МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
(РОСЖЕЛДОР)

ПРИКАЗ

16 октября 2017г. **Москва** **№** 395

Об утверждении Требований и мер по обеспечению безопасного режима эксплуатации средств криптографической защиты информации и назначении администратора безопасности

Во исполнение Федеральным агентством железнодорожного транспорта Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», приказа ФАПСИ 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», Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных 8м центром ФСБ России от 21.02.2008 №149/6/6-622, в соответствии с подпунктом 9.9 Положения о Федеральном агентстве железнодорожного транспорта, утвержденного постановлением Правительства Российской Федерации от 30.07.2004 № 397 **п р и к а з ы в а ю:**

1. Назначить администратором безопасности АПКШ начальника отдела информатизации федерального казенного учреждения «Управление служебных зданий федеральных органов исполнительной власти в области транспорта» Г.Г. Блинова.
2. Утвердить и ввести в действие Требования и меры по обеспечению безопасного режима эксплуатации аппаратно-программных комплексов шифрования (АПКШ) в Федеральном агентстве железнодорожного транспорта.
3. Утвердить и ввести в действие Руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи в Федеральном агентстве железнодорожного транспорта (далее – Руководство).
4. Утвердить и ввести в действие Форму журнала поэкземплярного учета средств криптографической защиты информации и ключевых носителей в центральном аппарате Федерального агентства железнодорожного транспорта.
5. Администратору информационной безопасности Г.Г. Блинову:

5.1. Ознакомить сотрудников Росжелдора, использующих в своей работе электронные подписи и средства электронной подписи, с настоящим приказом и утвержденным Руководством под расписку.

5.2. Обеспечить ведение журнала поэкземплярного учета средств криптографической защиты информации и ключевых носителей в центральном аппарате Федерального агентства железнодорожного транспорта.

6. Контроль за исполнением настоящего приказа возложить на заместителя руководителя Росжелдора, курирующего вопросы информатизации Росжелдора.

Руководитель В.Ю. Чепец

Г.Г. Блинов, ФКУ УСЗ
(499) 262-35-36

УТВЕРЖДЕНО
приказом Росжелдора
от 16.10.2017 № 395

Требования и меры по обеспечению безопасного режима эксплуатации аппаратно-программных комплексов шифрования (АПКШ) в Федеральном агентстве железнодорожного транспорта

1. Общие положения

1.1. Настоящие Требования определяют порядок организации и обеспечения функционирования средств криптографической защиты информации (далее – СКЗИ) аппаратно-программных комплексов шифрования (далее – АПКШ), предназначенных для защиты информации, содержащей персональные данные, при обработке её (информации) в государственных информационных системах.

1.2. АПКШ, используемые в Федеральном агентстве железнодорожного транспорта (Росжелдор), имеют централизованное управление. Управление АПКШ осуществляет федеральное казенное учреждение «Управление служебных зданий федеральных органов исполнительной власти в области транспорта». Управление осуществляется в соответствии с эксплуатационной документацией АПКШ.

1.3. Настоящие Требования содержат базовый набор мероприятий по обеспечению условий использования АПКШ, предусмотренных эксплуатационной и технической документацией к ним, который может быть адаптирован с учетом фактических условий эксплуатации.

1.4. Настоящие Требования основываются на:

– Приказе 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»;

– Типовых требованиях по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные 8-м центром ФСБ России от 21.02.2008 №149/6/6-622.

2. Требования к размещению АПКШ

2.1. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены АПКШ или хранятся ключевые документы к ним, должны обеспечивать сохранность персональных данных, СКЗИ и ключевых документов к ним. В указанных помещениях должна быть исключена возможность неконтролируемого (несанкционированного) проникновения и пребывания в них посторонних лиц.

2.2. В случае размещения указанных помещений на первом и последнем этажах здания, а также при наличии вблизи окон данного помещения

вспомогательных построек, пожарных лестниц, водосточных труб и т.д., оконные проемы должны быть оборудованы металлическими решетками или ставнями, охранной сигнализацией или другими средствами, препятствующими неконтролируемому проникновению посторонних лиц в помещения.

2.3. В помещениях, предназначенных для хранения носителей информации, ключевых документов АПКШ, эксплуатационной и технической документации, инсталлирующих носителей с программным обеспечением для АПКШ необходимо иметь надежно запираемый шкаф (ящик, хранилище) индивидуального пользования, оборудованный приспособлением для опечатывания. Ключи от этого хранилища должны находиться у действующего администратора безопасности АПКШ. Необходимо предусмотреть раздельное безопасное хранение действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих ключевых документов.

3. Порядок допуска к самостоятельной работе с АПКШ

3.1. Эксплуатация АПКШ должна осуществляться администратором безопасности, назначенным приказом руководителя Росжелдора.

3.2. К работе с АПКШ допускаются лица, назначенные администраторами безопасности и:

- ознакомленные под подпись с настоящими Требованиями;
- ознакомленные с требованиями действующих нормативно-правовых актов в части обеспечения безопасности персональных данных, определяющими порядок использования СКЗИ;
- изучившие эксплуатационно-техническую документацию АПКШ.

4. Порядок обращения с АПКШ и ключевыми документами к нему

4.1. Администратор безопасности осуществляет хранение инсталлирующих носителей с программным обеспечением для АПКШ, эксплуатационной и технической документации к АПКШ, ключевых документов в шкафах (ящиках, хранилищах и т.п.) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним.

4.2. Администратор безопасности ведет журнал учета выполнения работ с АПКШ. В журнале регистрируются работы, связанные с установкой, переустановкой, обновлением программного обеспечения, изменением конфигурации, плановым обслуживанием АПКШ. Форма журнала учета выполнения работ с АПКШ приведена в Приложении № 1.

4.3. АПКШ должен быть оборудован визуальными средствами контроля от вскрытия (опечатан, опломбирован).

4.4. Выполнение работ по вводу в эксплуатацию АПКШ оформляется соответствующим актом.

4.5. В случае увольнения администратора безопасности АПКШ, в организации приказом назначается новый администратор безопасности, ответственный за эксплуатацию АПКШ и проводится внеплановая смена ключевой информации.

5. Порядок уничтожения ключевых документов АПКШ

5.1. Выведенные из действия ключевые документы уничтожаются в срок не позднее 3 рабочих дней после получения новых ключей. Факт уничтожения отражается в журнале учета работ с АПКШ.

5.2. Уничтожением ключевого документа считается физическое уничтожение соответствующего ключевого носителя, исключающее возможность его дальнейшего использования и восстановления ключевой информации, или стирание криптоключей без повреждения ключевого носителя многократного использования.

5.3. Ключевые документы уничтожаются Администратором безопасности в случае стирания криптоключей с обязательной отметкой в журнале учета работ с АПКШ, либо с оформлением акта при физическом уничтожении ключевых документов.

6. Компрометация криптоключей

6.1. Компрометация криптоключей – утрата доверия к тому, что используемые (хранимые) криптоключи стали доступны неопределенному кругу лиц, не имеющим к ним доступ.

6.2. К случаям компрометации криптоключей относятся:

- утрата ключевых документов;
- утрата ключевых документов с последующим обнаружением;
- увольнение сотрудников, имевших доступ к ключевой информации;
- возникновение подозрений на утечку информации или ее искажение при хранении и передаче по каналам связи;
- нарушение целостности печатей на шкафах (ящиках, хранилищах и т.п.) с ключевыми документами;
- ключевые документы стали на время доступными постороннему лицу без контроля со стороны Администратора безопасности.

6.3. При компрометации ключевой информации Администратор безопасности обязан:

- прекратить передачу информации с использованием АПКШ;
- доложить о случившемся руководителю организации;
- произвести внеплановую смену ключевой информации.

Приложение №1
к требованиям и мерам по обеспечению безопасного режима эксплуатации аппаратно-программных комплексов шифрования (АПКШ)

Типовая форма журнала учета выполнения работ с АПКШ

Дата проведения	Наименование работ	Основание	Фамилия и подпись администратора, выполнившего работу	Примечание

УТВЕРЖДЕНО
приказом Росжелдора
от 16.10.2017 № 395

Руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи

1. Общие положения

1.1. Настоящее руководство разработано в соответствии с требованиями Федерального закона от 06.04.2011 №63-ФЗ «Об электронной подписи» и предназначено для лиц, заинтересованных в получении или владеющих сертификатом ключа проверки электронной подписи.

1.2. Руководство является средством информирования об условиях, рисках и порядке использования электронной подписи и средств электронной подписи (далее – средства ЭП), а также о мерах, необходимых для обеспечения безопасности при использовании электронной подписи.

1.3. Применение электронной подписи в государственных и иных информационных системах, а также в системах юридически значимого электронного документооборота, сопровождаются в том числе следующими рисками:

- финансовые убытки (в том числе штрафы и т.п.);
- репутационные риски;
- нарушение сроков оказания государственных и муниципальных услуг;
- нарушение правильного функционирования информационных систем.

1.4. Риски, связанные с применением электронной подписи, возникают вследствие возможности признания недействительности сделок, совершенных с использованием электронной подписи, недействительности документов, подписанных электронной подписью при несанкционированном получении злоумышленником ключа электронной подписи или несанкционированного использования рабочего места пользователя, на котором осуществляется выработка электронной подписи.

1.5. В целях снижения рисков необходимо выполнение приведенных в настоящем руководстве организационно-технических и административных мер по обеспечению безопасного функционирования средств обработки и передачи информации.

1.6. В соответствии с правилами функционирования информационных систем и систем обмена электронными документами, а также требованиями по эксплуатации средств ЭП могут быть установлены дополнительные требования по обеспечению их безопасной эксплуатации.

2. Требования к организации режима обеспечения безопасности помещений, в которых эксплуатируются средства электронной подписи

2.1. При эксплуатации средств ЭП должны быть реализованы меры, препятствующие возможности неконтролируемого проникновения или пребывания

в помещениях, где размещены (или хранятся) используемые средства ЭП и (или) носители ключевой, аутентифицирующей и парольной информации средств ЭП (далее – Помещения), лиц, не имеющих права доступа в Помещения. Указанные меры могут быть реализованы, в том числе, путем:

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

– утверждения правил доступа в Помещения в рабочее и нерабочее время, а также в нештатных ситуациях;

– утверждения перечня лиц, имеющих право доступа в Помещения.

2.2. В случае необходимости присутствия посторонних лиц в Помещениях должен быть обеспечен контроль за их действиями во избежание негативных воздействий с их стороны на средства электронной подписи, средства обработки информации и передаваемую информацию.

2.3. Внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им документов и сведений, включая ключи электронной подписи.

3. Требования по защите информации от несанкционированного доступа средств электронной подписи, общесистемного и специального программного обеспечения

3.1. При использовании средств ЭП должны выполняться следующие меры по защите информации от несанкционированного доступа:

3.1.1. Необходимо разработать и применить политику назначения и смены паролей (для входа в операционную систему, BIOS и т.д.) в соответствии со следующими правилами:

– длина пароля должна быть не менее 8 символов;

– в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

– пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, номера телефонов, даты рождения и т.д.), а также сокращения (USER, ADMIN, root, и т.д.);

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

– личный пароль пользователь не имеет права никому сообщать;

– периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 90 календарных дней.

3.1.2. При использовании ключей электронных подписей средства вычислительной техники должны быть сконфигурированы с учетом следующих требований:

– не использовать нестандартные, измененные или отладочные версии операционных систем;

– исключить возможность загрузки и использования операционной системы, отличной от предусмотренной штатной работой;

– исключить возможность удаленного управления, администрирования и модификации операционной системы и ее настроек;

– на средствах вычислительной техники с установленными средствами ЭП должна быть установлена только одна операционная система;

– все неиспользуемые сетевые компоненты системы необходимо отключить (протоколы, сервисы и т.п.);

– режимы безопасности, реализованные в операционной системе, должны быть настроены на максимальный уровень;

– всем пользователям и группам, зарегистрированным в операционной системе, необходимо назначить минимально возможные для нормальной работы права;

– необходимо предусмотреть меры, максимально ограничивающие доступ к ресурсам системы (в соответствующих условиях возможно полное удаление ресурса или его неиспользуемой части):

- системному реестру;
- файлам и каталогам;
- временным файлам;
- журналам системы;
- файлам подкачки;
- кэшируемой информации (пароли и т.п.);
- отладочной информации.

3.1.3. На средствах вычислительной техники необходимо:

– организовать стирание (по окончании сеанса работы средств электронной подписи) временных файлов и файлов подкачки, формируемых или модифицируемых в процессе их работы. Если это невыполнимо, то на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям;

– исключить попадание в систему программ, позволяющих использовать ошибки операционной системы, для повышения предоставленных привилегий;

– регулярно устанавливать пакеты обновлений безопасности операционной системы, обновлять антивирусные базы, а также исследовать информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий.

3.1.4. В случае подключения технических средств с установленными средствами ЭП к общедоступным сетям передачи данных необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов, полученных с ресурсов или с использованием общедоступных сетей передачи данных (в т.ч. Интернет), без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети. С целью исключения возможности несанкционированного доступа к системным ресурсам используемых операционных систем к программному обеспечению, в окружении которого функционируют средства ЭП и к компонентам средств ЭП со стороны указанных

сетей, должны использоваться дополнительные методы и средства защиты (например: установка межсетевых экранов, организация VPN-сетей и т.п.). Все средства защиты, должны иметь сертификат уполномоченного органа по сертификации средств защиты.

3.1.5. Необходимо организовать и использовать:

- систему аудита, организовать регулярный анализ результатов аудита;
- комплекс мероприятий по антивирусной защите.

3.2. Запрещается:

- осуществлять несанкционированное копирование ключевых носителей;
- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и иные средства отображения информации;
- использовать ключевые носители в режимах, не предусмотренных штатным режимом использования ключевого носителя;
- вносить какие-либо изменения в программное обеспечение средств ЭП;
- работать со средствами электронной подписи при включенных в техническое средство штатных средствах выхода в радиоканал;
- записывать на ключевые носители постороннюю информацию;
- оставлять средства вычислительной техники с установленными средствами ЭП без контроля после ввода ключевой информации;
- использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, который аннулирован, действие которого прекращено или приостановлено;
- удалять ключевую информацию с ключевого носителя до истечения срока действия, аннулирования или прекращения действия сертификата ключа проверки электронной подписи.

4. Требования по обеспечению информационной безопасности при обращении с носителями ключевой информации, содержащими ключи электронной подписи

4.1. Меры защиты ключей электронной подписи Ключи электронной подписи при их создании должны записываться на типы ключевых носителей, которые поддерживаются используемым средством ЭП согласно технической и эксплуатационной документации к ним.

Ключи электронной подписи на ключевом носителе должны быть защищены паролем (ПИН-кодом). При этом пароль (ПИН-код) формирует лицо, выполняющее процедуру создания ключей, в соответствии с требованиями на используемое средство ЭП.

Ответственность за конфиденциальность сохранения пароля (ПИН-кода) возлагается на владельца ключа электронной подписи.

4.2. Обращение с ключевой информацией и ключевыми носителями

Недопустимо пересылать файлы с ключевой информацией для работы в системах обмена электронными документами, по электронной почте в сети

Интернет или по внутренней электронной почте (кроме файлов квалифицированных сертификатов ключей проверки электронной подписи).

Ключевая информация должна размещаться на сменном носителе информации (floppy-диск, USBflash накопитель, e-Token, Рутокен, ESMART Token и др.). Размещение ключевой информации в реестре Windows, на локальном или сетевом диске, а также во встроенной памяти технического средства с установленными средствами ЭП, способствует реализации многочисленных сценариев совершения мошеннических действий злоумышленниками.

Носители ключевой информации должны использоваться только их владельцем либо уполномоченным лицом на использование данного носителя, и храниться в месте не доступном третьим лицам (сейф, опечатываемый бокс, закрывающийся металлический ящик и т.д.).

Носитель ключевой информации должен подключаться в считывающее устройство только на время выполнения средствами электронной подписи операций формирования и проверки электронной подписи, шифрования и дешифрования. Размещение носителя ключевой информации в считывателе на продолжительное время существенно повышает риск несанкционированного доступа к ключевой информации третьими лицами.

На носителе ключевой информации недопустимо хранить иную информацию (в том числе рабочие или личные файлы).

4.3. Обеспечение безопасности средств вычислительной техники с установленными средствами ЭП

С целью контроля исходящего и входящего подозрительного трафика, средства вычислительной техники с установленными средствами ЭП должны быть защищены от внешнего доступа программными или аппаратными средствами межсетевого экранирования. Эти средства должны пресекать отправку во внешние сети информации, инициированную программами, не имеющими соответствующих полномочий.

На технических средствах, используемых для работы в системах обмена электронными документами:

- на учетные записи пользователей операционной системы должны быть установлены пароли, удовлетворяющие требованиям, приведенным в разделе 3;
- должно быть установлено только лицензионное программное обеспечение;
- должно быть установлено лицензионное антивирусное программное обеспечение с регулярно обновляемыми антивирусными базами данных;
- должны быть отключены все неиспользуемые службы и процессы операционной системы Windows (в т.ч. службы удаленного администрирования и управления, службы общего доступа к ресурсам сети, системные диски и т.д.);
- должны регулярно устанавливаться обновления операционной системы;
- должен быть исключен доступ (физический и/или удаленный) к техническим средствам с установленными средствами ЭП третьих лиц, не имеющих полномочий для работы в системе обмена электронными документами;
- должна быть активирована подсистема регистрации событий информационной безопасности;

– должна быть включена автоматическая блокировка экрана после ухода ответственного сотрудника с рабочего места.

В качестве автоматизированного рабочего места для работы в системах обмена электронными документами крайне не рекомендуется выбирать переносной компьютер (ноутбук, планшет). Если выбран переносной компьютер, недопустимо его подключение к сетям общего доступа в местах свободного доступа в Интернет (Интернет-кафе, гостиницы, офисные центры и т.д.), при этом для хранения ключевой информации должен использоваться сменный носитель информации.

В случае передачи (списания, сдачи в ремонт) сторонним лицам технических средств, на которых были установлены средства ЭП, необходимо гарантированно удалить всю информацию (при условии исправности технических средств), использование которой третьими лицами может потенциально нанести вред организации, в том числе средства ЭП, журналы работы систем обмена электронными документами и т.д.).

5. Действия при компрометации ключей электронной подписи

5.1. К событиям, относящимся к компрометации ключей электронной подписи, относятся следующие ситуации:

– ознакомление неуполномоченного лица (лиц) с ключами электронной подписи;

– утрата ключевого носителя с ключами электронной подписи;

– увольнение пользователя ключа электронной подписи;

– нарушение целостности печатей на сейфах (шкафах, хранилищах), предназначенных для хранения ключевых носителей;

– утрата ключей от сейфов (шкафов, хранилищ) в случае нахождения в них ключевых носителей;

– случаи, когда невозможно достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника, утрата ключевого носителя с последующим обнаружением).

5.2. В случае компрометации ключей электронной подписи владелец квалифицированного сертификата ключа проверки электронной подписи должен:

1) прекратить использование ключа электронной подписи и соответствующего квалифицированного сертификата ключа проверки электронной подписи;

2) незамедлительно обратиться к администратору безопасности для аннулирования (прекращения действия) соответствующего сертификата ключа проверки электронной подписи и получения (при необходимости) нового сертификата ключа проверки электронной подписи.

УТВЕРЖДЕНО
приказом Росжелдора
от 16.10.2017 № 395

Журнал
поэкземплярного учета средств криптографической защиты информации и ключевых носителей в центральном аппарате Федерального агентства железнодорожного транспорта

Ответственный _____ _____ _____
(Должность) (Подпись) (ФИО)

Начат «____» _____ 20__ г.
Завершен «____» _____ 20__ г.

На _____ листах

№ п/п	Наименование СКЗИ	Регистрационный номер СКЗИ	Отметка о получении		Отметка о выдаче	
			От кого получены	Дата и номер сопроводи-тельного письма	Ф.И.О. пользователя СКЗИ, производившего подключение (установку)	Дата подключения (установки) и подписи лиц, Произведших подключение (установку)
1	2	3	4	5	6	7

Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств ИСПДН			Примечание
Ф.И.О. пользователя СКЗИ, производившего 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. пользователя СКЗИ, производившего Изъятие (уничтожение)	Номер акта или расписка об уничтожении	
8	9	10	11	12	13	14

595

РЕГИСТРАЦИОННО-КОНТРОЛЬНАЯ КАРТОЧКА

Регистрационный номер	Дата регистрации

Подписант	Исполнитель
Чепец Владимир Юрьевич, Росжелдор, Руководство, Руководитель	Блинов Г. Г., Начальник отдела

Вид документа	Категория срочности	Количество листов основного документа
Приказ		2

Краткое содержание

Об утверждении Требований и мер по обеспечению безопасного режима эксплуатации средств криптографической защиты информации и назначении администратора безопасности

Согласование

Плановая дата	Фактическая дата	Комментарии
11.10.2017	12.10.2017	

Визирование

Номер итерации	Порядковый номер	Действие	Фактический согласующий	Согласующий	Дата	Решение
1	4	Согласен	Загубный Юрий	Беспалов Андрей	12.10.2017 15:17	Согласен
1	4	В АРМ руководителю	Зимина Елена	Беспалов Андрей	11.10.2017 13:46	
1	3	Согласен	Меркулов Георгий	Меркулов Георгий	11.10.2017 11:51	Согласен
1	3	В АРМ руководителю	Карташёва Нина	Меркулов Георгий	09.10.2017 14:41	
1	2	Согласен	Белов Евгений	Белов Евгений	09.10.2017 13:57	Согласен
1	2	В АРМ руководителю	Семёновых Маргарита	Белов Евгений	09.10.2017 11:55	
1	1	Согласен	Казимир Евгений	Степняк Евгений	06.10.2017 14:10	Согласен

Подписание

Номер итерации	Порядковый номер	Действие	Фактический подписант	Подписант	Дата	Решение

Ознакомление

Резолюции и исполнение

Бумажный оригинал

Хранение документа

Номер тома	Комната\Стеллаж\Полка	Комментарий
0		

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
РАССЫЛКА СЛУЖЕБНЫХ ДОКУМЕНТОВ

приказ (наименование документа) от 16.10.2017 (дата) № 395 (исходящий номер)

Документ на 2 листах, приложение на _____ листах

№	Наименование адресатов	Кол-во экз. № экз.	Расписка в получении
1	Руководитель Агентства: **Чепец В.Ю.** **(ВЧ)**		
2	Заместители руководителя Агентства:		
	Луковников Е.В. **(ЕЛ)**		
3	Помощники руководителя и заместителей руководителя Агентства:		
	Попов Д.		
	Девятьярова А.Ю.		
4	**Административно-кадровое управление (АКУ)** **(Беспалов А.М.)**		
4.1	Отдел кадров и государственной службы		
4.2	Организационно-протокольный отдел		
4.3	Отдел документационного обеспечения и архивов	2	
5	**Управление транспортной безопасности (УТБ)** **(Егоренков Ю.В.)**		
5.1	Отдел оценки уязвимости и категорирования		
5.2	Отдел по работе с планами по обеспечению транспортной безопасности		
5.3	Отдел координации, анализа и прогнозирования		
6	**Управление экономики и финансов (УЭФ)** **(Зяблицкий И. Ю.)**		
6.1	Отдел финансов		
	Отдел бухгалтерского учета		
6.2	Отдел реализации инвестиционных программ		
6.3	Отдел экономики и федерального имущества		
7	**Управление учебных заведений и правового обеспечения (УУП) (Г.В.Меркулов)**	2	
7.1	Отдел правовой экспертизы и применения законодательства		
7.2	Отдел имущественных отношений и территориального планирования		
7.3	Отдел учебных заведений		
8	**Управление инфраструктуры и перевозок (УИП) (Шпади Д.В.)**		
8.1	Отдел перевозок		
8.2	Отдел инфраструктуры и технических средств		
8.3	Отдел по работе с пользователями услуг железнодорожного транспорта		
9	**Отдел мобилизационной подготовки (Кондрашов В.В.)**		
10	**Первый отдел**		
11	ФГП « Единая группа заказчика Федерального агентства железнодорожного транспорта»		
12	ФГП « Ведомственная охрана железнодорожного транспорта России (ФГП ВО ЖДТ России)		
13	ФКУ УСЗ **(Е.В.Белов)**	1	
14	Регистр сертификации на Федеральном ж.д.транспорте **(Гунченко Э.Н.)**		
15	Территориальные управления		
16	Высшие учебные заведения		
17	Средние специальные учебные заведения ж.-д. транспорта		
18	ФГБОУ «УМЦ ЖДТ» **(Старых О.В.)**		
	ИТОГО:	5	

Начальник управления,
Зам. нач. управления, нач. отдела _____ Винов В.Г.