

## СОГЛАШЕНИЕ *08-137/14129*

### об информационном взаимодействии в электронном виде по общедоступным каналам связи с использованием средств криптографической защиты информации между Межрайонной ИФНС России № 7 по Оренбургской области и Администрацией муниципального образования Надеждинский сельсовет Саракташского района Оренбургской области.

г. Оренбург

«*22*» *08* 2019 г.

Межрайонная ИФНС России № 7 по Оренбургской области (далее – Инспекция), в лице И.о. начальника Хакимова Станислава Станиславовича, действующего на основании Положения о Межрайонной ИФНС России № 7 по Оренбургской области от 06.10.2015 года и Администрацией муниципального образования Надеждинский сельсовет Саракташского района Оренбургской области (далее – Администрация) в лице Главы Муниципального образования *Тимко Оксана Анатольевна*

действующего на основании Устава Муниципального образования Надеждинский сельсовет Саракташского района Оренбургской области, вместе именуемые Стороны, заключили настоящее Соглашение о нижеследующем.

#### 1. Предмет соглашения

1.1 Настоящее Соглашение определяет порядок и условия использования средств криптографической защиты информации (далее – СКЗИ), включая алгоритмы усиленной квалифицированной электронной подписи (далее - УКЭП) при организации электронного обмена информацией между Инспекцией и Администрацией.

1.2. Перечень информации, форматы и сроки обмена определены приказом ФНС России от 22.10.2018 №ММВ-7-21/652@ «Об утверждении формы и формата представления информации об установлении, изменении и прекращении действия региональных и местных налогов, а также порядка направления указанной информации в электронной форме».

1.3. В рамках исполнения настоящего Соглашения стороны руководствуются:

- Федеральным законом от 06.04.2011 №63-ФЗ «Об электронной подписи»;
- Приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 №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» (далее – Приказ ФАПСИ от 13.06.2001 г. №152);
- Приказом ФСБ России от 09.02.2005 №66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (положение ПКЗ-2005)»;
- Приказом ФСБ России от 10.07.2014 №378 «Об утверждении Составы 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»;
- Требованиями эксплуатационной документации (формуляр, правила пользования) применяемых средств криптографической защиты информации.

## 2. Порядок использования СКЗИ

2.1. Перед началом использования СКЗИ Стороны выполняют следующие условия:

2.1.1. Назначают сотрудников, ответственных за работу со СКЗИ и обмениваются данной информацией.

2.1.2. Стороны обеспечивают обучение лиц, использующих криптосредства, работе с ними до допуска к самостоятельной работе.

2.1.3. Администраторы безопасности (ответственные пользователи) Сторон обеспечивают учет ключевых документов, выданных на имя сотрудников, уполномоченных работать с СКЗИ, дистрибутивов и эксплуатационной документации СКЗИ.

2.2. Стороны договорились при организации защищенного электронного обмена информацией использовать:

- Инспекция использует комплект программного обеспечения СКЗИ на базе «Крипто ПРО CSP», «Крипто-АРМ» и почтовый клиент «Mozilla Thunderbird».

- Администрация использует комплект программного обеспечения СКЗИ на базе «Крипто ПРО CSP», «Крипто-АРМ» и почтовый клиент «rad-adm2014@kovveva.ru @yandex.ru»

2.3. Непосредственную эксплуатацию СКЗИ организуют и обеспечивают уполномоченные сотрудники (пользователи СКЗИ), прошедшие обучение и допущенные к самостоятельной работе с СКЗИ.

2.4. Основаниями для прекращения (приостановления) обмена сведениями являются следующие условия:

2.4.1. Выявлены нарушения требований к обмену сведениями и защите информации при обмене сведениями, предусмотренные законодательством Российской Федерации, нормативными актами уполномоченных органов государственной власти и соглашением Сторон.

2.4.2. Заявление одной из Сторон с просьбой о приостановлении обмена сведениями, направленное в письменной форме не позднее, чем за три рабочих дня до даты начала приостановления обмена сведениями, указанной в заявлении.

2.4.3. Компрометация ключевой информации одной из Сторон. Под компрометацией ключа подразумевается утрата доверия к тому, что используемые закрытые ключи недоступны посторонним лицам, например, утрата ключевых носителей; увольнение сотрудников, имевших доступ к ключевой информации; доступ посторонних лиц к ключевой информации.

2.4.4. Иные основания, предусмотренные нормативно-правовыми актами Российской Федерации.

2.5. О прекращении обмена сведениями Сторона-инициатор незамедлительно уведомляет любым доступным способом другую Сторону. В срок, не превышающий три рабочих дня, Сторона-инициатор повторяет уведомление в письменной форме с указанием причин, даты начала и срока прекращения обмена сведениями.

2.6. Порядок действий при компрометации ключей шифрования определяется действующим порядком (Приказ ФАПСИ от 13.06.2001 г. №152).

2.7. Восстановление обмена производится после устранения причин, вызвавших прекращение обмена.

2.8. В ходе использования СКЗИ Стороны обеспечивают контроль за соблюдением условий использования СКЗИ, предусмотренных эксплуатационной и технической документацией к ним.

## 3. Использование (эксплуатация) средств криптографической защиты информации

3.1. Для обеспечения конфиденциальности и подлинности (подтверждения

целостности и авторства) сведений Стороны используют сертифицированные в установленном порядке СКЗИ, обеспечивающие в соответствии с требованиями ФСБ России безопасность информации по уровню класса СКЗИ КС1 или выше.

3.2. Стороны признают стойкость используемых СКЗИ и средств УКЭП достаточной для обеспечения конфиденциальности сведений и подтверждения подлинности УКЭП сведений при условии соблюдения требований по защите информации, технической и эксплуатационной документации на СКЗИ и средства УКЭП.

3.3. Управление ключевой системой, используемой при обмене сведениями, осуществляется Сторонами самостоятельно.

3.4. Удостоверяющий центр ФНС России осуществляет деятельность по изготовлению ключевых документов уполномоченных лиц Инспекции, регистрации владельцев сертификатов ключей подписи, управлению сертификатами ключей подписи.

3.5. Администрация в рамках обмена с Инспекцией используют ключевые документы, изготовленные аккредитованным Минкомсвязи России Удостоверяющим центром.

3.6. Стороны при обмене электронными документами обязуются производить соединение с почтовым сервером с целью проверки наличия электронных сообщений не менее 3-х раз в сутки.

3.7. Информация от Инспекции отправляется с ящика [kp2.r5638@nalog.ru](mailto:kp2.r5638@nalog.ru).

3.8. Информация от Администрации отправляется с электронного почтового ящика [nad-adm@omciaka.beva.ru](mailto:nad-adm@omciaka.beva.ru) в [vk@yandex.ru](mailto:vk@yandex.ru).

#### **4. Признание сведений, переданных в электронном виде**

4.1. Сведения, заверенные подлинными УКЭП уполномоченных сотрудников, признаются Сторонами, вне зависимости от того, существуют ли такие документы, содержащие данные сведения, на бумажных носителях или нет.

4.2. Сведения, оформленные в соответствии с указанными требованиями, не могут быть оспорены только на том основании, что они переданы в электронной форме.

#### **5. Права и обязанности Сторон**

5.1. При обмене сведениями Стороны имеют следующие права:

5.1.1. Отказывать одной из Сторон в приеме сведений с указанием причин отказа.

5.1.2. Прекращать обмен сведениями при наличии оснований, предусмотренных п. 2.4. настоящего Соглашения.

5.1.3. Запрашивать у одной из Сторон при необходимости заверенные копии переданной с использованием системы электронного документооборота информации на бумажном носителе.

5.2. При обмене сведениями Стороны обязаны:

5.2.1. Соблюдать требования нормативных документов, правил пользования.

5.2.2. Вести архивы входящих и исходящих сведений.

5.2.3. Обеспечивать условия использования, хранения и уничтожения закрытых ключей УКЭП и ключей шифрования (аутентификации).

5.2.4. Осуществлять контроль полученных сведений и сообщать друг другу об обнаруженных ошибках.

5.2.5. Обеспечить доступ к автоматизированному рабочему месту с установленными СКЗИ только уполномоченным сотрудникам.

5.2.6. Своевременно проводить мероприятия по приостановке действия или отзыву сертификатов ключей подписи уполномоченных сотрудников.

5.2.7. Своевременно информировать друг друга о фактах компрометации ключей УКЭП и/или ключей шифрования.

5.2.8. Своевременно информировать друг друга обо всех случаях возникновения технических неисправностей или других обстоятельств, препятствующих обмену сведениями.

## 6. Ответственность Сторон

6.1. Каждая Сторона несет ответственность за содержание сведений, заверенных подлинной (в соответствии со ст. 11 Федерального закона от 06.04.2011 №63-ФЗ «Об электронной подписи») УКЭП своего уполномоченного сотрудника.

6.2. Стороны несут ответственность за нарушение конфиденциальности информации в соответствии с действующим законодательством Российской Федерации.

6.3. Стороны несут ответственность за проверку достоверности УКЭП при проверке входящих электронных документов.

6.4. Стороны несут ответственность за отправку конфиденциальной информации по общедоступным сетям связи без криптографической защиты или ввиду ее неработоспособности.

## 7. Порядок разрешения разногласий

7.1. В случае возникновения споров и разногласий в связи с обменом сведениями Стороны проводят техническую экспертизу силами ответственных сотрудников Сторон и/или ответственных за защиту информации. По результатам технической экспертизы Стороны принимают решение по урегулированию разногласия.

7.2. Споры, по которым не достигнуто соглашение Сторон после проведения технической экспертизы, разрешаются в Арбитражном суде.

## 8. Срок действия Соглашения и порядок его изменения

8.1. Настоящее Соглашение заключается на неограниченный срок и вступает в силу со дня его подписания Сторонами.

8.2. Внесение изменений и дополнений в настоящее Соглашение оформляется в виде документа, подписываемого уполномоченными должностными лицами Сторон с указанием даты начала действия изменений.

Подписи сторон:

И.о. начальника  
Межрайонной ИФНС России № 7  
по Оренбургской области



С.С. Хахимов

Глава муниципального образования  
Надеждинский сельсовет  
Саракташского района Оренбургской  
области



Тимоко О. А.

Фамилия И.О.