техническую документацию к ним, ключевые документы;

– контролировать передачу криптосредств, эксплуатационной и технической документации к ним, ключевых документов между пользователями криптосредств и (или) ответственным пользователем криптосредств под расписку в соответствующем Журнале;

– пломбировать (опечатывать) и контролировать сохранность печатей (пломб) на аппаратных средствах, с которыми осуществляется штатное функционирование криптосредств, а также аппаратных и аппаратно-программных криптосредствах;

– контролировать получение и доставку криптосредств, эксплуатационной и технической документации к ним;

– заблаговременно делать заказы на изготовление очередных ключевых документов и рассылку на места использования для своевременной замены действующих ключевых документов;

– контролировать уничтожение неиспользованных или выведенных из действия ключевых документов в сроки, указанные в эксплуатационной и технической документации к соответствующим криптосредствам, или, если срок уничтожения эксплуатационной и технической документацией не установлен, не позднее 10 суток после вывода их из действия (окончания срока действия) под расписку в соответствующем Журнале;

– выводить из действия носители ключевой информации (далее – НКИ), в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие НКИ;

– принимать решение в чрезвычайных случаях, когда отсутствуют НКИ для замены скомпрометированных, об использовании скомпрометированных НКИ;

– проводить инструктаж пользователей криптосредств по правилам работы с криптосредствами и ключевыми документами.

Требовать прекращения обработки защищаемой информации в случае нарушения установленного порядка работ с криптосредствами или нарушения функционирования криптосредств.

Участвовать в анализе ситуаций, касающихся нарушения условий хранения носителей защищаемой информации, использования криптосредств, которые могут привести к нарушению конфиденциальности защищаемой информации.

Контролировать исполнение пользователями криптосредств требований Инструкции пользователя криптосредств _____, а также требований действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности защищаемой информации.

Принимать все необходимые меры для обеспечения безопасности защищаемой информации, в случае получения от пользователей информации о фактах утраты, компрометации ключевой информации, в частности, обеспечить выполнение следующих мероприятий:

– в каждом случае, по факту (или предполагаемой) компрометации ключевых документов, проводится служебное расследование; результатом расследования является квалификация или не квалификация данного события как компрометация;

– о факте компрометации ключевой информации пользователями криптосредств совместно с ответственным пользователем криптосредств производится информирование всех заинтересованных участников информационного обмена;

– выведенные из действия скомпрометированные ключевые документы после проведения расследования уничтожаются, о чем делается соответствующая запись в Журнале;

– для своевременного восстановления связи пользователю криптосредств выдается новый НКИ; для этого создаётся резервный запас НКИ, использование которых осуществляется в случаях крайней необходимости по решению ответственного пользователя криптосредств.

Подготавливать копии НКИ, которые подлежат основному учету и хранятся в сейфе ответственного пользователя криптосредств. Данные копии применяются с разрешения руководителя _____, если по результатам расследования не было установлено факта компрометации.

Хранить резервные НКИ отдельно от рабочих (актуальных) НКИ, с целью обеспечения невозможности их одновременной компрометации.

Своевременно информировать руководителя _____ о фактах утраты или недостачи криптосредств, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемой информации.

3. Права

Ответственный пользователь криптосредств имеет право:

Знакомиться с нормативными актами _____, регламентирующими процессы обработки защищаемой информации.

Требовать от пользователей ИС соблюдения требований действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности защищаемой информации.

Требовать прекращения работы в ИС, как в целом, так и отдельных пользователей криптосредств, в случае выявления нарушений требований по работе с криптосредствами, предназначенными для обеспечения безопасности защищаемой информации, или в связи с нарушением функционирования криптосредств.

С инструкцией ознакомлен:

_____

Приложение № 2
к Приказу

Перечень сотрудников _____, допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, в государственной информационной системе «Единая централизованная информационная система бухгалтерского учета и отчетности Республики Тыва»

№ п/п	ФИО Сотрудника	Должность
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		

Приложение № 3
к Приказу

Инструкция пользователя криптосредств

_____

1. Общие положения

Настоящая Инструкция пользователя криптосредств _____ (далее – Инструкция) определяет права и обязанности пользователей криптосредств, порядок обращения с криптосредствами, а также определяет порядок восстановления связи в случае компрометации действующих ключей к криптосредствам.

Пользователем криптосредств является сотрудник _____ (далее – _____), включенный в перечень сотрудников, допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, в Государственной информационной системы «Единая централизованная информационная система бухгалтерского учета и отчетности Республики Тыва» (далее – ИС), утвержденный нормативным актом _____.

Непосредственно к работе с криптосредствами, предназначенными для обеспечения безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, в ИС _____, пользователи допускаются только после соответствующего обучения. Обучение пользователей правилам работы с криптосредствами осуществляют сотрудники соответствующего органа криптографической защиты. Заключение о допуске или не допуске к работе с криптосредствами должно быть отмечено в Журнале обучения пользователей правилам работы с криптосредствами.

Пользователь криптосредств должен знать нормы действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну (далее – защищаемая информация), а также в области защиты информации при ее передаче по открытым каналам связи с использованием средств криптографической защиты.

В своей деятельности, связанной с обработкой защищаемой информации с использованием криптосредств, пользователь криптосредств руководствуется настоящей Инструкцией.

Пользователи криптосредств несут персональную ответственность за обеспечение конфиденциальности ключевой информации и защиту криптосредств от несанкционированного использования.

2. Обязанности и права пользователя криптосредств

Пользователь криптосредств обязан:

– соблюдать требования по обеспечению безопасности функционирования криптосредств;

– обеспечить конфиденциальность всей информации ограниченного распространения, доступной по роду выполняемых функциональных обязанностей;

– сдать ответственному пользователю криптосредств _____ (далее – Ответственный) носители ключевой информации (далее – НКИ) при увольнении или отстранении от исполнения обязанностей, связанных с использованием криптосредств;

– сдать Ответственному НКИ по окончании срока действия сертификата ключа, а также в случае компрометации ключа;

– немедленно уведомлять руководителя структурного подразделения или Ответственного о компрометации НКИ, о фактах утраты или недостачи криптосредств;

– в пределах своей компетенции предоставлять информацию комиссии, проводящей служебные расследования по фактам компрометации, а также выявлению причин нарушения требований безопасности функционирования криптосредств.

Пользователю криптосредств запрещается:

– осуществлять несанкционированное и безучётное копирование ключевых данных;

– хранить НКИ вне сейфов и помещений, гарантирующих их сохранность и конфиденциальность;

– передавать НКИ каким бы то ни было лицам, кроме Ответственного;

– во время работы оставлять НКИ без присмотра (например, на рабочем столе или в разъеме системного блока ПЭВМ);

– хранить на НКИ какую-либо информацию, кроме ключевой;

– использовать в помещениях, где применяются криптосредства, личные технические средства, позволяющие осуществлять копирование ключевой информации;

– использовать НКИ, выведенные из действия.

Пользователь имеет право:

– вносить предложения руководству _____ по вопросам использования криптосредств;

– повышать уровень квалификации по использованию криптосредств.

3. Порядок обращения с криптосредствами

Монтаж и установка криптосредства осуществляются органом криптографической защиты.

Служебные помещения, в которых размещаются криптосредства, должны отвечать всем требованиям по оборудованию и охране, предъявляемым к помещениям, выделенным для работы с конфиденциальной информацией. Для хранения НКИ помещения обеспечиваются сейфами (металлическими шкафами), оборудуются охранной сигнализацией и по убытии сотрудников закрываются, опечатываются личными печатями ответственных лиц (либо закрываются кодовым замком) и сдаются под охрану.

Для хранения НКИ пользователь криптосредств должен быть обеспечен личным сейфом. В случае отсутствия индивидуального сейфа по окончании рабочего дня пользователь криптосредств обязан сдавать НКИ Ответственному под подпись в Журнале учета и выдачи носителей с ключевой информацией.

Дубликаты ключей от сейфов (а также значения кодов – при наличии кодовых замков) пользователей криптосредств должны храниться в сейфе руководителя структурного подразделения или Ответственного в упаковках, опечатанных личными печатями пользователей криптосредств. Несанкционированное изготовление дубликатов ключей запрещено. В случае утери ключа механизм (секрет) замка (либо сам сейф) должен быть заменён.

К эксплуатации криптосредств допускаются лица, прошедшие соответствующую подготовку и изучившие правила пользования данным криптосредством.

Все программное обеспечение ПЭВМ, предназначенное для установки криптосредств, должно иметь соответствующие лицензии. Установка средств разработки и отладки программ на рабочую станцию, использующую криптосредства, не допускается.

4. Восстановление связи в случае компрометации действующих ключей к криптосредствам

Под компрометацией криптографического ключа понимается утрата доверия к тому, что данный ключ обеспечивает однозначную идентификацию владельца НКИ и конфиденциальность информации, обрабатываемой с его помощью. К событиям, связанным с компрометацией действующих криптографических ключей, относятся:

– утрата (хищение) НКИ, в том числе – с последующим их обнаружением;

– увольнение (переназначение) сотрудников, имевших доступ к НКИ;

– передача секретных ключей по линии связи в открытом виде;

– нарушение правил хранения НКИ;

– вскрытие фактов утечки передаваемой информации или её искажения (подмены, подделки);

– ошибки при совершении криптографических операций;

– несанкционированное или безучётное копирование ключевой информации;

– все случаи, когда нельзя достоверно установить, что произошло с НКИ (в том числе случаи, когда НКИ вышел из строя и доказательно не опровергнута вероятность того, что данный факт произошел в результате злоумышленных действий).

При наступлении любого из перечисленных выше событий пользователь криптосредств или владелец НКИ должен немедленно прекратить связь с другими абонентами и сообщить о факте компрометации (или предполагаемом факте компрометации) Ответственному лично, по телефону, электронной почте или другим доступным способом. В любом случае пользователь криптосредств или владелец НКИ обязан убедиться, что его сообщение получено и прочтено.

При подтверждении факта компрометации действующих ключей пользователь криптосредств обязан обеспечить немедленное изъятие из обращения скомпрометированных криптографических ключей и сдачу Ответственному в течение 3 рабочих дней.

Для восстановления конфиденциальной связи после компрометации действующих ключей пользователь криптосредств получает у Ответственного новые ключи.

ЛИСТ ОЗНАКОМЛЕНИЯ
с Инструкцией пользователя криптосредств

№ п/п	Ф.И.О.	Должность	Дата	Подпись

Приложение № 4
к Приказу

Перечень помещений, где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств

№ п/п	Адрес места расположения	Наименование структурного подразделения	Наименование помещения
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			

Приложение № 5
к Приказу

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

№ п/п	ФИО Сотрудника	Должность
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		

Приложение № 6
к Приказу

Порядок доступа в помещения, где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств

Настоящий Порядок регламентирует условия и порядок осуществления доступа в помещения _____ (далее – _____), где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств (далее – Помещения) в целях организации режима, препятствующего возможности неконтролируемого проникновения или пребывания в Помещениях лиц, не имеющих прав доступа в Помещения.

Настоящий Порядок разработан в соответствии с требованиями 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», приказа ФСБ России от 10 июля 2014 г. № 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», приказа ФАПСИ от 13 июня 2001 г. № 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».

Для Помещений организуется режим, препятствующий возможности неконтролируемого проникновения или пребывания в Помещениях лиц, не имеющих прав доступа в Помещения.

Помещения, где размещены используемые криптосредства, хранятся криптосредства, должны быть оснащены входными дверьми с замками, должно обеспечиваться постоянное закрытие дверей таких Помещений на замок и их открытие только для санкционированного прохода. Данные Помещения должны опечатываться по окончании рабочего дня/оборудоваться соответствующими

техническими устройствами, сигнализирующими о несанкционированном вскрытии.

Доступ в Помещения в рабочее (служебное) время имеют сотрудники, включенные в Перечень лиц, имеющих доступ в Помещения, утвержденный нормативным актом _____.

В нерабочее (неслужебное) время пребывание вышеуказанных сотрудников разрешается на основании служебных записок (или иных видов разрешающих документов), подписанных руководителем _____.

Нахождение в Помещениях посторонних лиц в рабочее (служебное) и нерабочее (неслужебное) время запрещается.

Уборка и техническое обслуживание Помещений допускаются только в присутствии Сотрудников _____.

Руководитель и лица, его замещающие, могут находиться в Помещениях в любое время, в том числе в нерабочие и праздничные дни.

О попытках неконтролируемого проникновения посторонних лиц в Помещения необходимо незамедлительно сообщать руководителю структурного подразделения _____ или руководителю _____.

В случае возникновения нештатной ситуации необходимо незамедлительно сообщать руководителю структурного подразделения _____ или руководителю _____.

Сотрудники органов МЧС и аварийных служб, врачи «скорой помощи» допускаются в Помещения для ликвидации нештатной ситуации, иных чрезвычайных ситуаций или оказания медицинской помощи в сопровождении руководителя структурного подразделения _____ или руководителя _____.

ЛИСТ ОЗНАКОМЛЕНИЯ

с Порядком доступа в помещения, где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств

№ п/п	Ф.И.О.	Должность	Дата	Подпись

Приложение № 7
к Приказу

Журнал поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче		Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя СКЗИ	Дата и расписка в получении	Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, произведших подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ	Дата изъятия (уничтожения)	Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, производивших изъятие (уничтожение)	Номер акта или расписка об уничтожении	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Приложение № 8
к Приказу

ЛИЦЕВОЙ СЧЕТ
пользователя криптосредств

_____

(должность, ФИО)

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о передаче		Отметка о возврате, уничтожении		Примечание
				От кого получены	Дата и расписка в получении	Кому передано СКЗИ	Дата и расписка в передаче	Дата возврата (уничтожения)	Расписка о возврате (уничтожении)	
1	2	3	4	5	6	7	8	9	10	11

Приложение № 9
к Приказу

Журнал учета и выдачи носителей с ключевой информацией

№ п/п	Учетный/ регистрационный (заводской) номер	Дата выдачи/сдачи	Выдано			Сдано		
			Ф.И.О. пользователя носителя с ключевой информацией	Подпись пользователя носителя с ключевой информацией	Подпись ответственного пользователя криптосредств	Ф.И.О. пользователя носителя с ключевой информацией	Подпись пользователя носителя с ключевой информацией	Подпись ответственного пользователя криптосредств
1	2	3	4	5	6	7	8	9

Приложение № 10
к Приказу

Журнал обучения пользователей правилам работы с криптосредствами

№ п/п	Ф.И.О. пользователя СКЗИ	Должность пользователя СКЗИ	Наименование СКЗИ, к работе с которым допущен сотрудник	Отметка о допуске/не допуске к самостоятельной работе с СКЗИ	Ф.И.О. ответственного пользователя СКЗИ / сотрудника органа криптографической защиты, проводившего обучение	Подпись ответственного пользователя СКЗИ / сотрудника органа криптографической защиты	Дата	Примечание
1	2	3	4	5	6	7	8	9

Приложение № 7
к Регламенту

УТВЕРЖДАЮ

Руководитель _____

«___» _____ 20__ г.

АКТ № _____

о готовности подключения пользователей к государственной информационной системе «Единая централизованная информационная система бюджетного (бухгалтерского) учета и отчетности Республики Тыва»

Комиссия

_____

наименование организации

в составе:

Председатель комиссии: _____

Члены комиссии: _____

_____

составила настоящий акт о том, что проведена проверка выполнения требований в соответствии с Регламентом подключения пользователей к Государственной информационной системе «Единая централизованная информационная система бюджетного (бухгалтерского) учета и отчетности Республики Тыва», 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 государственной информационной системой «Единая централизованная информационная система бюджетного (бухгалтерского) учета и отчетности Республики Тыва», технические и программные средства, участвующие в обработке информации при взаимодействии с ИС, 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 ИС, 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 пользователей ИС, технических и программных средств, участвующих в обработке информации при взаимодействии с ИС, а также проверка настроек и корректности функционирования следующих средств защиты информации и средств криптографической защиты информации, установленных на АРМ пользователя ИС:

средства криптографической защиты информации:

_____,
наименование СКЗИ (например, СКЗИ ПО ViPNet Client)

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)

средства межсетевого экранирования:

_____,
наименование средства защиты информации

средства обнаружения вторжений:

_____ _____,
наименование средства защиты информации

Заключение комиссии:

принятые организационные и технические меры по обеспечению информационной безопасности

_____,
(наименование организации)

соответствуют Регламенту подключения пользователей к Государственной информационной системе «Единая централизованная информационная система бюджетного (бухгалтерского) учета и отчетности Республики Тыва», автоматизированные рабочие места для подключения и обработки информации в государственной информационной системе «Единая централизованная информационная система бюджетного (бухгалтерского) учета и отчетности Республики Тыва» готовы и прошли аттестационные испытания:

_____.

(номер аттестата соответствия, дата выдачи)

Председатель:

_____	_____
(подпись)	(фамилия, имя, отчество)

Члены комиссии:

_____	_____
(подпись)	(фамилия, имя, отчество)
_____	_____
(подпись)	(фамилия, имя, отчество)