ЧĂВАШ РЕСПУБЛИКИН
ЦИФРА АТАЛАНĂВĔПЕ
ИНФОРМАЦИ ПОЛИТИКИН ТАТА
МАССĂЛЛĂ КОММУНИКАЦИСЕН
МИНИСТЕРСТВИ

ПРИКАЗ

01.10.2019 223 №

Шупашкар хули

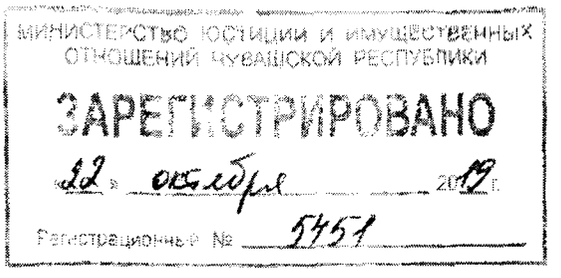
МИНИСТЕРСТВО
ЦИФРОВОГО РАЗВИТИЯ,
ИНФОРМАЦИОННОЙ ПОЛИТИКИ
И МАССОВЫХ КОММУНИКАЦИЙ
ЧУВАШСКОЙ РЕСПУБЛИКИ

ПРИКАЗ

01.10.2019 № 223

г. Чебоксары

Об утверждении регламента подключения пользователей к информационной системе поддержки и управления контрольно-надзорной деятельностью в Чувашской Республике



В целях обеспечения информационной безопасности при организации подключения автоматизированных рабочих мест, предназначенных для обеспечения информационного взаимодействия с информационной системой поддержки и управления контрольно-надзорной деятельностью в Чувашской Республике по защищенным с использованием шифровальных (криптографических) средств каналам передачи данных п р и к а з ы в а ю:

1. Утвердить регламент подключения пользователей к информационной системе поддержки и управления контрольно-надзорной деятельностью в Чувашской Республике.

2. Контроль за исполнением настоящего приказа возложить на заместителя министра Е.Ю. Грабко.

3. Настоящий приказ вступает в силу через десять дней после дня его официального опубликования.

Министр М.В. Анисимов

УТВЕРЖДЕН
приказом Министерства цифрового
развития, информационной политики
и массовых коммуникаций
Чувашской Республики
от 01.10.2019 № 223

Регламент
подключения пользователей к информационной системе поддержки и управления контрольно-надзорной деятельностью в Чувашской Республике

1. Общие положения

1.1. Регламент подключения пользователей к информационной системе поддержки и управления контрольно-надзорной деятельностью в Чувашской Республике (далее соответственно – Регламент, ИС «КНД ЧР») определяет содержание и порядок выполнения мероприятий, необходимых для подключения пользователей к ИС «КНД ЧР».

1.2. В настоящем Регламенте используются следующие понятия:

ИС «КНД ЧР» – информационная система регионального уровня, обеспечивающая автоматизацию процессов организации и осуществления регионального государственного контроля (надзора), в части процедур организации и проведения плановых и внеплановых проверок деятельности юридических лиц и индивидуальных предпринимателей, в том числе с учетом применения риск-ориентированного подхода;

оператор ИС «КНД ЧР» – орган исполнительной власти Чувашской Республики, уполномоченный на осуществление контрольно-надзорной деятельности;

оператор инфраструктуры ИС «КНД ЧР» – Министерство цифрового развития, информационной политики и массовых коммуникаций Чувашской Республики;

технический оператор инфраструктуры ИС «КНД ЧР» – бюджетное учреждение Чувашской Республики «Центр информационных технологий» Министерства цифрового развития, информационной политики и массовых коммуникаций Чувашской Республики (далее – БУ «Центр информационных технологий» Мининформполитики Чувашии);

должностные лица контрольно-надзорных органов – должностные лица органов исполнительной власти Чувашской Республики, уполномоченные на осуществление государственного контроля (надзора);

внешние пользователи – юридические лица и индивидуальные предприниматели, чья деятельность проверяется органами государственного контроля (надзора), экспертные организации, эксперты;

пользователи – должностные лица контрольно-надзорных органов, внешние пользователи;

закрытый контур ИС «КНД ЧР» – контур информационной системы,

содержащий сведения, используемые должностными лицами контрольно-надзорных органов;

открытый контур ИС «КНД ЧР» – контур информационной системы, содержащий сведения, используемые внешними пользователями;

иные понятия и термины, используемые в настоящем Регламенте, применяются в значениях, определенных федеральными законами «Об информации, информационных технологиях и о защите информации», «Об электронной подписи» и принимаемыми в соответствии с ними иными нормативными правовыми актами.

1.3. Основной целью Регламента является определение необходимых мероприятий по обеспечению информационной безопасности, проводимых оператором инфраструктуры ИС «КНД ЧР», техническим оператором инфраструктуры ИС «КНД ЧР» при организации подключения автоматизированных рабочих мест, предназначенных для обеспечения информационного взаимодействия с ИС «КНД ЧР» (далее – АРМ пользователей) по защищенным с использованием шифровальных (криптографических) средств каналам передачи данных (далее также – защищенное информационное взаимодействие).

1.4. Принимаемые оператором инфраструктуры ИС «КНД ЧР», техническим оператором инфраструктуры ИС «КНД ЧР» меры по защите информации при её обработке в ИС «КНД ЧР», в том числе при подключении АРМ пользователей к ИС «КНД ЧР», должны соответствовать требованиям Федерального закона «Об информации, информационных технологиях и о защите информации», принимаемым в соответствии с ним иным нормативным правовым актам, методическим и руководящим документам Федеральной службы по техническому и экспортному контролю (далее – ФСТЭК России) и Федеральной службы безопасности Российской Федерации (далее – ФСБ России) в области защиты информации и настоящему Регламенту.

1.5. В соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утверждёнными приказом ФСТЭК России от 11 февраля 2013 г. № 17 (зарегистрирован в Министерстве юстиции Российской Федерации 31 мая 2013 г., регистрационный № 28608), и требованиями 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 г. № 152 (зарегистрирован в Министерстве юстиции Российской Федерации 6 августа 2001 г., регистрационный № 2848), при обработке защищаемой информации в информационных системах с использованием средств криптографической защиты информации и её передаче по сетям связи общего пользования, в том числе информационно-телекоммуникационной сети «Интернет» (далее – сеть Интернет), должны применяться сертифицированные по требованиям безопасности информации средства защиты информации и средства криптографической защиты информации (далее также – СКЗИ).

1.6. Применяемые организационные и технические меры защиты информации должны удовлетворять требованиям, установленным для 3 класса

защищенности государственных информационных систем.

2. Требования к реализации организационных и технических мероприятий по обеспечению защиты информации при её обработке на автоматизированных рабочих местах должностных лиц контрольно-надзорных органов

2.1. В целях организации защищенного информационного взаимодействия с ИС «КНД ЧР» органы исполнительной власти Чувашской Республики обеспечивают реализацию организационных и технических мероприятий по обеспечению безопасности защищаемой информации при её обработке на автоматизированном рабочем месте должностного лица контрольно-надзорного органа (далее – АРМ должностного лица контрольно-надзорного органа).

2.2. Организационные мероприятия по обеспечению защиты информации должны включать:

назначение должностных лиц, ответственных за обеспечение информационного взаимодействия с ИС «КНД ЧР»;

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, в том числе носители защищаемой информации, носители ключевой, аутентифицирующей и парольной информации (далее – защищаемое помещение);

принятие мер, направленных на обеспечение защиты информации при их обработке в государственных информационных системах.

2.3. Технические мероприятия по обеспечению защиты информации должны включать:

установку и настройку средства антивирусной защиты;

установку и настройку СКЗИ и средств электронной подписи (при необходимости);

получение и установку ключей электронной подписи и сертификатов ключей проверки электронной подписи или парольно-ключевой информации, используемой для обеспечения защищенного информационного взаимодействия должностного лица контрольно-надзорного органа с ИС «КНД ЧР» (в зависимости от выбранной схемы информационного взаимодействия).

2.4. В целях реализации технических требований разработаны типовые схемы подключения АРМ должностного лица контрольно-надзорного органа к ИС «КНД ЧР» и приведены в приложении № 1 к настоящему Регламенту.

2.5. На АРМ должностного лица контрольно-надзорного органа, предназначенного для обеспечения защищенного информационного взаимодействия с ИС «КНД ЧР», должны быть установлены и настроены сертифицированные на соответствие требованиям по безопасности информации средства антивирусной защиты и СКЗИ (в зависимости от выбранной схемы информационного взаимодействия).

2.6. СКЗИ, используемые для обеспечения защищенного информационного взаимодействия с ИС «КНД ЧР», должны соответствовать требованиям ФСБ России к шифровальным (криптографическим) средствам класса КС1 и выше.

2.7. Реализация антивирусной защиты на АРМ должностных лиц контрольно-надзорных органов 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.

2.8. Перечень рекомендуемых средств защиты информации и СКЗИ приведен в приложении № 2 к настоящему Регламенту.

3. Требования к реализации организационных и технических мероприятий по обеспечению защиты информации при её обработке на автоматизированных рабочих местах внешних пользователей

3.1. В целях организации защищенного информационного взаимодействия с ИС «КНД ЧР» внешним пользователям рекомендуется обеспечить реализацию организационных и технических мероприятий по обеспечению безопасности защищаемой информации при её обработке на автоматизированных рабочих местах внешних пользователей (далее – АРМ внешних пользователей).

3.2. Организационные мероприятия по обеспечению защиты информации должны включать:

назначение должностных лиц, ответственных за обеспечение информационного взаимодействия с ИС «КНД ЧР»;

принятие мер, направленных на обеспечение защиты информации при их обработке в государственных информационных системах.

3.3. Технические мероприятия по обеспечению защиты информации должны включать установку и настройку средства антивирусной защиты.

3.4. В целях реализации технических требований разработаны типовые схемы подключения АРМ внешних пользователей к ИС «КНД ЧР» и приведены в приложении № 1 к настоящему Регламенту.

4. Порядок подключения должностных лиц контрольно-надзорных органов к ИС «КНД ЧР»

4.1. Установка и настройка программного обеспечения, средств защиты информации и СКЗИ осуществляется должностными лицами контрольно-надзорных органов в соответствии с эксплуатационной документацией на используемые средства защиты информации и СКЗИ.

4.2. Для организации защищенного информационного взаимодействия АРМ

должностного лица с ИС «КНД ЧР» посредством СКЗИ «Континент TLS VPN Клиент» (Вариант 1) требуются ключи электронной подписи и сертификаты ключей проверки электронной подписи, соответствующие требованиям Федерального закона «Об электронной подписи» и национальному стандарту Российской Федерации 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 Регламентом удостоверяющего центра БУ «Центр информационных технологий» Мининформполитики Чувашии, который размещен в информационно-телекоммуникационной сети «Интернет» по адресу: http://uc-cit.cap.ru.

Изготовление сертификата ключа проверки электронной подписи, который не является квалифицированным сертификатом и может использоваться только для организации защищенного информационного взаимодействия с ИС «КНД ЧР», осуществляется техническим оператором инфраструктуры ИС «КНД ЧР» в течение пяти рабочих дней со дня предоставления должностным лицом заявки на изготовление сертификата ключа проверки электронной подписи по форме согласно приложению № 3 к настоящему Регламенту.

4.3. Для организации защищенного информационного взаимодействия АРМ должностного лица контрольно-надзорного органа с ИС «КНД ЧР» посредством программного обеспечения ViPNet Client версия 4 (Вариант 2) требуется парольно-ключевая информация в сеть 2921.

Изготовление парольно-ключевой информации для организации защищенного информационного взаимодействия с ИС «КНД ЧР» осуществляется техническим оператором инфраструктуры ИС «КНД ЧР» при наличии свободных лицензий в течение пяти рабочих дней со дня предоставления должностным лицом заявки по форме согласно приложению № 4 к настоящему Регламенту.

4.4. Если АРМ должностного лица контрольно-надзорного органа расположено в защищенной сети, организованной посредством программно-аппаратного комплекса ViPNet Coordinator HW в сети 2921 (Вариант 3), для организации защищенного информационного взаимодействия АРМ должностного лица контрольно-надзорного органа с ИС «КНД ЧР» установка дополнительных СКЗИ на АРМ должностного лица контрольно-надзорного органа не требуется.

4.5. Проверка возможности подключения к ИС «КНД ЧР» с АРМ должностного лица контрольно-надзорного органа осуществляется путем открытия веб-ресурса по адресу: https://www.knd.cap.ru с использованием веб-браузера или специализированного прикладного программного обеспечения, установленного на АРМ должностного лица контрольно-надзорного органа.

Доступ должностных лиц для обработки информации в ИС «КНД ЧР» осуществляется только после выполнения организационных и технических мероприятий в соответствии с требованиями настоящего Регламента.

Выполнение вышеуказанных мероприятий подтверждается соответствующим актом о готовности, который оформляется по форме согласно приложению № 5 к настоящему Регламенту и предоставляется оператору ИС «КНД ЧР».

4.6. В случае принятия должностным лицом контрольно-надзорного органа решения о прекращении доступа к ИС «КНД ЧР» необходимо не позднее трех

рабочих дней со дня принятия данного решения представить техническому оператору инфраструктуры ИС «КНД ЧР» заявку на прекращение действия (отзыв) сертификата ключа проверки электронной подписи, используемого для организации защищенного информационного взаимодействия с ИС «КНД ЧР», по форме согласно приложению № 6 к настоящему Регламенту или заявку на прекращение действия (отзыв) парольно-ключевой информации для подключения к сети с номером 2921 по форме согласно приложению № 7 к настоящему Регламенту.

4.7. 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 ИС «КНД ЧР», должностное лицо контрольно-надзорного органа обязано немедленно уведомить технического оператора инфраструктуры ИС «КНД ЧР» 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.

5. Порядок подключения внешних пользователей к ИС «КНД ЧР»

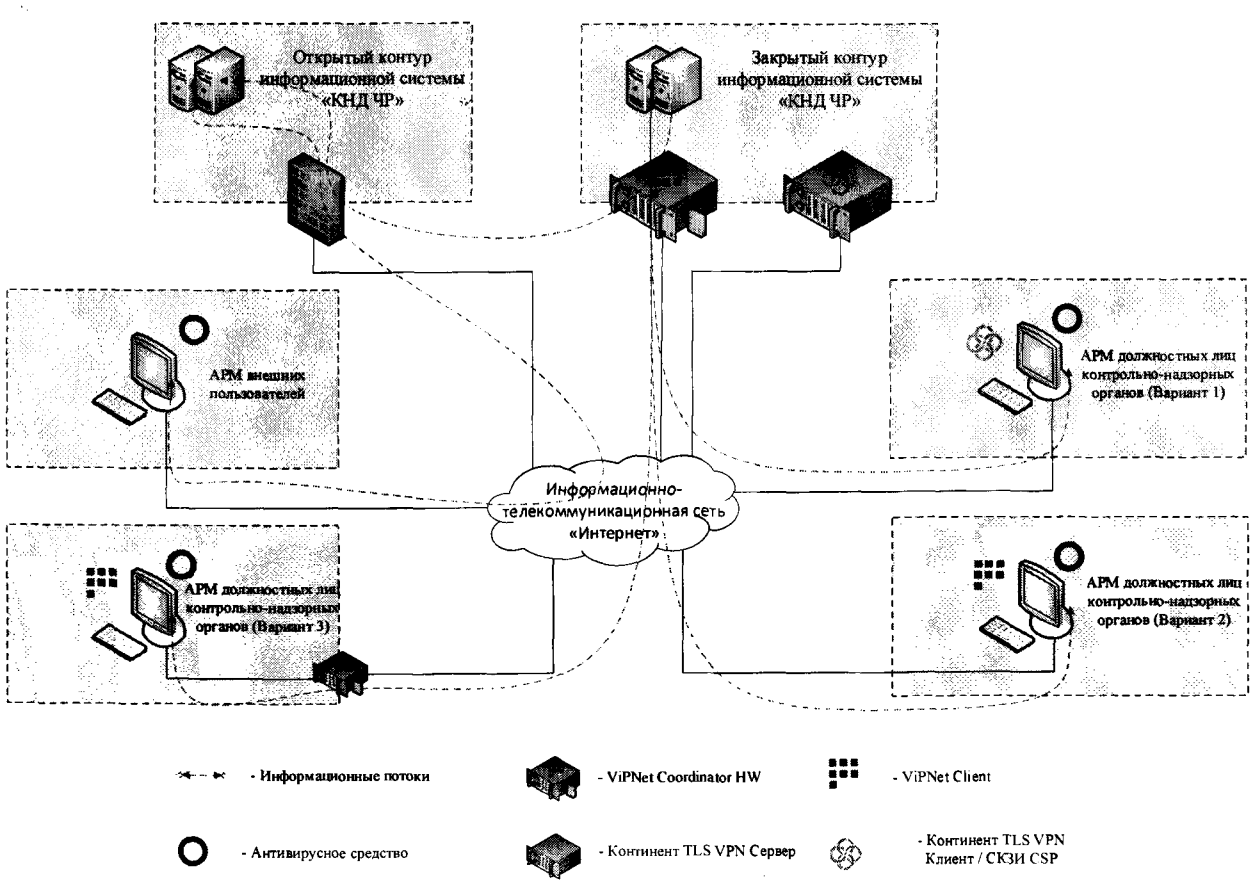
5.1. Установка и настройка программного обеспечения, средств защиты информации осуществляется внешними пользователями в соответствии с эксплуатационной документацией на используемые средства защиты информации.

5.2. Проверка возможности подключения к ИС «КНД ЧР» с АРМ внешнего пользователя осуществляется путем открытия веб-ресурса по адресу: https://www.proverki.cap.ru с использованием веб-браузера или специализированного прикладного программного обеспечения, установленного на АРМ пользователя.

5.3. Оформление акта о готовности для внешних пользователей не требуется.

Приложение № 1
к регламенту подключения
пользователей к информационной
системе поддержки и управления
контрольно-надзорной деятельностью
в Чувашской Республике

Обобщенная схема информационного взаимодействия АРМ с ИС «КНД ЧР»



Приложение № 2
к регламенту подключения
пользователей к информационной
системе поддержки и управления
контрольно-надзорной деятельностью
в Чувашской Республике

Перечень рекомендуемых сертифицированных средств защиты информации и средств криптографической защиты информации

1. Средства криптографической защиты информации (далее – СКЗИ) и средства электронной подписи:
   - СКЗИ «КриптоПро CSP» версии 4.0 или выше, либо СКЗИ «ViPNet CSP» версии 4.2 или выше;
   - ПО ViPNet Client версия 4;
   - СКЗИ «Континент TLS VPN Клиент».

СКЗИ «Континент TLS VPN Клиент» рекомендуется устанавливать для организации защищенного информационного взаимодействия с информационной системой «КНД ЧР» в случае 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 комплект поставки СКЗИ «Континент TLS VPN Клиент».

2. Средства антивирусной защиты информации:
   - Программное изделие «Kaspersky Endpoint Security 10 для Windows»;
   - Программное обеспечение «Dr.Web Enterprise Security Suite»;
   - Иное сертифицированное антивирусное средство.

Приложение № 3
к регламенту подключения
пользователей к информационной
системе поддержки и управления
контрольно-надзорной деятельностью
в Чувашской Республике

На бланке Учреждения внешнего пользователя

БУ «Центр информационных технологий» Мининформполитики Чувашии

ЗАЯВКА
на изготовление сертификата ключа проверки электронной подписи

_____
(наименование организации)

в целях организации защищенного информационного взаимодействия при подключении к информационной системе «КНД ЧР» просит изготовить сертификат ключа проверки электронной подписи, содержащий следующие данные[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].

_____ _____ / _____ /
(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.

[2] Указывается только в случае, если запрос на изготовление сертификата формируется на АРМ внешнего пользователя ИС «КНД ЧР».

Приложение № 4
к регламенту подключения
пользователей к информационной
системе поддержки и управления
контрольно-надзорной деятельностью
в Чувашской Республике

На бланке Учреждения внешнего пользователя

БУ «Центр информационных технологий» Мининформполитики Чувашии

ЗАЯВКА
на изготовление парольно-ключевой информации для подключения к сети с номером 2921

_____
(наименование организации)

в целях организации защищенного информационного взаимодействия при подключении к информационной системе «КНД ЧР» просит изготовить парольно-ключевую информацию для подключения к сети с номером 2921.

_____
(наименование организации)

провела мероприятия по закупке оборудования и необходимых лицензий

_____,
(название вашего ViPNet-совместимого технического решения)

для подключения к информационной системе «КНД ЧР» по схеме № 2.

_____ _____ / _____ /
(должность руководителя) (подпись) (расшифровка)

Приложение № 5
к регламенту подключения
пользователей к информационной
системе поддержки и управления
контрольно-надзорной деятельностью
в Чувашской Республике

УТВЕРЖДАЮ

«___» _____ 20___ г. *Руководитель*

_____

Акт № _____
о готовности подключения пользователей к
информационной системе «КНД ЧР»

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 информационной системе поддержки и управления контрольно-надзорной деятельностью в Чувашской Республике, утвержденным приказом Министерства цифрового развития, информационной политики и массовых коммуникаций Чувашской Республики 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 Федеральным законом «Об информации, информационных технологиях и о защите информации» и принимаемыми в соответствии с ним 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 информационной системой «КНД ЧР» (далее – ИС «КНД ЧР»), технические и программные средства, участвующие в обработке информации при взаимодействии с ИС «КНД ЧР», 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 «КНД ЧР», знания ими основных положений

законодательства в области защиты информации, 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 (зарегистрирован в Министерстве юстиции Российской Федерации 6 августа 2001 г., регистрационный № 2848).

4. Готовности АРМ пользователя, технических и программных средств, участвующих в обработке информации при взаимодействии с ИС «КНД ЧР», а также проверка настроек и корректности функционирования следующих средств защиты информации и средств криптографической защиты информации, установленных на АРМ пользователя:

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 (заполняется при наличии):

_____;
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 ИС «КНД ЧР» 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 № 6
к регламенту подключения
пользователей к информационной
системе поддержки и управления
контрольно-надзорной деятельностью
в Чувашской Республике

На бланке Учреждения внешнего пользователя

БУ «Центр информационных технологий» Мининформполитики 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 информационной системой «КНД ЧР», содержащего следующие данные[1]:

Серийный номер сертификата	
ОГРН организации	
Фамилия	
Имя Отчество	
СНИЛС	

_____ _____ / _____ /
(должность руководителя) (подпись) (расшифровка)

[1] Серийный номер сертификата указывается в обязательном порядке, иные данные указываются, если они присутствуют в сертификате.

Приложение № 7
к регламенту подключения
пользователей к информационной
системе поддержки и управления
контрольно-надзорной деятельностью
в Чувашской Республике

На бланке Учреждения внешнего пользователя

БУ «Центр информационных технологий» Мининформполитики Чувашии

ЗАЯВКА
на прекращение действия (отзыв) парольно-ключевой информации для подключения к сети с номером 2921

_____
(наименование организации)

в связи с

_____
(причина прекращения действия парольно-ключевой информации)

просит прекратить действие парольно-ключевой информации для подключения к сети с номером 2921, используемого для организации защищенного информационного взаимодействия с информационной системой «КНД ЧР», содержащего следующие данные:

Имя пользователя ViPNet	
Сетевой узел ViPNet	

_____ _____ / _____ /
(должность руководителя) (подпись) (расшифровка)