МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
(РОСЖЕЛДОР)

П Р И К А З

16.11.2017 **Москва** **№** 446

Об утверждении Требований по подключению к государственным информационным системам Федерального агентства железнодорожного транспорта

Во исполнение Федеральным агентством железнодорожного транспорта (Росжелдор) п. 4 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 № 17, в соответствии с п.п. 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. Утвердить Требования по подключению к государственным информационным системам Федерального агентства железнодорожного транспорта (далее – Требования по подключению к ГИС Росжелдора).

2. Федеральному казенному учреждению «Управление служебных зданий федеральных органов исполнительной власти в области транспорта» (Е.В. Белову):

2.1. Предусматривать в заключаемых договорах обязанность лиц, обрабатывающих информацию, являющуюся государственным информационным ресурсом, обладателем (заказчиком) или оператором которой является Росжелдор, по поручению Росжелдора обеспечивать защиту информации в соответствии с законодательством Российской Федерации об информации, информационных технологиях и о защите информации, Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 № 17, и Требованиями по подключению к ГИС Росжелдора.

2.2. Обеспечивать подключение территориальных органов, подведомственных, подрядных организаций Росжелдора и иных организаций к государственным информационным системам Росжелдора в соответствии с р. 6 Требований по подключению к ГИС Росжелдора.

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

Руководитель В.Ю. Чепец

УТВЕРЖДЕНО
приказом Росжелдора
от 16.11.2017 № 446

Требования по подключению к государственным информационным системам Федерального агентства железнодорожного транспорта

1. Общие положения

Технические и организационные меры по защите информации на автоматизированных рабочих местах (далее – АРМ), на которых необходим доступ к государственным информационным системам (далее – ГИС) Федерального агентства железнодорожного транспорта (Росжелдор) разработаны на основании следующих руководящих документов:

- Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказа ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- Приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Методического документа «Меры защиты информации в государственных информационных системах», утвержденного ФСТЭК России 11.02.2014;
- «Методических рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утвержденных руководством 8 центра ФСБ России 21.02.2008 № 149/5-144;
- «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 руководством 8 центра ФСБ России 21.02.2008 № 149/6/6-622.

2. Назначение и состав ГИС Росжелдора

Все ГИС Росжелдора представляют собой совокупность персонала, информационных технологий, технических средств и средств автоматизации.

ГИС Росжелдора, в которых обрабатываются персональные данные, аттестованы по 3 классу защищенности информационных систем и 4 уровню защищенности персональных данных.

Для информационных систем 3 класса защищённости меры защиты информации обеспечивают 4 уровень защищённости персональных данных.

Перечень ГИС Росжелдора, подлежащих защите информации утвержден приказом Росжелдора от 31.10.2017 № 423 «Об утверждении документов, регламентирующих мероприятия по обеспечению информационной безопасности в Федеральном агентстве железнодорожного транспорта».

3. Мероприятия по защите информации при подключении к ГИС Росжелдора

3.1. Общие требования.

При подключении к ГИС Росжелдора на АРМ должны быть реализованы следующие меры защиты информации:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации;
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности информации;
- обеспечение целостности информационной системы и информации;
- обеспечение доступности информации;
- защита технических средств;
- защита информационной системы, ее средств и систем связи и передачи данных.

Для получения доступа к ГИС Росжелдора на АРМ рекомендуется установить и настроить сертифицированные средства защиты информации, приведенные в Таблице 1, или руководствоваться п. 5 настоящего документа.

Таблица 1

№ п/п	Наименование и тип технического средства	Сведения о сертификате
1.	СЗИ от НСД Secret Net 7	Сертификат соответствия ФСТЭК № 2707 выдан 07.09.2012 Продлен до: 07.09.2018
2.	СЗИ от НСД Secret Net Studio 8 (для АРМ под управлением ОС	Сертификат соответствия ФСТЭК № 3675 выдан 12.12.2016

№ п/п	Наименование и тип технического средства	Сведения о сертификате
	Windows 10)	Действителен до: 12.12.2019
3.	Kaspersky Endpoint Security для бизнеса – Стандартный	Сертификат соответствия ФСТЭК № 3025 выдан 25.11.2013 Действителен до: 25.11.2019
4.	Программное обеспечение VipNet Client for Windows 4.x (КС2)	Сертификат соответствия ФСБ России № СФ/124-2876 выдан 30.03.2016 Действителен до: 31.12.2018 Сертификат соответствия ФСТЭК России № 3727 выдан 30.11.2016 Действителен до: 30.11.2019

3.2. Организационные мероприятия по обеспечению безопасности информации.

Комплекс организационных мероприятий по защите информации, при подключении к ГИС Росжелдора, должен включать в себя следующие меры:

- все технические средства обработки информации и носители информации должны быть размещены в пределах контролируемой зоны;
- все помещения, в которых происходит обработка и хранение защищаемой информации, а также помещение с оборудованием, обеспечивающим технологический процесс обработки информации, должны быть оснащены средствами охранно-пожарной сигнализации;
- входные двери в помещения должны быть оснащены надежными замками;
- допуск в помещения вспомогательного и обслуживающего персонала (уборщиц, электромонтеров, сантехников и т.д.) должен производиться только в случае служебной необходимости в присутствии лиц, ответственных за эксплуатацию помещений;
- физическая охрана технических средств информационной системы должна предусматривать контроль доступа в помещения;
- должно проводиться резервирование технических средств, дублирование массивов и носителей информации;
- должен быть определен перечень лиц, допущенных к обработке информации в ГИС;
- должен быть назначен ответственный за обеспечение безопасности информации;
- все машинные носители информации, средства защиты информации должны быть учтены в специальных журналах.

3.3. Технические мероприятия

3.3.1. Общие требования к реализации технических мероприятий по обеспечению безопасности информации.

Применяемые технические средства защиты информации должны соответствовать требованиям к средствам защиты информации определенным в п. 26 Приказа ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований

о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» для информационных систем 3 класса защищенности.

В информационных системах 3 класса защищенности применяются средства защиты информации 6 класса, а также средства вычислительной техники не ниже 5 класса.

На АРМ пользователей, подключающихся к ГИС Росжелдора должны быть реализованы следующие технические меры для обеспечения 3 класса защищенности ГИС и 4 уровня защищенности персональных данных, если они обрабатываются на АРМ:

− защита от НСД с использованием сертифицированных ФСТЭК СрЗИ - не ниже 4 класса в соответствии с руководящим документом «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», утвержденным решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30.03.1992;

− средства антивирусной защиты — соответствующие 6 классу защиты, тип «В», в соответствии с требованиями к антивирусной защите, утвержденными приказом ФСТЭК России от 20.03.2012 № 28 «Об утверждении Требований к средствам антивирусной защиты», вступившим в действие 01.08.2012;

− межсетевые экраны — соответствующие 6 классу защиты, в соответствии с информационным сообщением ФСТЭК от 28.04.2016 № 240/24/1986 «Об утверждении Требований к межсетевым экранам».

3.3.2. Обеспечение безопасности информации при передаче по телекоммуникационным каналам связи.

При передаче информации по телекоммуникационным каналам связи необходимо обеспечить защиту передаваемой информации от несанкционированного доступа к ней криптографическими средствами защиты информации.

Применяемые криптографические средства защиты информации должны быть полностью совместимы с уже существующими средствами защиты каналов связи Росжелдора (ViPNet сеть № 11277, в составе: ПО ViPNet Administrator, ПАК ViPNet Coordinator HW1000).

Класс применяемых криптографических средств - КС2.

4. Порядок проведения мероприятий по защите информации при подключении к ГИС Росжелдора

Для проведения работ по защите информации при подключении к ГИС Росжелдора необходимо руководствоваться нормативными документами, перечисленными в разделе № 1 текущего документа, для проведения указанных мероприятий допускается привлечение организаций, имеющих лицензию на деятельность по технической защите конфиденциальной информации

в соответствии с Федеральным законом от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности».

5. Рекомендации к средствам защиты информации.

Применяемые технические средства защиты информации должны быть сертифицированы ФСТЭК России (ФСБ России в части средств криптографической защиты информации) и соответствовать требованиям к средствам защиты информации определенным:

- Приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» для информационных систем 3 класса защищенности;
- Приказом ФСТЭК России от 06.12.2011 № 638 «Об утверждении Требований к системам обнаружения вторжений»;
- Приказом ФСТЭК России от 20.03.2012 № 28 «Об утверждении Требований к средствам антивирусной защиты».

Меры по защите АРМ пользователей ГИС Росжелдора определяются пользователями самостоятельно (или с привлечением организаций – лицензиатов ФСТЭК России и ФСБ России по направлениям технической и криптографической защиты информации) в зависимости от уже реализованных в учреждении мер организационного и технического характера по обеспечению безопасности информации в соответствии с требованиями федеральных законов и нормативных документов ФСТЭК России и ФСБ России, а также в соответствии с требованиями настоящего документа.

При выборе средств защиты необходимо также руководствоваться следующими рекомендациями:

Таблица 2

№ п/п	Средства защиты информации	
1.	Средства антивирусной защиты	Средства антивирусной защиты должны быть лицензионными и сертифицированными ФСТЭК России с ежедневно обновляемыми базами сигнатур (например, Kaspersky Endpoint Security - медиапак или эквивалент).
2.	Средства защиты информации при передаче по каналам связи	Применяемые средства должны быть полностью совместимы с уже существующими средствами защиты каналов связи Росжелдора (ViPNet сеть № 11277) (например, ViPNet Coordinator HW, ViPNet Client, или эквивалент)
3.	Средства межсетевого экранирования	Средства межсетевого экранирования должны корректно функционировать в рамках существующей инфраструктуры Росжелдора (например, ViPNet Coordinator HW, ViPNet Client, или эквивалент)
4.	Средства защиты от несанкционированного доступа	Средство от НСД SecretNet или эквивалент

6. Подключение к ГИС Росжелдора

Подключение АРМ пользователей к ГИС Росжелдора производиться только после выполнения учреждением всех требований по обеспечению безопасности информации (в том числе и персональных данных) предусмотренных федеральными законами, нормативными документами и определенными настоящим документом.

Предоставление доступа пользователей к ГИС Росжелдора должно осуществляется на основании заявок, оформленных по форме, приведенной в Приложении № 1 к настоящим требованиям.

Ответственными за допуск сотрудников к ГИС Росжелдора являются руководители учреждений и организаций, подключенных к ГИС Росжелдора.

Приложение 1

Заявка на подключение к
государственной информационной системе _____
Федерального агентства железнодорожного транспорта

Прошу предоставить доступ к государственной информационной системе

_____

Данные об органе/организации			
Полное наименование органа/организации			
Краткое наименование органа/организации			
Данные об уполномоченном должностном лице органа/организации			
№ п/п	Фамилия, Имя отчество	должность	Рабочий телефон Адрес электронной почты
1			
2			
3			
4			
5			
6			
Данные о проведении мероприятий по защите информации			
Дата и номер аттестата соответствия	*Если имеется*		
Используемые средства защиты информации			
ФИО, контактная информация администратора безопасности			
Данные о согласовании доступа с оператором государственной информационной системы			
Номер и дата документа о согласовании доступа			
Кем согласовано (Должность, ФИО)			

Руководитель _____ *Фамилия, Инициалы*

(дата)