ПРОСТАЯ ПОДПИСЬ РАБОТНИКА

ОАО «Аэрофлот – российские авиалинии» 31.01.2014г. был издан Приказ №31 «Об утверждении Регламента применения простой электронной подписи в комплексной информационной системе «Аккорд».

В соответствии с данным приказом в целях совершенствования процедур ознакомления летного состава ОАО «Аэрофлот» с документами, непосредственно касающимися их трудовой деятельности, с 01.05.2014г. планируется ввести указанный Регламент.

Поскольку применение электронной подписи является сложным и важным вопросом, ШПЛС *представляет* свое мотивированное мнение по данной теме.

Нормативное регулирование:

1) Федеральный закон от 06.04.2011г. № 63-ФЗ «Об электронной подписи»;

2) Гражданский кодекс РФ, Часть первая статьи 160 и 434;

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

4) Федеральный закон от 27.07.2006г. № 152-ФЗ «О персональных данных»;

5) Приказ Минкомсвязи России от 29 сентября 2011 г. № 242 «Об утверждении порядка передачи реестров квалифицированных сертификатов ключей проверки электронной подписи и иной информации в федеральный орган исполнительной власти, уполномоченный в сфере использования электронной подписи в случае прекращения деятельности аккредитованного удостоверяющего центра»;

6) Приказ Минкомсвязи России от 5 октября 2011 г. № 250 «Об утверждении порядка формирования и ведения реестров квалифицированных сертификатов ключей проверки электронной подписи, а также предоставления информации из таких реестров»;

7) Приказ ФСБ РФ от 27.12.2011 № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра»;

8) Приказ ФСБ РФ от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;

9) Частный случай применения простой электронной подписи – это Федеральный закон от 27.07.2010г. №210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;

10) Что касается Трудового кодекса РФ, там содержатся нормы, регулирующие применения электронной подписи только в отношении дистанционного работника (фрилансера).

В соответствии со статьей 2 Федерального закона от 06.04.2011г. № 63-ФЗ «Об электронной подписи» (далее ФЗ № 63) электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

В целях обеспечения юридической значимости электронного документа его подпись должна позволять:

1) установить лицо, подписавшее документ; 2) установить неизменность документа после его подписи; 3) обеспечить невозможность отказа от факта подписания документа.

Видами электронных подписей, отношения в области использования которых регулируются ФЗ № 63, являются простая электронная подпись и усиленная электронная подпись. Различаются усиленная неквалифицированная электронная подпись (далее – неквалифицированная электронная подпись) и усиленная квалифицированная электронная подпись (далее – квалифицированная электронная подпись).

Простой электронной подписью является электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом (ст. 5 ФЗ № 63).

Электронный документ считается подписанным простой электронной подписью (далее также – ПЭП) при выполнении, в том числе одного из следующих условий:

1) простая электронная подпись содержится в самом электронном документе;

2) ключ простой электронной подписи применяется в соответствии с правилами, установленными оператором информационной системы, с использованием которой осуществляются создание и (или) отправка электронного документа, и в созданном и (или) отправленном электронном документе содержится информация, указывающая на лицо, от имени которого был создан и (или) отправлен электронный документ.

Информация в электронной форме, подписанная простой электронной подписью или неквалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, в случаях, установленных федеральными законами (*пример, государственные и муниципальные услуги*), принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между участниками электронного взаимодействия.

В части 2 статьи 6 ФЗ № 63 законодатель установил дополнительные требования к соглашениям между участниками электронного взаимодействия и нормативным правовым актам, на основании которых электронный документ, подписанный электронной подписью, будет считаться равнозначным подписанному документу на бумажном носителе. Использование простой электронной подписи вне рамок таких соглашений (нормативных актов) влечет отказ в признании подписанных документов.

Указанные нормативно-правовые акты и соглашения между участниками электронного взаимодействия должны предусматривать, в частности:

1) правила определения лица, подписывающего электронный документ, по его простой электронной подписи. Для того, чтобы установить лицо, подписывающее электронный документ, в него включается соответствующая информация в соответствии с п. 2 ч. 1 ст. 9 ФЗ № 63 электронная подпись используется для того, чтобы проверить, действительно ли электронный документ подписан именно тем лицом, которое указано в документе. Поэтому «определение» в данном смысле следует понимать не как идентификацию, а как аутентификацию, другими словами, «установление подлинности».

2) обязанность лица, создающего и (или) использующего ключ электронной подписи, соблюдать его конфиденциальность. Здесь ключ понимается как общее обозначение ключа, кода, пароля или иного средства, используемого для подписания документа простой электронной подписью. Ключ может быть создан и передан лицу оператором информационной системы, в рамках которой осуществляется электронный документооборот, либо другим лицом, которому оператор делегирует соответствующие полномочия. Лицо, отвечающее за создание ключей, обязано обеспечивать конфиденциальность каждого из них, а лицо, использующее ключ, – конфиденциальность своего ключа. **Обладателем ключа** будет являться лицо, от имени которого будет считаться подписанным электронный документ, если он подписан с использованием данного ключа. Требование соблюдать конфиденциальность своего ключа предполагает, что ключ может быть передан его обладателем третьему лицу как средство делегирования права подписи (аналогичное допущение предполагает и формулировка ч. 1 ст. 10 ФЗ № 63). Представляется, что нормативно-правовыми актами, соглашениями участников электронного взаимодействия или порядком исполь-

зования корпоративной информационной системы данное требование может быть при необходимости усилено до требования хранить свой ключ в тайне и обеспечить защиту от доступа к нему любых третьих лиц. В случае если лицо нарушает указанное требование и не соблюдает конфиденциальность ключа, для него наступают последствия, являющиеся общепринятыми в практике использования электронных подписей: оно считается лицом, самостоятельно подписавшим все документы, подписанные с помощью его ключа, а бремя доказывания обратного и установления действительного автора документа ложится на него самого.

Стоит отметить, что в соответствии со статьей 9 ФЗ № 63 информация в электронной форме, подписанная квалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, кроме случая, если федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе. Также, если в соответствии с федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или обычаем делового оборота документ должен быть заверен печатью, электронный документ, подписанный усиленной электронной подписью и признаваемый равнозначным документу на бумажном носителе, подписанному собственноручной подписью, признается равнозначным документу на бумажном носителе, подписанному собственноручной подписью и заверенному печатью.

Таким образом, отличие ПЭП от других видов, перечисленных в ст. 5 ФЗ № 63, заключается в том, что из двух основных функций, обеспечиваемых технологией электронной подписи: обеспечение целостности документа и аутентификация лица, подписавшего документ – она обеспечивает лишь вторую. Другими словами, электронный документ, подписанный ПЭП, может впоследствии быть изменен, и установить это с помощью проверки электронной подписи будет невозможно. По этой же причине законодатель формулирует требование нахождения ПЭП в самом электронном документе: поскольку механизм формирования подписи никак не зависит от содержимого электронного документа, то определить, что данная электронная подпись, хранящаяся в виде отдельного файла, создавалась для подписания определенного документа, невозможно.

Из названного отличия вытекает и другое следствие. Использование ПЭП как средства определения лица, подписавшего документ, невозможно вне рамок специализированной информационной системы.

В литературе приводится следующий интересный пример: если участники электронного взаимодействия договорятся о формировании простой электронной подписи с помощью некоторого обособленного программного средства и последующем размещении ее в документе посредством обычного текстового редактора, никто не помешает недобросовестному получателю документа впоследствии перенести эту подпись в другой электронный документ (путем простого копирования) и доказать, что изначально подпись относилась к другому документу, будет невозможно. Поэтому **простая электронная подпись может применяться исключительно в рамках документооборота с использованием специально разработанной для этих целей информационной системы**. Невозможность перенесения электронной подписи в другой документ, контроль целостности (неизменности) подписанного документа в этом случае будет обеспечиваться функциональными возможностями самой информационной системы. Именно поэтому в п. 2 ч. 2 ст. 9 указывается, что создание и (или) отправка документа осуществляются с использованием информационной системы, а ключ простой электронной подписи применяется в соответствии с правилами (регламентом), установленными оператором этой системы.

В литературе также отмечается, что в ФЗ № 63 существует техническая неточность, поскольку простая электронная подпись не требует использования собственно ключа, а может строиться на использовании кодов, паролей и иных средств. Пользователь входит в систему, используя пароль, ключ на смарт-карте и т.д., после чего работает с документами в рамках информационной системы, причем при осуществлении определенных операций (создание, редактирование, отправка документа и т.д.) простая электронная подпись будет создаваться и присоединяться к документу автоматически.

Основной сферой использования ПЭП является электронный документооборот в рамках корпоративной информационной системы с определенным и ограниченным кругом пользователей. Подтвердить подлинность лица, подписавшего документ, другому лицу, не входящему в этот круг пользователей, с помощью простой универсальной процедуры (как это имеет место для квалифицированной электронной подписи) невозможно, хотя при необходимости можно провести такое доказательство в судебном порядке, опираясь на алгоритмы и регламент работы информационной системы (при условии, что можно доказать добросовестность оператора информационной системы). В правоотношениях, где участникам документооборота необходимо подтверждать авторство электронной подписи внешним по отношению к информационной системе пользователям (например, в суде), должны использоваться другие виды подписи.

В ст. 3 ФЗ № 63 указано, что порядок использования электронной подписи в корпоративной информационной системе может также устанавливаться оператором информационной системы, пример предлагаемый ОАО «Аэрофлот» Регламента применения простой электронной подписи в комплексной информационной системе «Аккорд». Становясь пользователем корпоративной информационной системы, лицо, как правило, соглашается с порядком ее использования.

К отношениям, связанным с использованием ПЭП, не применяются положения большей части статей ФЗ № 63. В частности, простая электронная подпись не имеет сертификата и не может подтверждаться удостоверяющим центром (это связано с тем, что механизм простой электронной подписи не базируется на универсальных криптографических алгоритмах). Соответственно, к программным средствам подписания электронного документа и проверки подписи не предъявляется никаких особых требований, однако ФЗ № 63 и не содержит условий, при которых простая электронная подпись признается действительной. Повторим, что такие условия должны определяться иными нормативными актами, соглашениями участников электронного взаимодействия или порядком использования корпоративной информационной системы.

Так, например, ст. 21.2 Федерального закона от 27.07.2010 N 210-ФЗ устанавливает, что запрос и иные документы, необходимые для предоставления государственной или муниципальной услуги, подписанные простой электронной подписью и поданные заявителем с соблюдением требований данного закона, признаются равнозначными запросу и иным документам, подписанным собственноручной подписью и представленным на бумажном носителе, за исключением случаев, если федеральными законами или иными нормативными правовыми актами установлен запрет на обращение за получением государственной или муниципальной услуги в электронной форме. Федеральный закон от 27.07.2010 № 210-ФЗ также устанавливает, что правила использования простых электронных подписей при оказании государственных и муниципальных услуг, устанавливаемые Правительством РФ, должны предусматривать следующие дополнительные требования:

1) требования, которым должны соответствовать простые электронные подписи и (или) технологии их создания;

2) способы установления личности лица при выдаче ему ключа простой электронной подписи в целях получения государственных и муниципальных услуг.

Одно из оснований, подтверждающих тот факт, ПЭП является недостаточно надежным средством с точки зрения обеспечения информационной безопасности и может стать слабым местом системы, в которой она используется, является то, что в соответствии с ФЗ № 63 использование простой электронной подписи для подписания электронных документов, содержащих сведения, составляющие государственную тайну, или в информационной системе, содержащей сведения, составляющие государственную тайну, не допускается.

Кроме того, в соответствии со статьей 312.1 ТК РФ (гл. 49.1 Особенности регулирования труда дистанционных работников) для подписания электронного трудового договора стороны должны использовать исключительно квалифицированную электронную подпись. Для подтверждения ознакомления с приказом о приеме на работу, правилами внутреннего трудового распорядка, иными документами в электронном виде, сотрудник так же должен использовать только усиленную квалифицированную электронную подпись. Документы, касающиеся трудовых отношений с дистанционным работником (приказ о приеме на работу, правила внутреннего трудового распорядка, приказы о прекращении трудового договора, о переводе, листок временной нетрудоспособности и т.д.), все равно оформляются в бумажном виде. Просто делается копия этих документов в электронной форме, которая заверяется квалифицированной электронной подписью работодателя и направляется дистанционному работнику на ознакомление. Именно эту копию работник и подписывает своей электронной подписью.

Изменения в трудовой договор и любые документы, требующие подписи и печати работодателя, не могут быть подписаны посредством ПЭП.

Из вышеизложенных норм закона, можно сделать следующий вывод по вопросу применения ПЭП:

Простые подписи создаются с помощью кодов, паролей и других инструментов, которые позволяют идентифицировать автора документа, но не позволяют проверить его на предмет наличия изменений с момента подписания. ПЭП, в отличие от прежней электронно-цифровой подписи, не предназначена для защиты документа от подделки. Она не позволяет обнаружить возможное искажение содержания документа. Единственная ее функция — подтверждение факта формирования электронной подписи (а не самого документа!) определенным лицом. Целям определения лица, подписавшего электронный документ, а также обнаружения факта внесения изменений в документ после его подписания служит усиленная электронная подпись. Именно эта подпись (в двух видах — неквалифицированная и квалифицированная) является аналогом прежней электронной цифровой подписи. Поэтому *«простую электронную подпись безопаснее использовать только в случае доверительных отношений с партнером по бизнесу. Из перечисленных трех подписей эта подпись наименее защищенная.»*(с)

Проанализировав на соответствие закону Регламент применения простой электронной подписи в комплексной информационной системе «Аккорд» (далее – Регламент) с учетом того, что создателем в лице Савина В.С., и, скорей всего, собственником КИС является ОАО «Аэрофлот» хотим отметить, что в нем содержится большое количество не раскрытых вопросов, «подводных камней», которые могут негативно отразиться в будущем на работнике при его желании защитить свои права, в том числе в суде.

Возможно, мы ошибаемся в своих выводах и, как сказал на форуме AFLCREW замКЛО Влад Иванов, – *«Позиция нашего профсоюза ясна – исчезает возможность дергать отряд, а значит популярность может снизиться.* – поскольку, – *Конечно удобнее профсоюзу, чтобы 1000 пилотов отряда ВС А 320 ЕЖЕМЕСЯЧНО ездили подписывать график полетов в ЛК. Ведь всегда в этом случае можно прокуратуру или инспекцию натравить...»* –, но тем, кто подписал соглашение о дополнении (изменении) к трудовому договору (контракту) о признании своей ЭП собственноручной подписи на бумажном носителе, или собирается его подписать стоит обратить внимание на следующие моменты:

1) Исходя из вышеизложенных норм закона, ПЭП только подтверждает авторство документа, но не обеспечивает целостность документа и не может подтвердить подлинность или идентичность документа.

В связи с чем указание на эти функции в пункте 1.3 и разделе 2 Регламента и их соблюдение остается только на совести работодателя (а есть ли у него совесть?).

Кроме того, в законе не предусмотрено требование «неотрицание авторства» (раздел 2 Регламента) – требование неотрекаемости, то есть невозможности в последующем для лица, сформировавшего подпись, отказаться от своей подписи. В литературе, по данному вопросу приведен пример, почему возможность подтвердить факт формирования подписи не препятствует в дальнейшем отказу от нее.

Пример из литературы по данному вопросу: «Предположим, что вы сообщили некоему лицу секретный пароль и договорились, что данный пароль не может быть разглашен ни при каких условиях. Затем это лицо передает вам лично документ, содержащий указанный секретный пароль. В этом случае вы можете определить лицо, подписавшее документ секретным паролем, но не сможете доказать в суде, что данный документ подписал паролем этот человек. Это связано с тем, что вы также знали данный пароль и, соответственно, могли его использовать для подписи документа. Кроме того, если речь идет об электронном документе, то вы могли произвольным образом исказить полученный документ. И, соответственно, ваш корреспондент может утверждать, что на самом деле он подписал совершенно другой документ, а вы не сможете доказать обратное. То есть, мы имеем пример простой подписи, которая не выполняет привычные функции собственноручной подписи, а именно, не обеспечивает невозможность отказа от подписанного документа. Примером такой ситуации в жизни является широко распространенная практика использования разовых паролей для подтверждения платежных операций в системах дистанционного банковского обслуживания. Установив со своим клиентом защищенный канал связи и получив подтверждение операции использованием разового пароля, банк может уверен, что платеж подтвержден именно этим лицом. Но ни банк, ни клиент не имеют электронного документа, который можно было бы предъявить третьему лицу и доказать, что данное платежное поручение подписал простой подписью именно клиент.».

2) Информация в электронной форме и сама ПЭП находятся в системе документооборота КИС «Аккорд», подконтрольной работодателю. Нет гарантий, что в удобные для работодателя моменты он не будет вносить изменения в уже подписанные вами документы (локальные акты, графики, менять дату ознакомления).

Кроме того, в силу ненадежности простой электронной подписи помимо работодателя изменения в электронные документы могут быть внесены и со стороны третьих лиц (например, нанятых квалифицированных системных администраторов – хакеров).

3) В Регламенте не раскрывается понятие *закрытого ключа*, порядок его выдачи и хранения на отчуждаемых носителях. При этом данное понятие имеет важное значение и должно быть установлено. Оно определено, к примеру, в соглашениях об электронном обмене данными Банк-Клиент.

Вот одно из наиболее понятных определений, которое удалось нам найти в Интернете:

Закрытый ключ ЭЦП – это уникальная последовательность символов, которая известна только его владельцу. При помощи *закрытого ключа электронной цифровой подписи* можно создавать ЭЦП в электронных документах, используя специальные программные средства. Закрытый ключ ЭЦП выдается участнику информационной системы вместе с сертификатом открытого ключа ЭЦП. Невозможность подделки электронного документа и электронной цифровой подписи может быть обеспечена только при условии содержания *закрытого ключа ЭЦП* в тайне. Закрытый ключ всегда идет в паре с **открытым ключом ЭЦП**, при помощи которого можно удостовериться в подлинности электронной цифровой подписи. Основным назначением закрытого ключа ЭЦП является создание его владельцем своей электронной цифровой подписи в электронных документах, т.е. их подписание. Кроме того, т.к. электронную подпись можно создать, только воспользовавшись закрытым ключом ЭЦП, то, соответственно, можно доказать свое авторство подписи под документом, и, в то же время, нельзя отказаться от своей подписи.

4) Один из важных недочетов Регламента – это отсутствие четкого перечня электронных документов, которые будут подписываться посредством ПЭП (пункты 1.2 и 3.1). Таким образом, подписывается соглашение без ключевого объекта регулирования.

5) Пунктом 3.7 Регламента установлены сроки ознакомления с документами, но не предусмотрены санкции за нарушение сроков ознакомления. При этом ТК РФ не предусматривает конкретных сроков для ознакомления с актами работодателя.

Поскольку присоединение к данному регламенту осуществляется путем подписания дополнительного соглашения к трудовому договору, возникает вопрос: может ли расцениваться пропуск указанных выше сроков как нарушение работником своих трудовых обязанностей, дающее основание для применения к нему со стороны работодателя дисциплинарного взыскания? Кроме того, пунктом 3.7 установлено, что период ознакомления начинается с момента опубликования электронного документа, а не с момента ВАШЕГО уведомления о публиковании документа. Вместе с тем, во вторник и четверг вы в обязательном порядке должны сами узнавать о размещении в системе электронных документов. А что будет если работник не позвонил, в том числе, по объективном причинам? Каждый ли вспомнит об этом, учитывая загруженность работы? А если ему не пришло SMS или оповещение по средством e-mail, и он не узнал о размещении документов? Нарушение условия трудового договор – дисциплинарное взыскание? Суд?

Также, стоит обратить внимание, что локальные акты имеют зачастую большой объем, и в силу своей загруженности члены летных экипажей могут физически не успеть в установленные сроки ознакомиться с актами. Опять же возникает вопрос санкций?

6) Абсурд положения пункта 3.9 Регламента: *«Оператор системы обеспечивает защиту... Оператором системы является владелец КИС «Аккорд»*, т.е. – Аэрофлот. Таким образом, все находится под контролем работодателя.

Никому не надо рассказывать, что и раньше информация в Аккорде постоянно таинственным образом менялась, особенно наряды и табели учета рабочего времени.

При возникновении трудовых споров в суде, и в том числе при направлении жалоб в инспекцию труда, не факт, что у вас на руках будут доказательств ваших требований, то есть редакция тех актов, с которыми вы знакомились и вообще акт с вашей подписью, поскольку информация доступна только для участников информационной системы.

Также стоит отметить, что порядок, в соответствии с которым можно будет использовать электронные документы в судах, пока на законодательном уровне в полной мере не урегулирован. В ГПК (ст. 71) и АПК (ст. 75) лишь существуют нормы о том, что в качестве письменных доказательств могут использоваться электронные документы. При этом, судебная практика применения в качестве письменных доказательств документов, подписанных электронной подписью минимальная, принимая во внимание то, что зачастую и бумажных носителей оказывается недостаточно!

7) Пункт 3.18 Регламента говорит о том, что время подписи фиксируется КИС «Аккорд». То есть при наличии возможности изменения администратором информационной системы Аккорд даты подписания (ознакомления) документа, у работника могут возникнуть проблемы. Статьей 392 ТК РФ определено, что работник имеет право обратиться в суд за разрешением индивидуального трудового спора в течение трех месяцев со дня, когда он узнал или должен был узнать о нарушении своего права, а по спорам об увольнении – в течение одного месяца со дня вручения ему копии приказа об увольнении либо со дня выдачи трудовой книжки.

Таким образом, существует реальная возможность пропуска сроков обращения в суд за защитой своих прав.

8) В пункте 3.16 Регламента указано, что подписанию ЭП в КИС «Аккорд» подлежат *основные реквизиты* и *содержание документа*. Слово «содержание» может толковаться двусмысленно. По словарю Ушакова «содержание» – это (*одно из значений*) то, о чем рассказывается или говорится, тема, основной смысл, сущность изложения.

То есть читая данный пункт дословно, он может пониматься так, что работодатель не обязан представлять полный текст документа, при этом работодатель будет указывать, что работник был ознакомлен со всем текстом документа. И вашу неосведомленность ещё нужно будет доказать в суде, при необходимости конечно.

9) В Регламенте не предусмотрено, кто входит в комиссию по разбору конфликтных ситуаций. Если она будет состоять только из представителей работодателя, то на объективность данной комиссии можно не рассчитывать. Исходя из положений Регламента и закона, «бремя доказывания» так называемых авторства, целостности и подлинности электронного документа лежит на работнике.

Это те немногие моменты, на которые мы хотели бы обратить внимание членов летных экипажей при принятии ими решения о присоединении к Регламенту.

В заключении хотим отметить, что применение электронного документооборота и электронных подписей, в частности, в организации это прогрессивно и удобно, экономит, возможно, время работников и, точно, время кадровых служб работодателя. Мы поддерживаем эту инициативу ОАО «Аэрофлот – РА» и нашей целью не стоит как-то навредить руководству компании. Просто данные действия работодателя должны соответствовать закону, не ущемлять интересы работников и не нарушать их прав.

Считаем, что Регламент требует доработки, а сама система «Аккорд» должна контролироваться не только работодателем. К сожалению, руководство ОАО «Аэрофлот» несколько лет назад лишило органы РОО «ШПЛС» пропусков на территорию работодателя, а также непосредственно доступа к КИС «Аккорд», и у нас нет возможности отслеживать издание локальных актов работодателя и проверять их легитимность.

В связи с изложенным, повторно советуем не подписывать дополнительные соглашения к трудовому договору о признании своей ЭП собственноручной подписи на бумажном носителе договору и присоединении к Регламенту в существующей редакции.

РОО «ШПЛС»

Учредитель: Президиум Шереметьевского профсоюза летного состава
Телефон: (495) 995-16-78;
Адрес редакции: 141426, М.О., Химкинский р-н, А/п «Шереметьево-1», БЦ «Аэро-Плаза», оф. 509
Сайт ШПЛС: www.шплс.рф E-mail: shpls@mail.ru