



МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
(РОСЖЕЛДОР)**

ПРИКАЗ

31.10.2017

Москва

№

423

Об утверждении документов, регламентирующих мероприятия по обеспечению информационной безопасности в Федеральном агентстве железнодорожного транспорта

Во исполнение Федеральным агентством железнодорожного транспорта (Росжелдор) требований ч. 1, 4 ст. 16 Федерального закона Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», ч. 1 ст. 18.1, ч. 1, 2 ст. 19 Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», п. 1 Перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами, утвержденного постановлением Правительства Российской Федерации от 21.03.2012 № 211, 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:

1.1. Перечень государственных информационных систем Федерального агентства железнодорожного транспорта, подлежащих защите информации.

1.2. Перечень сведений, содержащих персональные данные, обрабатываемых в государственных информационных системах центрального аппарата Федерального агентства железнодорожного транспорта;

1.3. Порядок доступа в помещения, в которых ведется обработка персональных данных в центральном аппарате Федерального агентства железнодорожного транспорта;

1.4. Перечень должностей государственных гражданских служащих центрального аппарата Федерального агентства железнодорожного транспорта, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;

1.5. Перечень лиц, допущенных к автоматизированной обработке персональных данных, обрабатываемых в государственных информационных системах Федерального агентства железнодорожного транспорта;

1.6. Матрицу доступа пользователей государственных информационных систем Федерального агентства железнодорожного транспорта;

1.7. Политику в отношении обработки персональных данных субъектов в центральном аппарате Федерального агентства железнодорожного транспорта;

1.8. Правила обработки и обеспечения защиты персональных данных в центральном аппарате Федерального агентства железнодорожного транспорта;

1.9. Регламент рассмотрения запросов субъектов персональных данных или их представителей, об обработке их персональных данных в центральном аппарате Федерального агентства железнодорожного транспорта;

1.10. Форму запроса на предоставление сведений об обработке персональных данных субъекта персональных данных в центральном аппарате Федерального агентства железнодорожного транспорта;

1.11. Форму журнала учета обращений субъектов персональных данных о выполнении их законных прав, при обработке персональных данных в государственных информационных системах Федерального агентства железнодорожного транспорта;

1.12. Регламент предоставления прав доступа к информации ограниченного доступа, не содержащей государственную тайну, обрабатываемой в государственных информационных системах Федерального агентства железнодорожного транспорта;

1.13. Инструкцию по организации антивирусной защиты в государственных информационных системах Федерального агентства железнодорожного транспорта;

1.14. Инструкцию по организации парольной защиты в государственных информационных системах Федерального агентства железнодорожного транспорта;

1.15. Инструкцию пользователя государственной информационной системы персональных данных Федерального агентства железнодорожного транспорта;

1.16. Форму согласия субъекта на обработку персональных данных;

1.17. Форму обязательства о соблюдении режима защиты персональных данных в центральном аппарате Федерального агентства железнодорожного транспорта;

1.18. Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в центральном аппарате Федерального агентства железнодорожного транспорта;

1.19. Регламент проведения технического обслуживания в центральном аппарате Федерального агентства железнодорожного транспорта;

1.20. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Федеральном агентстве железнодорожного транспорта;

1.21. Перечень разрешенного к использованию программного обеспечения в государственных информационных системах Федерального агентства железнодорожного транспорта;

1.22. План мероприятий по обеспечению защиты государственных информационных систем и персональных данных в центральном аппарате Федерального агентства железнодорожного транспорта;

1.23. Форму журнала учета мероприятий по контролю обеспечения защиты государственных информационных систем и персональных данных в центральном аппарате Федерального агентства железнодорожного транспорта;

1.24. Форму журнала выдачи съемных носителей информации для работы в государственных информационных системах и обработки персональных данных в центральном аппарате Федерального агентства железнодорожного транспорта;

1.25. Форму журнала поэкземплярного учета средств защиты информации в центральном аппарате Федерального агентства железнодорожного транспорта.

2. Признать утратившим силу приказ Росжелдора от 20.12.2016 № 582 «Об утверждении документов, регламентирующих мероприятия по обеспечению информационной безопасности в Федеральном агентстве железнодорожного транспорта».

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

Врио руководителя

Е.В. Луковников

УТВЕРЖДЕНО
приказом Росжелдора
от 31.10.2017 № 423

ПЕРЕЧЕНЬ
государственных информационных систем Федерального агентства железнодорожного транспорта,
подлежащих защите информации

№ п/п	Наименование ГИС	Оператор системы Адрес размещения системы	Обрабатываются персональные данные
1.	Государственная информационная система «Информационная система обеспечения финансово-экономической деятельности Федерального агентства железнодорожного транспорта»	Федеральное агентство железнодорожного транспорта 105064, г. Москва, ул. Старая Басманная, д. 11/2 стр. 1.	да
2.	Государственная информационная система «Система электронного документооборота Федерального агентства железнодорожного транспорта»	Федеральное агентство железнодорожного транспорта г. Москва, ул. Старая Басманная, д. 11/2 стр. 1.	да
3.	Государственная информационная система «Электронная почтовая система Федерального агентства железнодорожного транспорта»	Федеральное агентство железнодорожного транспорта Центр обработки данных АО «Ростелеком», г. Москва, Сущевский вал, д 26	да

4.	Государственная информационная система «Официальный сайт Федерального агентства железнодорожного транспорта (www.roszeldor.ru)»	Федеральное агентство железнодорожного транспорта Центр обработки данных АО «Ростелеком», г. Москва, Суцевский вал, д 26	да
5.	Государственная информационная система «Информационная система пономерного учета пассажирских вагонов локомотивной тяги»	Федеральное агентство железнодорожного транспорта 105064, г. Москва, ул. Старая Басманная, д. 11/2 стр. 1.	нет
6.	Государственная информационная система «Информационная система пономерного учета локомотивов»	Федеральное агентство железнодорожного транспорта 105064, г. Москва, ул. Старая Басманная, д. 11/2 стр. 1.	нет
7.	Государственная информационная система «Информационная система ведения перечней железнодорожных станций»	Федеральное агентство железнодорожного транспорта 105064, г. Москва, ул. Старая Басманная, д. 11/2 стр. 1.	нет
8.	Государственная информационная система «Информационная система обеспечения предоставления государственных услуг Федерального агентства железнодорожного транспорта»	Федеральное агентство железнодорожного транспорта 105064, г. Москва, ул. Старая Басманная, д. 11/2 стр. 1.	нет

**Перечень сведений, содержащих персональные данные, обрабатываемых
в государственных информационных системах Федерального агентства
железнодорожного транспорта**

1. Государственная информационная система «Информационная система обеспечения финансово-экономической деятельности Федерального агентства железнодорожного транспорта»

В государственной информационной системе (далее – ГИС) «Информационная система обеспечения финансово-экономической деятельности Федерального агентства железнодорожного транспорта» осуществляется обработка сведений, содержащих персональные данные граждан Российской Федерации в составе:

- ФИО;
- Паспортные данные;
- ИНН;
- СНИЛС;
- Характер, вид и место работы;
- Сведения из трудовой книжки;
- Место жительства;
- Гражданство;
- Образование;
- Сведения об имеющихся научных степенях и научных званиях;
- Стаж работы;
- Сведения о состоянии в браке;
- Данные страхового свидетельства государственного пенсионного страхования;
- Страховой полис ОМС;
- Состав семьи;
- Сведения о воинском учете;
- Сведения об аттестации;
- Сведения о повышении квалификации;
- Сведения о поощрениях;
- Сведения об отпуске;
- Сведения о социальных льготах;
- Сведения об имуществе;
- Сведения о доходах;
- Адрес электронной почты;
- Телефон.

2. Государственная информационная система «Система электронного документооборота Федерального агентства железнодорожного транспорта»

В ГИС «Система электронного документооборота Федерального агентства железнодорожного транспорта» осуществляется обработка сведений, содержащих персональные данные граждан Российской Федерации в составе:

- ФИО;
- Должность и место работы;
- Место жительства / почтовый адрес;
- Адрес электронной почты;
- Телефон.

3. Государственная информационная система «Официальный сайт Федерального агентства железнодорожного транспорта (www.roszeldor.ru)»

В ГИС «Официальный сайт Федерального агентства железнодорожного транспорта» осуществляется обработка сведений, содержащих персональные данные граждан Российской Федерации в составе:

- ФИО;
- Должность и место работы;
- Место жительства/ почтовый адрес;
- Адрес электронной почты;
- Телефон.

4. Государственная информационная система «Электронная почтовая система Федерального агентства железнодорожного транспорта»

В ГИС «Электронная почтовая система Федерального агентства железнодорожного транспорта» осуществляется обработка сведений, содержащих персональные данные граждан Российской Федерации в составе:

- ФИО;
- Должность и место работы;
- Место жительства/ почтовый адрес;
- Адрес электронной почты;
- Телефон.

**Порядок доступа в помещения,
в которых ведется обработка персональных данных,
в центральном аппарате Федерального агентства железнодорожного
транспорта**

1. Общие положения

1.1. Порядок доступа в помещения, в которых ведется обработка персональных данных, к техническим средствам защиты информации, а также в помещения, в которых они установлены (далее – Порядок), определяет технические меры по обеспечению контроля и управления физическим доступом в центральном аппарате Федерального агентства железнодорожного транспорта (Росжелдор).

1.2. Настоящий Порядок определяет ответственных лиц за контроль и управление физическим доступом к техническим средствам, обрабатывающим персональные данные, а также к техническим средствам защиты информации и помещениям, в которых они установлены в Росжелдоре.

**2. Обеспечение контроля и управления физическим доступом
к техническим средствам защиты информации и техническим средствам,
обрабатывающим персональные данные**

2.1. Контроль и управление физическим доступом в контролируруемую зону Росжелдора осуществляется контрольно-пропускной службой, состоящей из работников подведомственной организации Росжелдора – Федеральное государственное предприятие «Ведомственная охрана железнодорожного транспорта Российской Федерации» (ФГП ВО ЖДТ России).

2.2. Выдачу ключей для доступа в помещения Росжелдора, расположенных в контролируемой зоне, сотрудникам Росжелдора ежедневно в начале рабочего дня осуществляет сотрудник подведомственной организации Росжелдора – Федеральное казенное учреждение «Управление служебных зданий федеральных органов исполнительной власти в области транспорта» (далее – ФКУ УСЗ) или подрядной организации, на которого возложена данная обязанность. В конце рабочего дня ключи возвращаются под роспись сотруднику Росжелдора.

2.3. Для предоставления разового доступа в контролируемую зону Росжелдора физических лиц, не являющихся сотрудниками Росжелдора осуществляется оформление разовых пропусков для входа в административное здание посредством оформления заявки в бюро пропусков ФГП ВО ЖДТ России.

2.4. Для предоставления постоянного доступа осуществляется внесение пропуска в соответствующие списки ФГП ВО ЖДТ России посредством обращения в Административно-кадровое управление Росжелдора.

2.5. Выявление фактов несанкционированного доступа в контролируемую зону Росжелдора осуществляется с помощью камер наблюдения, установленных на каждом этаже здания, в котором расположен Росжелдор.

2.6. Доступ в помещения, в которых расположены автоматизированные рабочие места государственных гражданских служащих, с которых осуществляется обработка персональных данных, имеют государственные гражданские служащие Росжелдора, а также работники подведомственных и подрядных организаций Росжелдора. Работники подведомственных и подрядных организаций Росжелдора могут находиться в данных помещениях только в присутствии государственных гражданских служащих Росжелдора.

2.7. Доступ в помещения, в которых расположены сервера государственных информационных систем Росжелдора, в которых осуществляется обработка персональных данных, имеют: администратор информационной безопасности и работники ФКУ УСЗ, ответственных за организацию, координацию и контроль реализации мероприятий по информатизации, направленных на создание, развитие, модернизацию, эксплуатацию и вывод из эксплуатации информационных систем и компонентов информационно-телекоммуникационной инфраструктуры Росжелдора. Работники других подведомственных и подрядных организаций Росжелдора могут находиться в данных помещениях только в присутствии работников ФКУ УСЗ или администратора информационной безопасности.

3. Ответственные за организацию контроля и управления физическим доступом к техническим средствам защиты информации и техническим средствам, обрабатывающим персональные данные

3.1. Ответственность за повседневный и периодический контроль возлагается на администратора информационной безопасности.

3.2. Ответственность за управление физическим доступом на территории обработки защищаемой информации и доступом к техническим средствам защиты информации в Росжелдоре возлагается на сотрудника ФКУ УСЗ или подрядной организации, на которого возложена обязанность по выдаче ключей для доступа в помещения Росжелдора, расположенных в контролируемой зоне.

УТВЕРЖДЕНО
приказом Росжелдора
от 31.10.2017 № 423

Перечень должностей государственных гражданских служащих центрального аппарата Федерального агентства железнодорожного транспорта, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным

1.	Руководитель
2.	Заместитель руководителя
3.	Начальник управления
4.	Заместитель начальника управления
5.	Начальник отдела
6.	Заместитель начальника отдела
7.	Главный специалист-эксперт
8.	Ведущий специалист-эксперт
9.	Ведущий эксперт
10.	Специалист-эксперт
11.	Специалист 1 разряда
12.	Специалист-эксперт
13.	Старший специалист 1 разряда
14.	Старший специалист 3 разряда

УТВЕРЖДЕНО
приказом Росжелдора
от 31.10.2017 № 423

**Перечень лиц,
допущенных к автоматизированной обработке персональных данных,
обрабатываемых в государственных информационных системах
Федерального агентства железнодорожного транспорта**

Перечень лиц, допущенных к автоматизированной обработке персональных данных, обрабатываемых в государственной информационной системе «Информационная система обеспечения финансово-экономической деятельности Федерального агентства железнодорожного транспорта»:

№ п/п	ФИО государственного гражданского служащего	Должность
Руководство Федерального агентства железнодорожного транспорта		
1.	Чепец Владимир Юрьевич	Руководитель
2.	Луковников Евгений Валентинович	Заместитель руководителя
Административно-кадровое управление		
3.	Беспалов Андрей Михайлович	Начальник управления
4.	Загубный Юрий Николаевич	Зам. начальника управления
Отдел кадров и государственной службы		
5.	Потапова Вера Александровна	Начальник отдела
6.	Шарифуллина Маргарита Анатольевна	Заместитель начальника отдела
7.	Максименко Ирина Николаевна	Главный специалист-эксперт
8.	Боченина Алина Александровна	Главный специалист-эксперт
9.	Симонова Светлана Владимировна	Специалист-эксперт
10.	Самохина Анастасия Владиславовна	Ведущий эксперт
Организационно-протокольный отдел		
11.	Зими́на Елена Павловна	Начальник отдела
12.	Судибор Марина Николаевна	Главный специалист-эксперт
13.	Сарибекян Рита Сарибекевна	Специалист 1 разряда
14.	Кондакова Марина Сергеевна	Ведущий эксперт
Отдел документационного обеспечения и архивов		
15.	Жаворонков Андрей Всеволодович	Начальник отдела
16.	Никифор Елена Александровна	Заместитель начальника отдела
17.	Меркулова Татьяна Юрьевна	Главный специалист-эксперт
18.	Назарова Виктория Павловна	Специалист-эксперт
19.	Быстрова Анна Андреевна	Старший специалист 1 разряда
20.	Бережная Людмила Витальевна	Старший специалист 3 разряда
Управление экономики и финансов		

№ п/п	ФИО государственного гражданского служащего	Должность
21.	Зяблицкий Игорь Юрьевич	Начальник управления
22.	Васильев Игорь Алексеевич	Зам. начальника управления
23.	Водянова Маргарита Николаевна	Заместитель начальника управления - главный бухгалтер
Отдел бухгалтерского учета		
24.	Данилова Татьяна Владимировна	Начальник отдела-зам. главного бухгалтера
25.	Горбачева Екатерина Александровна	Главный специалист-эксперт
26.	Прудникова Надежда Викторовна	Ведущий специалист-эксперт
27.	Щеголев Дмитрий Владимирович	Ведущий специалист-эксперт
28.	Гмыря Олеся Алексеевна	Ведущий специалист-эксперт
Отдел экономики и финансов		
29.	Сердюкова Наталья Александровна	Начальник отдела
30.	Горячева Елена Сергеевна	Заместитель начальника отдела
31.	Сперанская Ирина Игоревна	Главный специалист-эксперт
32.	Севостьянова Наталия Олеговна	Главный специалист-эксперт
33.	Шмакова Евгения павловна	Ведущий специалист-эксперт
Отдел реализации программ и инвестиционных проектов		
34.	Перестюк Михаил Михайлович	Начальник отдела
35.	Адуйский Артем Евгеньевич	Заместитель начальника отдела
36.	Калюжная Виктория Александровна	Заместитель начальника отдела
37.	Горбик Ирина Павловна	Главный специалист-эксперт

Перечень лиц, допущенных к автоматизированной обработке персональных данных, обрабатываемых в государственной информационной системе «Система электронного документооборота Федерального агентства железнодорожного транспорта»:

№ п/п	ФИО государственного гражданского служащего	Должность
Руководство Федерального агентства железнодорожного транспорта		
1.	Чепец Владимир Юрьевич	Руководитель
2.	Луковников Евгений Валентинович	Заместитель руководителя
Административно-кадровое управление		
3.	Беспалов Андрей Михайлович	Начальник управления
4.	Загубный Юрий Николаевич	Зам. начальника управления
Отдел кадров и государственной службы		
5.	Потапова Вера Александровна	Начальник отдела
6.	Шарифуллина Маргарита Анатольевна	Заместитель начальника отдела
7.	Максименко Ирина Николаевна	Главный специалист-эксперт
8.	Боченина Алина Александровна	Главный специалист-эксперт

№ п/п	ФИО государственного гражданского служащего	Должность
9.	Симонова Светлана Владимировна	Специалист-эксперт
10.	Самохина Анастасия Владиславовна	Ведущий эксперт
Организационно-протокольный отдел		
11.	Зими́на Елена Павловна	Начальник отдела
12.	Судибор Марина Николаевна	Главный специалист-эксперт
13.	Сарибекян Рита Сарибековна	Специалист 1 разряда
14.	Кондакова Марина Сергеевна	Ведущий эксперт
Отдел документационного обеспечения и архивов		
15.	Жаворонков Андрей Всеволодович	<u>Начальник</u> отдела
16.	Никифор Елена Александровна	Заместитель начальника отдела
17.	Меркулова Татьяна Юрьевна	Главный специалист-эксперт
18.	Назарова Виктория Павловна	Специалист-эксперт
19.	Быстрова Анна Андреевна	Старший специалист 1 разряда
20.	Бережная Людмила Витальевна	Старший специалист 3 разряда
Управление экономики и финансов		
21.	Зяблицкий Игорь Юрьевич	Начальник управления
22.	Васильев Игорь Алексеевич	Зам. начальника управления
23.	Водянова Маргарита Николаевна	Заместитель начальника управления - главный бухгалтер
Отдел бухгалтерского учета		
24.	Данилова Татьяна Владимировна	Начальник отдела-зам. главного бухгалтера
25.	Горбачева Екатерина Александровна	Главный специалист-эксперт
26.	Прудникова Надежда Викторовна	Ведущий специалист-эксперт
27.	Щеголев Дмитрий Владимирович	Ведущий специалист-эксперт
28.	Гмыря Олеся Алексеевна	Ведущий специалист-эксперт
Отдел экономики и финансов		
29.	Сердюкова Наталья Александровна	Начальник отдела
30.	Горячева Елена Сергеевна	Заместитель начальника отдела
31.	Сперанская Ирина Игоревна	Главный специалист-эксперт
32.	Севостьянова Наталия Олеговна	Главный специалист-эксперт
33.	Шмакова Евгения павловна	Ведущий специалист-эксперт
Отдел реализации программ и инвестиционных проектов		
34.	Перестюк Михаил Михайлович	Начальник отдела
35.	Адуйский Артем Евгеньевич	Заместитель начальника отдела
36.	Калюжная Виктория Александровна	Заместитель начальника отдела
37.	Горбик Ирина Павловна	Главный специалист-эксперт
Управление инфраструктуры и перевозок		
38.	Шпади Дмитрий Владимирович	Начальник управления
39.	Захарова Татьяна Викторовна	Зам. начальника управления
40.	Григорьев Константин	Зам. начальника управления

№ п/п	ФИО государственного гражданского служащего	Должность
	Владимирович	
Отдел перевозок		
41.	Петров Алексей Геннадьевич	Начальник отдела
42.	Тумилович Михаил Константинович	Заместитель начальника отдела
43.	Каталымова Наталия Николаевна	Главный специалист-эксперт
44.	Кудряшов Юрий Олегович	Ведущий специалист-эксперт
45.	Кролик Ольга Петровна	Специалист 1 разряда
Отдел инфраструктуры и технических средств		
46.	Есипов Алексей Николаевич	Начальник отдела
47.	Тарасов Евгений Викторович	Главный специалист-эксперт
48.	Лавренова Татьяна Владимировна	Главный специалист-эксперт
49.	Лагметова Екатерина Викторовна	Главный специалист-эксперт
Отдел по работе с пользователями услуг железнодорожного транспорта		
50.	Новосёлов Виктор Николаевич	Начальник отдела
51.	Буякова Вера Николаевна	Заместитель начальника отдела
52.	Митькина Галина Ильинична	Главный специалист-эксперт
53.	Мамедова Леда Багировна	Главный специалист-эксперт
54.	Кривенко Ксения Григорьевна	Ведущий специалист-эксперт
Управление транспортной безопасностью		
55.	Егоренков Юрий Вячеславович	Начальник управления
56.	Рябов Михаил Васильевич	Заместитель начальника управления
57.	Титов Павел Викторович	Заместитель начальника управления
Отдел оценки уязвимости и категорирования		
58.	Кекул Виктор Михайлович	Начальник отдела
59.	Балашов Д.митрий Рудольфович	Заместитель начальника отдела
60.	Копытин Валерий Алексеевич	Главный специалист-эксперт
61.	Асмолова Олеся Сергеевна	Главный специалист-эксперт
62.	Макогончук Каролина Андреевна	Ведущий специалист-эксперт
Отдел по работе с планами по обеспечению транспортной безопасности		
63.	Винокуров Олег Михайлович	Начальник отдела
64.	Наливайко Станислав Александрович	Заместитель начальника отдела
65.	Гнусарева Екатерина Алексеевна	Главный специалист-эксперт
66.	Спасская Алина Александровна	Ведущий специалист-эксперт
Отдел координации, анализа и прогнозирования		
67.	Карабанов Владимир Владимирович	Начальник отдела
68.	Батальщиков Иван Иванович	Заместитель начальника отдела
69.	Морозова Ирина Александровна	Главный специалист-эксперт
70.	Габец Наталья Владимировна	Главный специалист-эксперт
71.	Балашова Ирина Витальевна	Старший специалист 1 разряда
Отдел гражданской обороны и ликвидации чрезвычайных ситуаций на		

№ п/п	ФИО государственного гражданского служащего	Должность
железнодорожном транспорте общего пользования		
72.	Середин Роман Александрович	Начальник отдела
73.	Ступаков Игорь Викторович	Главный специалист-эксперт
74.	Ефимова Екатерина Сергеевна	Ведущий специалист-эксперт
Управление учебных заведений и правового обеспечения		
75.	Меркулов Георигий Владимирович	Начальник управления
76.	Веретенникова Наталия Валерьевна	Зам.начальника управления
Отдел правовой экспертизы и применения законодательства		
77.	Кохановский Павел Александрович	Начальник отдела
78.	Артюнян Анаит	Зам.начальника отдела
79.	Глотов Евгений Андреевич	Главный специалист-эксперт
80.	Никанорова Анна Викторовна	Главный специалист-эксперт
81.	Карташева Нина Александровна	Главный специалист-эксперт
Отдел имущественных отношений и территориального планирования		
82.	Саутиева Радима Султановна	Начальник отдела
83.	Першина Дарья Сергеевна	Заместитель начальника отдела
84.	Щетинникова Светлана Геннадьевна	Главный специалист-эксперт
Отдел учебных заведений		
85.	Царицынский Владислав Викторович	Начальник отдела
86.	Минкина Лариса Владимировна	Заместитель начальника отдела
87.	Девятьярова Арина Юрьевна	Главный специалист-эксперт
88.	Кокорев Сергей Викторович	Главный специалист-эксперт
89.	Дарькина Мария Александровна	Ведущий специалист-эксперт

Перечень лиц, допущенных к автоматизированной обработке персональных данных, обрабатываемых в государственной информационной системе «Электронная почтовая система Федерального агентства железнодорожного транспорта»:

№ п/ п	ФИО государственного гражданского служащего	Должность
Руководство Федерального агентства железнодорожного транспорта		
1.	Чепец Владимир Юрьевич	Руководитель
2.	Луковников Евгений Валентинович	Заместитель руководителя
Административно-кадровое управление		
3.	Беспалов Андрей Михайлович	Начальник управления
4.	Загубный Юрий Николаевич	Зам. начальника управления
Отдел кадров и государственной службы		
5.	Потапова Вера Александровна	Начальник отдела
6.	Шарифуллина Маргарита Анатольевна	Заместитель начальника отдела

№ п/ п	ФИО государственного гражданского служащего	Должность
7.	Максименко Ирина Николаевна	Главный специалист-эксперт
8.	Боченина Алина Александровна	Главный специалист-эксперт
9.	Симонова Светлана Владимировна	Специалист-эксперт
10.	Самохина Анастасия Владиславовна	Ведущий эксперт
Организационно-протокольный отдел		
11.	Зими́на Елена Павловна	Начальник отдела
12.	Судибор Марина Николаевна	Главный специалист-эксперт
13.	Сарибекян Рита Сарибековна	Специалист 1 разряда
14.	Кондакова Марина Сергеевна	Ведущий эксперт
Отдел документационного обеспечения и архивов		
15.	Жаворонков Андрей Всеволодович	<u>Начальник отдела</u>
16.	Никифор Елена Александровна	Заместитель начальника отдела
17.	Меркулова Татьяна Юрьевна	Главный специалист-эксперт
18.	Назарова Виктория Павловна	Специалист-эксперт
19.	Быстрова Анна Андреевна	Старший специалист 1 разряда
20.	Бережная Людмила Витальевна	Старший специалист 3 разряда
Управление экономики и финансов		
21.	Зяблицкий Игорь Юрьевич	Начальник управления
22.	Васильев Игорь Алексеевич	Зам. начальника управления
23.	Водянова Маргарита Николаевна	Заместитель начальника управления - главный бухгалтер
Отдел бухгалтерского учета		
24.	Данилова Татьяна Владимировна	Начальник отдела-зам. главного бухгалтера
25.	Горбачева Екатерина Александровна	Главный специалист-эксперт
26.	Прудникова Надежда Викторовна	Ведущий специалист-эксперт
27.	Щеголев Дмитрий Владимирович	Ведущий специалист-эксперт
28.	Гмыря Олеся Алексеевна	Ведущий специалист-эксперт
Отдел экономики и финансов		
29.	Сердюкова Наталья Александровна	Начальник отдела
30.	Горячева Елена Сергеевна	Заместитель начальника отдела
31.	Сперанская Ирина Игоревна	Главный специалист-эксперт
32.	Севостьянова Наталия Олеговна	Главный специалист-эксперт
33.	Шмакова Евгения павловна	Ведущий специалист-эксперт
Отдел реализации программ и инвестиционных проектов		
34.	Перестюк Михаил Михайлович	Начальник отдела
35.	Адуйский Артем Евгеньевич	Заместитель начальника отдела
36.	Калюжная Виктория Александровна	Заместитель начальника отдела
37.	Горбик Ирина Павловна	Главный специалист-эксперт
Управление инфраструктуры и перевозок		

№ п/п	ФИО государственного гражданского служащего	Должность
38.	Шпади Дмитрий Владимирович	Начальник управления
39.	Захарова Татьяна Викторовна	Зам. начальника управления
40.	Григорьев Константин Владимирович	Зам. начальника управления
Отдел перевозок		
41.	Петров Алексей Геннадьевич	Начальник отдела
42.	Тумилович Михаил Константинович	Заместитель начальника отдела
43.	Каталымова Наталия Николаевна	Главный специалист-эксперт
44.	Кудряшов Юрий Олегович	Ведущий специалист-эксперт
45.	Кролик Ольга Петровна	Специалист 1 разряда
Отдел инфраструктуры и технических средств		
46.	Есипов Алексей Николаевич	Начальник отдела
47.	Тарасов Евгений Викторович	Главный специалист-эксперт
48.	Лавренова Татьяна Владимировна	Главный специалист-эксперт
49.	Лагметова Екатерина Викторовна	Главный специалист-эксперт
Отдел по работе с пользователями услуг железнодорожного транспорта		
50.	Новосёлов Виктор Николаевич	Начальник отдела
51.	Буякова Вера Николаевна	Заместитель начальника отдела
52.	Митькина Галина Ильинична	Главный специалист-эксперт
53.	Мамедова Леда Багировна	Главный специалист-эксперт
54.	Кривенко Ксения Григорьевна	Ведущий специалист-эксперт
Управление транспортной безопасностью		
55.	Егоренков Юрий Вячеславович	Начальник управления
56.	Рябов Михаил Васильевич	Заместитель начальника управления
57.	Титов Павел Викторович	Заместитель начальника управления
Отдел оценки уязвимости и категорирования		
58.	Кекул Виктор Михайлович	Начальник отдела
59.	Балашов Дмитрий Рудольфович	Заместитель начальника отдела
60.	Копытин Валерий Алексеевич	Главный специалист-эксперт
61.	Асмолова Олеся Сергеевна	Главный специалист-эксперт
62.	Макогончук Каролина Андреевна	Ведущий специалист-эксперт
Отдел по работе с планами по обеспечению транспортной безопасности		
63.	Винокуров Олег Михайлович	Начальник отдела
64.	Наливайко Станислав Александрович	Заместитель начальника отдела
65.	Гнусарева Екатерина Алексеевна	Главный специалист-эксперт
66.	Спасская Алина Александровна	Ведущий специалист-эксперт
Отдел координации, анализа и прогнозирования		
67.	Карабанов Владимир Владимирович	Начальник отдела
68.	Батальщиков Иван Иванович	Заместитель начальника отдела
69.	Морозова Ирина Александровна	Главный специалист-эксперт
70.	Габец Наталья Владимировна	Главный специалист-эксперт

№ п/п	ФИО государственного гражданского служащего	Должность
71.	Балашова Ирина Витальевна	Старший специалист 1 разряда
Отдел гражданской обороны и ликвидации чрезвычайных ситуаций на железнодорожном транспорте общего пользования		
72.	Середин Роман Александрович	Начальник отдела
73.	Ступаков Игорь Викторович	Главный специалист-эксперт
74.	Ефимова Екатерина Сергеевна	Ведущий специалист-эксперт
Управление учебных заведений и правового обеспечения		
75.	Меркулов Георгий Владимирович	Начальник управления
76.	Веретенникова Наталия Валерьевна	Зам.начальника управления
Отдел правовой экспертизы и применения законодательства		
77.	Кохановский Павел Александрович	Начальник отдела
78.	Артюнян Анаит	Зам.начальника отдела
79.	Глотов Евгений Андреевич	Главный специалист-эксперт
80.	Никанорова Анна Викторовна	Главный специалист-эксперт
81.	Карташева Нина Александровна	Главный специалист-эксперт
Отдел имущественных отношений и территориального планирования		
82.	Саутиева Радима Султановна	Начальник отдела
83.	Першина Дарья Сергеевна	Заместитель начальника отдела
84.	Щетинникова Светлана Геннадьевна	Главный специалист-эксперт
Отдел учебных заведений		
85.	Царицынский Владислав Викторович	Начальник отдела
86.	Минкина Лариса Владимировна	Заместитель начальника отдела
87.	Девятьярова Арина Юрьевна	Главный специалист-эксперт
88.	Кокорев Сергей Викторович	Главный специалист-эксперт
89.	Дарькина Мария Александровна	Ведущий специалист-эксперт

К государственным информационным системам Федерального агентства железнодорожного транспорта с правами администраторов имеют доступ:

№ п/п	ФИО	Организация	Основание допуска
1.	Блинов Геннадий Геннадьевич	ФКУ УСЗ - подведомственная Росжелдору организация	Устав ФКУ УСЗ: «2.1. Целью создания Учреждения являются ... организация, координация и контроль реализации мероприятий по информатизации, направленных на создание, развитие, модернизацию, эксплуатацию и вывод из эксплуатации информационных систем и компонентов информационно-телекоммуникационной инфраструктуры Росжелдора.»
2.	Фолин Владимир Георгиевич		
3.	Семёновых Маргарита Александровна		

Также к государственным информационным системам Росжелдора с правами администраторов имеют доступ работники подрядных организаций на основании государственных контрактов или договоров на создание, обеспечение эксплуатации или развитие государственных информационных систем Росжелдора:

№ п/п	ФИО	Организация	Основание допуска (номер, дата договора)
1.	Лукиных Олег	ИП Абрамов К.М.	84 от 28.08.2017
2.	Абрамов Константин Михайлович	ИП Абрамов К.М.	84 от 28.08.2017
3.	Мухаев Сергей Юрьевич	ИП Абрамов К.М.	84 от 28.08.2017
4.	Зисганов Илья Сергеевич	ИП Абрамов К.М.	84 от 28.08.2017
5.	Пляцовой Павел Сергеевич	ООО «Альфа Док»	101 от 29.09.2017
6.	Юрьев Александр Борисович	ООО «Альфа Док»	101 от 29.09.2017
7.	Цыникин Андрей Анатольевич	ООО «Альфа Док»	101 от 29.09.2017
8.	Комков Алексей Владимирович	ООО «Виваком»	Договор от 28.09.2017 № 99д на поддержку информационного ресурса www.roszeldor.ru
9.	Гилязов Тимур Алексович	ООО «Интегрикс»	ГК на оказание услуг по системному администрированию информационных систем и компонентов информационно-телекоммуникационной инфраструктуры центрального аппарата Федерального агентства железнодорожного транспорта

УТВЕРЖДЕНО
приказом Росжелдора
от 31.10.2017 № 423

Матрица доступа пользователей государственных информационных систем Федерального агентства железнодорожного транспорта

Объект доступа Субъект доступа	Тип доступа	База данных системы	Интернет	Принтер	Внешний носитель	Системные каталоги ¹	Объекты профиля пользователя ²
Пользователь ГИС «Информационная система обеспечения финансово-экономической деятельности Федерального агентства железнодорожного транспорта»	Чтение	X	X			X	X
	Запись ³	X	X	X			X
	Запрет доступа ⁴				X		
Пользователь ГИС «Система электронного документооборота Федерального агентства железнодорожного транспорта»	Чтение	X	X			X	X
	Запись	X	X	X			X
	Запрет доступа				X		
Пользователь ГИС «Электронная почтовая система Федерального агентства железнодорожного транспорта»	Чтение	X	X			X	X
	Запись	X	X	X			X
	Запрет доступа				X		
Пользователь ГИС «Официальный сайт Федерального агентства железнодорожного транспорта (www.roszeldor.ru)»	Чтение	X	X			X	X
	Запись	X	X	X			X
	Запрет доступа				X		
Пользователь ГИС «Информационная система пономерного учета пассажирских вагонов локомотивной тяги»	Чтение	X	X			X	X
	Запись	X	X	X			X
	Запрет доступа				X		
Пользователь ГИС «Информационная система пономерного учета локомотивов»	Чтение	X	X			X	X
	Запись	X	X	X			X
	Запрет доступа				X		

¹ Системные каталоги включают в себя директорию операционной системы (C:\Windows) а так же каталоги прикладного программного обеспечения (C:\Program files);

² К объектам профиля пользователя относят каталоги «Рабочий стол», «Мои документы», «Мои рисунки», а так же каталоги, в которых хранятся пользовательские настройки прикладного программного обеспечения «Application Data», «Local Settings» и другие;

³ К операциям записи так же относят модификацию, удаление и изменение прав доступа;

⁴ Запрет доступа имеет приоритет над остальными правами пользователя, в том числе групповыми.

Пользователь ГИС «Информационная система ведения перечней железнодорожных станций»	Чтение	X	X			X	X
	Запись	X	X	X			X
	Запрет доступа				X		
Пользователь ГИС «Информационная система обеспечения предоставления государственных услуг Федерального агентства железнодорожного транспорта»	Чтение	X	X			X	X
	Запись	X	X	X			X
	Запрет доступа				X		

Политика в отношении обработки персональных данных в центральном аппарате Федерального агентства железнодорожного транспорта

1. Настоящая Политика разработана в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152), постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ними нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» и устанавливает единый порядок обработки персональных данных субъектов, не являющихся государственными гражданскими служащими Федерального агентства железнодорожного транспорта (Росжелдор) в Росжелдоре.

2. В настоящей Политике используются следующие термины и понятия:

2.1. персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

2.2. обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;

2.3. информационная система персональных данных – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

2.4. обработка персональных данных без использования средств автоматизации (неавтоматизированная) – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

3. Руководитель Росжелдора назначает ответственных за организацию обработки персональных данных, обеспечивающих обработку персональных

данных в соответствии с требованиями Федерального закона № 152-ФЗ и других нормативных правовых актов Российской Федерации.

4. Обработка персональных данных осуществляется при выполнении следующих требований:

– после направления уведомления об обработке персональных данных в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций, за исключением случаев, предусмотренных частью 2 статьи 22 Федерального закона № 152-ФЗ;

– обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных за исключением случаев, предусмотренных частью 2 статьи 6 Федерального закона № 152-ФЗ;

– после принятия необходимых мер по защите персональных данных.

5. Государственные гражданские служащие Росжелдора, допущенные к обработке персональных данных, в обязательном порядке под роспись знакомятся с данной Политикой и другими локальными актами по вопросам обработки персональных данных и подписывают обязательство о неразглашении информации, содержащей персональные данные, по форме, утвержденной приказом Росжелдора.

6. Порядок определения защищаемой информации

6.1. Росжелдор создает в пределах своих полномочий, установленных в соответствии с федеральными законами государственные информационные системы, обрабатывающие персональные данные.

6.2. В Росжелдоре определяется и утверждается перечень сведений, содержащих персональные данные, и перечень государственных информационных систем, обрабатывающих персональные данные.

6.3. На стадии проектирования каждой государственной информационной системы, обрабатывающей персональные данные, определяются цели обработки и содержание персональных данных, утверждается перечень обрабатываемых персональных данных.

7. Порядок обработки персональных данных в государственных информационных системах персональных данных с использованием средств автоматизации

7.1. Обработка персональных данных в государственных информационных системах, обрабатывающих персональные данные Росжелдора с использованием средств автоматизации осуществляется в соответствии с требованиями постановления Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

7.2. Комиссией из работников Федерального казенного учреждения «Управление служебных зданий федеральных органов исполнительной власти» или Росжелдора, на которых возложены обязанности по обеспечению информационной безопасности в Росжелдоре, осуществляется определение уровня защищенности персональных данных, обрабатываемых в государственных информационных системах персональных данных, в соответствии с постановлением Правительства Российской Федерации от 01 ноября 2012 г.

№ 1119 в зависимости от категории обрабатываемых данных, их объема, наличия трудовых взаимоотношений субъектов персональных данных с Росжелдором и типа актуальных угроз.

7.3. Мероприятия по обеспечению безопасности персональных данных на стадиях проектирования и ввода в эксплуатацию объектов информатизации проводятся в соответствии с приказом ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и приказом ФСТЭК России от 18 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

7.4. Не допускается обработка персональных данных в государственных информационных системах с использованием средств автоматизации при отсутствии:

- утвержденных организационно-технических документов о порядке эксплуатации государственных информационных систем, обрабатывающих персональные данные, включающих акт по определению класса защищенности государственной информационной системы, акт по определению уровня защищенности персональных данных, инструкций пользователя и администратора, инструкций по организации парольной и антивирусной защиты, и других нормативных и методических документов;

- настроенных средств защиты от несанкционированного доступа, средств антивирусной защиты, средств межсетевой защиты, резервного копирования информации и других программных и технических средств в соответствии с техническим или частным техническим заданием на систему защиты информации;

- охраны и организации порядка допуска в помещения, в которых размещены технические средства для обработки и защиты персональных данных.

7.5. Росжелдор прекращает обработку персональных данных или обеспечивает прекращение их обработки лицом, действующим по поручению Росжелдора, в случаях:

- изменения, признания утратившими силу нормативных правовых актов, устанавливающих правовые основания обработки персональных данных;

- изменения или расторжения соглашений, заключенных Росжелдором во исполнение нормативных правовых актов, на основании которых осуществляется обработка персональных данных;

- выявления неправомерной обработки персональных данных, осуществляемой Росжелдором или лицом, действующим по поручению Росжелдора;

- достижения цели обработки персональных данных;

- отзыва субъектом персональных данных согласия на обработку его персональных данных, если в соответствии с законодательством Российской

Федерации обработка персональных данных допускается только с согласия субъекта персональных данных.

8. Обработка персональных данных, осуществляемая без использования средств автоматизации, выполняется в соответствии с требованиями, установленными постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

9. Лицам, допущенным к обработке персональных данных, запрещается:

– обрабатывать персональные данные в присутствии лиц, не допущенных к их обработке;

– осуществлять ввод персональных данных под диктовку.

10. Ответственность должностных лиц

10.1. Государственные гражданские служащие Росжелдора и работники подведомственных Росжелдору и подрядных организаций, допущенные к обработке персональных данных, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

УТВЕРЖДЕНО
приказом Росжелдора
от 31.10.2017 № 423

**Правила обработки и обеспечения защиты персональных данных
в центральном аппарате Федерального агентства железнодорожного
транспорта**

1. Общие положения

1.1. Настоящие Правила обработки и обеспечения защиты персональных данных (далее – Правила) в центральном аппарате Федерального агентства железнодорожного транспорта (далее – Росжелдор) устанавливают процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в области правил обработки и защиты персональных данных, (далее - ПДн), а также определяют для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований.

1.2. Целью настоящего документа является формирование общих правил для обеспечения защиты ПДн, обрабатываемых в государственных информационных системах Росжелдора, от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности персональных данных.

1.3. Правила разработаны в соответствии с Конституцией РФ, Трудовым кодексом РФ, Федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и иными нормативными правовыми актами в области обеспечения защиты ПДн, действующими на территории Российской Федерации.

1.4. В настоящем документе используются следующие термины:

- персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
- оператор (в данном случае Росжелдор) – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных

данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

– обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

– автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

– неавтоматизированная обработка персональных данных – обработка персональных данных субъекта без использования средств вычислительной техники;

– распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

– предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

– блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

– уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

– обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

– информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

– трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

– безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационной системе;

- контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств;
- конфиденциальность персональных данных – обязательное для соблюдения оператором или иным лицом, получившим доступ к персональным данным, требования не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.
- технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

2. Область действия

2.1. Правила являются обязательными для исполнения всеми государственными гражданскими служащими Росжелдора, осуществляющими обработку персональных данных и имеющих доступ к ним.

3. Обработка персональных данных субъектов персональных данных

3.1. Государственные гражданские служащие Росжелдора не имеют права получать и обрабатывать персональные данные субъектов, не соответствующие целям их обработки.

3.2. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются государственными гражданскими служащими Росжелдора.

3.3. Передавать персональные данные субъектов для обработки третьим лицам можно только после получения Росжелдором от субъекта персональных данных письменного согласия на передачу конкретному лицу (организации), кроме случаев, установленных действующим законодательством Российской Федерации. Передача персональных данных на материальном носителе информации фиксируется в соответствующих журналах работниками, ответственными за документооборот в Росжелдоре. Передача персональных данных в электронном

виде по защищенным каналам связи фиксируется в электронных журналах средств защиты информации.

3.4. Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

3.4.1. фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

3.4.2. фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

3.4.3. наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

3.4.4. цель обработки персональных данных;

3.4.5. перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

3.4.6. наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;

3.4.7. перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

3.4.8. срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

3.4.9. подпись субъекта персональных данных.

3.5. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных или в случае достижения целей обработки персональных данных государственный гражданский служащий Росжелдора, ответственный за организацию обработки и обеспечение безопасности персональных данных инициирует сбор, блокировку обработки с последующим уничтожением персональных данных субъекта, кроме случаев, установленных законодательством Российской Федерации.

3.6. При обработке персональных данных субъекта по его запросу могут быть предоставлены следующие данные:

- подтверждение факта обработки персональных данных в Росжелдоре;
- правовые основания и цели обработки персональных данных;
- применяемые в Росжелдоре способы обработки персональных данных;
- наименование и место нахождения Росжелдора, сведения о лицах (за исключением работников Росжелдора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Росжелдором или на основании Федерального закона;

- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом;
- наименование или фамилия, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Росжелдора, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные федеральными законами.

3.7. В случае получения запросов от уполномоченного органа по защите прав субъектов персональных данных в адрес Росжелдора работник, ответственный за организацию обработки и обеспечение безопасности персональных данных, обязан представить документы и локальные акты по обеспечению безопасности обработки персональных данных субъектов и (или) иным образом подтвердить принятие необходимых мер в течение тридцати дней с даты получения такого запроса.

3.8. В соответствии с законодательством Российской Федерации в целях обеспечения прав и свобод человека и гражданина Росжелдор при обработке персональных данных субъекта должны соблюдать следующие общие требования:

- обработка персональных данных должна осуществляться на законной и справедливой основе;
- обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;
- не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- обработке подлежат только персональные данные, которые отвечают целям их обработки;
- содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки;
- при обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Росжелдор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных;
- хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат

уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом;

– при определении объема и содержания обрабатываемых персональных данных Росжелдор должен руководствоваться действующим законодательством Российской Федерации и локальными нормативными актами Росжелдора;

– при принятии решений, затрагивающих интересы субъекта, Росжелдор не имеет права основываться на персональных данных субъекта, полученных исключительно в результате их автоматизированной обработки или электронного получения;

– защита персональных данных субъекта от неправомерного их использования или утраты обеспечивается Росжелдором в порядке, установленном действующим законодательством Российской Федерации;

– государственные гражданские служащие Росжелдора должны быть ознакомлены под роспись с организационно-распорядительными документами Росжелдора, устанавливающими порядок обработки и защиты персональных данных, а также об их правах и обязанностях в этой области;

– доступ государственных гражданских служащих Росжелдора к персональным данным субъектов персональных данных в информационных системах регламентируется только на основании локальных нормативных актов Росжелдора с указанием перечня допущенных лиц, прав доступа, необходимых для выполнения служебных обязанностей;

– обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ;

– уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных, с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление);

– уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе; а если это не допускается техническими особенностями материального носителя, путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными;

– при хранении материальных носителей персональных данных должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним.

3.9. При передаче персональных данных субъекта государственными гражданскими служащими Росжелдора должны соблюдаться следующие требования:

- не сообщать персональные данные субъекта третьей стороне без его письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, установленных Федеральным законом;
- осуществлять передачу персональных данных субъектов в пределах Росжелдора в соответствии с нормативными документами внутреннего документооборота.

3.10. Допускается передача персональных данных субъектов сторонним организациям, если данная передача обусловлена Федеральным законом либо соответствующим соглашением и не нарушает прав субъекта персональных данных.

3.11. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных Росжелдор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Росжелдора) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных Росжелдор обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Росжелдора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

3.12. В случае подтверждения факта неточности персональных данных Росжелдор на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Росжелдора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

3.13. В случае выявления неправомерной обработки персональных данных, осуществляемой Росжелдором или лицом, действующим по поручению Росжелдора, Росжелдор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению Росжелдора. В случае, если обеспечить правомерность обработки

персональных данных невозможно, Росжелдор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Росжелдор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя, либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

3.14. В случае достижения цели обработки персональных данных Росжелдор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Росжелдора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Росжелдора) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом или другими федеральными законами.

3.15. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Росжелдор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению Росжелдора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Росжелдора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом от 27 июля 2006 г. № 152-ФЗ или другими федеральными законами.

3.16. В случае отсутствия возможности уничтожения персональных данных в течение установленного срока, Росжелдор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Росжелдора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

3.17. Государственные гражданские служащие Росжелдора несут персональную ответственность за сохранность персональных данных, к которым они имеют доступ.

3.18. Государственные гражданские служащие Росжелдора, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, могут быть привлечены к ответственности, предусмотренной действующим законодательством Российской Федерации и локальными нормативными актами Росжелдора.

4. Оценка угроз безопасности информации

4.1. Материальными носителями персональных данных, применяющимися в технических средствах и системах, являются: бумажные носители и накопители на жестких магнитных дисках.

4.2. Основные виды угроз и источники угроз безопасности представлены в частных моделях угроз безопасности для каждой государственной информационной системы Росжелдора.

5. Цели и сроки обработки данных в информационных системах персональных данных

5.1. Цели и сроки хранения данных в государственных информационных системах персональных данных Росжелдора определяются в рамках каждой государственной информационной системы персональных данных отдельно в соответствующей модели угроз, утверждаемой в установленном порядке, с обязательным указанием нормативных документов, регламентирующих сроки хранения. Основным документом, регламентирующим сроки хранения, является Федеральный закон Российской Федерации от 22 октября 2004 г. № 125-ФЗ «Об архивном деле в Российской Федерации».

6. Организационные мероприятия по защите персональных данных при их обработке в государственных информационных системах персональных данных Росжелдора

6.1. Организационные мероприятия по защите персональных данных связаны с формированием пакета документов по защите персональных данных, их разработкой, официальным оформлением и доведением до исполнителей, а также организацией контроля за соблюдением установленных этими документами правил и требований. Состав внутренних документов, разрабатываемых на основании действующего законодательства Российской Федерации и локальных нормативных актов Росжелдора, определяется на этапе приведения процессов обработки персональных данных в Росжелдора в соответствие требованиям законодательства. Состав документов определяется Росжелдором при возможном привлечении организаций-лицензиатов.

6.2. Мероприятия должны исключить возможность утечки информации, обрабатываемой в государственных информационных системах персональных

данных Росжелдора, и обеспечить запрет передачи персональных данных по открытым каналам связи без применения установленных мер по ее защите, а также исключить возможность внесения в контролируруемую зону устройств регистрации и накопления информации без соответствующего разрешения.

6.3. Обязанность поддерживать комплект документов по защите персональных данных в актуальном состоянии возлагается на ответственного за организацию обработки и обеспечение безопасности персональных данных.

6.4. Организационные мероприятия по защите персональных данных, обрабатываемых на автоматизированных рабочих местах государственных гражданских служащих Росжелдора, должны быть связаны с обеспечением:

- ограничения физического доступа и контроля доступа к техническим средствам, обрабатывающим персональные данные;
- сохранности съемных и машинных носителей информации, материалов печати и исключения доступа к ним посторонних лиц;
- исключения возможностей несанкционированного просмотра изображений с монитора автоматизированного рабочего места через дверные проемы, окна – в том числе с использованием средств телевизионной, фотографической и визуальной оптической разведки, находящихся за границами контролируемой зоны;
- режима блокирования доступа к автоматизированному рабочему месту во время отсутствия государственного гражданского служащего на месте;
- режима блокирования доступа в помещение с установленным автоматизированным рабочим местом в рабочее время при отсутствии государственного гражданского служащего на месте.

6.5. Организационные мероприятия по защите персональных данных в локальных вычислительных сетях Росжелдора должны осуществлять:

- обеспечение режима запрета на входение в локально вычислительную сеть под чужой учетной записью;
- обеспечение периодической смены паролей пользователями;
- обеспечение хранения файлов с информацией в групповых каталогах (каталогах, информация в которых является доступной для определенной группы лиц), структура которых однозначно отображает организационную структуру управления/отдела, и разрешения доступа к нему только государственных гражданских служащих соответствующей структурной единицы;
- обеспечение файлового обмена информацией между пользователями управления/отдела через создаваемый каталог общего использования, информация в котором является доступной для имеющих санкционированный доступ в локально-вычислительной сети пользователей;
- обеспечение контроля присвоения пользователям учетных записей и их удаление или блокирование при увольнении государственного гражданского служащего Росжелдора;
- обеспечение резервного копирования электронных информационных ресурсов;

– обеспечение режима разграничения и контроля доступа к аппаратным и программным ресурсам локальных вычислительных сетей и автоматизированных рабочих мест.

7. Технические мероприятия по защите персональных данных

7.1. Технические мероприятия по защите информации разрабатываются по результатам обследования автоматизированных государственных информационных систем персональных данных, предназначенных для обработки персональных данных, и оценки возможностей обеспечения защиты на основе применения организационных мер защиты и активизации встроенных механизмов защиты используемых операционных систем и аппаратного обеспечения.

7.2. Требуется осуществлять следующие технические мероприятия:

- применение сертифицированных средств антивирусной защиты;
- применение сертифицированных программных и (или) аппаратных средств защиты информации от несанкционированного доступа, контроля целостности, регистрации и учета действий пользователей государственных информационных систем персональных данных Росжелдора;
- защита персональных данных при межсетевом взаимодействии с использованием сертифицированных средств защиты;
- применение сертифицированных средств для организации защищенного канала для передачи персональных данных по каналам связи;
- предотвращение несанкционированной записи персональных данных на съемные носители информации или вывода персональных данных на печать;
- регулярный мониторинг и контроль защищенности системы защиты информации.

8. Контроль состояния системы защиты персональных данных

8.1. В рамках проверок состояния защиты персональных данных рекомендуется осуществлять контроль:

- наличия в управлениях нормативных документов по защите информации и доведения их до государственных гражданских служащих под роспись;
- знания и выполнения государственными гражданскими служащими требований локальных нормативных актов Росжелдора по защите персональных данных при их обработке в государственных информационных системах Росжелдора;
- наличия и комплектности эксплуатационной и технической документации на систему защиты информации, а также факта ознакомления государственных гражданских служащих Росжелдора и работников подведомственных и подрядных организаций с инструкциями пользователя и администратора государственной информационной системы, а также инструкцией администратора информационной безопасности с соответствующей отметкой об ознакомлении в инструкциях;

- работоспособности системы защиты информации;
- определение (актуализация) требований по безопасности персональных данных при разработке (модернизации) государственных информационных систем персональных данных Росжелдора.

8.2. Контроль за состоянием системы защиты персональных данных осуществляется в плановом и внеплановом порядке ответственным за организацию обработки и обеспечение безопасности персональных данных, назначаемым руководителем Росжелдора.

9. План контрольных мероприятий

9.1. С целью выявления и предотвращения нарушений законодательства Российской Федерации в сфере защиты персональных данных, ответственными за организацию обработки и обеспечение безопасности персональных данных проводятся контролирующие мероприятия в соответствии с планом мероприятий по обеспечению защиты персональных данных.

9.2. При возникновении внештатных ситуаций, повлекших несанкционированное уничтожение данных, нарушение целостности и другие несанкционированные изменения информации, проводятся внеплановые контролирующие мероприятия.

**Регламент рассмотрения запросов субъектов персональных данных
или их представителей об обработке их персональных данных в центральном
аппарате Федерального агентства железнодорожного транспорта**

1. Общие положения

1.1. Регламент рассмотрения запросов субъектов персональных данных или их представителей об обработке их персональных данных в центральном аппарате Федерального агентства железнодорожного транспорта (далее – Регламент) разработан в соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – федеральный закон № 152-ФЗ) и определяет порядок работы с запросами субъектов персональных данных или их представителей, об обработке Федеральным агентством железнодорожного транспорта (далее – Росжелдор или оператор) их персональных данных (далее – ПДн).

1.2. Настоящий регламент определяет порядок получения государственным гражданским служащим Росжелдора (далее – работник) запросов субъектов ПДн, порядок обработки запросов ответственными в этой компетенции работниками, порядок формирования ответов на запросы, а также порядок передачи ответов на запросы субъектам ПДн.

2. Порядок обращения субъекта ПДн к Росжелдору

2.1. Субъект ПДн имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

2.1.1. подтверждение факта обработки персональных данных Росжелдором;

2.1.2. правовые основания и цели обработки персональных данных;

2.1.3. цели и применяемые оператором способы обработки персональных данных;

2.1.4. наименование и место нахождения Росжелдора, сведения о лицах (за исключением работников Росжелдора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Росжелдором или на основании федерального закона;

2.1.5. обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

2.1.6. сроки обработки персональных данных, в том числе сроки их хранения;

2.1.7. порядок осуществления субъектом персональных данных прав, предусмотренных федеральным законом № 152-ФЗ;

2.1.8. информацию об осуществленной или о предполагаемой трансграничной передаче данных;

2.1.9. наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Росжелдора, если обработка поручена или будет поручена такому лицу;

2.1.10. иные сведения, предусмотренные федеральным законом № 152-ФЗ или другими федеральными законами.

2.2. Запрос может поступить как в письменном, так и в устном виде.

2.3. Запрос субъекта ПДн на предоставление информации, должен содержать следующую обязательную информацию:

– номер основного документа, удостоверяющего личность субъекта ПДн или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта ПДн или его законного представителя;

– реквизиты доверенности законного представителя субъекта ПДн или иного документа, предусмотренного действующим законодательством Российской Федерации, на основании которого действует законный представитель;

– сведения, подтверждающие участие субъекта ПДн в отношениях с Росжелдором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки ПДн Росжелдором.

2.4. При предъявлении письменного запроса субъект ПДн обязан предъявить основной документ, удостоверяющий личность субъекта ПДн, а законный представитель субъекта ПДн должен предъявить оригинал нотариально заверенной доверенности от субъекта ПДн (или иной документ, предусмотренный действующим законодательством Российской Федерации) с указанием полномочий, в том числе получение сведений от Росжелдора, и предоставить работнику Росжелдора заверенную копию вместе с запросом.

2.5. При устном запросе субъекта ПДн с требованием предоставить информацию о наличии ПДн работник, ответственный за организацию обработки и обеспечение безопасности ПДн, обязан предоставить субъекту ПДн бланк запроса, форма которого должна быть утверждена Росжелдором в установленном порядке. Учитывая тот факт, что в запросе содержится конфиденциальная информация субъекта, работник, ответственный за организацию обработки и обеспечение безопасности ПДн, обязан предоставить субъекту конверт для помещения запроса.

2.6. В случае получения запроса от субъекта ПДн почтовым отправлением работник, получивший запрос, обязан направить его в адрес работника, ответственного за организацию обработки и обеспечение безопасности ПДн, либо уполномоченного им работника.

2.7. Все обращения субъектов ПДн должны быть переданы работнику, ответственному за организацию обработки и обеспечение безопасности ПДн, либо уполномоченному им работнику в течение 1 (одного) рабочего дня от даты получения запроса с приложением пояснительной записки в свободной форме, содержащей сведения о том кто из работников, когда и при каких обстоятельствах получил на руки запрос субъекта.

2.8. В случае получения запроса в электронной форме и подписанного электронной подписью в соответствии с требованиями федеральных законов

Российской Федерации также инициализируется процедура ответа субъекту в порядке, предусмотренном Регламентом.

2.9. Сведения по запросам субъектов должны быть предоставлены субъекту ПДн в доступной форме, и в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн.

2.10. В случае, если сведения, указанные в части 7 статьи 14 федерального закона № 152-ФЗ, а также обрабатываемые ПДн были предоставлены для ознакомления субъекту ПДн по его запросу, субъект ПДн вправе обратиться повторно или направить повторный запрос в целях получения сведений, указанных в части 7 статьи 14 федерального закона № 152-ФЗ, и ознакомления с такими ПДн не ранее чем через 30 (тридцать) дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законодательством Российской Федерации, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн.

2.11. Субъект ПДн вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных в части 7 статьи 14 федерального закона № 152-ФЗ, а также в целях ознакомления с обрабатываемыми ПДн до истечения 30 дней, в случае, если такие сведения и (или) обрабатываемые ПДн не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в части 7 статьи 14 федерального закона № 152-ФЗ, должен содержать обоснование направления повторного запроса.

2.12. Росжелдор вправе отказать субъекту ПДн в выполнении повторного запроса, не соответствующего условиям, описанным выше. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Росжелдоре.

3. Порядок регистрации запроса субъекта ПДн

3.1. Работник, ответственный за организацию обработки и обеспечение безопасности ПДн, в день получения запроса обязан зарегистрировать принятый запрос в журнал учета обращений субъектов ПДн по выполнению их законных прав учреждением (далее – журнал) по форме, утвержденной Росжелдором.

3.2. Журнал должен быть пронумерован, прошит, скреплен печатью и подписью уполномоченного работника.

3.3. Все запросы и ответы на них должны храниться в сейфе работника, ответственного за организацию обработки и обеспечение безопасности ПДн, или в специальном помещении учреждения, защищенном от несанкционированного доступа третьих лиц.

4. Проверка наличия/отсутствия ПДн субъекта ПДн в государственных информационных системах ПДн Росжелдора

4.1. По факту регистрации запроса работник, ответственный за организацию обработки и обеспечение безопасности ПДн, внимательно изучает запрос на предмет соответствия требованиям Положения об обработке и обеспечении защиты персональных данных, утвержденного Росжелдором, и действующего законодательства Российской Федерации.

4.2. В случае, если запрос оформлен ненадлежащим образом, а именно: в нем отсутствует информация о субъекте ПДн, подпись субъекта или его законного представителя или иная информация, которая должна быть отражена в соответствии с настоящим Регламентом, то работник, ответственный за организацию обработки и обеспечение безопасности ПДн, либо уполномоченное им лицо оформляет отказ в предоставлении информации.

4.3. В случае, если запрос оформлен в соответствии с требованиями законодательства Российской Федерации, то работник, ответственный за организацию обработки и обеспечение безопасности ПДн с привлечением пользователей государственной информационной системы ПДн, в которой обрабатывается искомая информация, находит всю информацию о субъекте ПДн и собирает данные по ПДн субъекта или констатирует факт, что ПДн о субъекте в государственной информационной системе ПДн отсутствуют. В зависимости от результатов поиска ПДн субъекта ПДн работник, ответственный за обработку запросов, составляет ответ на запрос субъекта ПДн.

4.4. Работник, ответственный за организацию обработки и обеспечение безопасности ПДн, в целях скорейшего сбора информации может направить запрос о субъекте пользователям государственных информационных систем ПДн Росжелдора по электронной почте, поставив в копию непосредственного руководителя отдела. Пользователи государственных информационных систем ПДн учреждения должны в течение 5 суток отреагировать на запрос ответственного за обработку запросов работника и предоставить всю информацию по субъекту ПДн, а если она отсутствует – сообщить об этом.

5. Оформление и содержание ответа на запрос при наличии или отсутствии ПДн субъекта в государственных информационных системах ПДн Росжелдора

5.1. В случае, если в государственных информационных системах Росжелдора имеется или отсутствует информация о ПДн субъекта, обратившегося с запросом, работник, ответственный за обработку запроса, составляет ответ на запрос субъекта в произвольной форме по существу вопросов.

5.2. Работник, ответственный за организацию обработки и обеспечение безопасности ПДн, либо уполномоченное им лицо:

– подписывает ответ на запрос по ПДн субъекта, ставит печать учреждения, упаковывает в конверт для отправки посредством почтового отправления либо готовит ответ для вручения субъекту ПДн или его законному представителю способом, указанным в запросе, под подпись;

– дубликат ответа прикладывается к запросу и хранится вместе с запросом;

– в журнале учета обращений субъектов ПДн по выполнению их законных прав делается отметка об ответе на запрос, краткое содержание ответа (положительный, отрицательный, отказ), отражает дату отправления ответа, способ его отправления (почтовое отправление, лично в руки субъекту или его законному представителю), а также ставит свою подпись.

5.3. Срок ответа на запрос субъекта ПДн не может превышать 30 (тридцать) календарных дней от даты получения запроса от субъекта, если иной срок не будет установлен действующим законодательством Российской Федерации.

УТВЕРЖДЕНО
приказом Росжелдора
от 31.10.2017 № 423

В Федеральное агентство
железнодорожного транспорта

От _____

Адрес: _____

Паспорт № _____ выдан _____

**Запрос
на предоставление сведений
об обработке персональных данных субъекта персональных данных**

В соответствии со статьей 14 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», я имею право получить от вас сведения об обработке моих персональных данных.

Прошу вас предоставить мне следующую информацию:

1. осуществляется ли обработка моих персональных данных;
2. цель обработки моих персональных данных;
3. перечень обрабатываемых вами моих персональных данных и источников их получения;
4. способы обработки моих персональных данных;
5. сведения о лицах, которые имеют доступ к моим персональным данным или которым может быть предоставлен такой доступ;
6. сроки обработки моих персональных данных, в том числе сроки их хранения.

Ответ на настоящий запрос прошу направить в письменной форме по вышеуказанному адресу в предусмотренный законом срок.

« ____ » _____ 20__ г.

_____ (подпись)

_____ (И.О. Фамилия)

УТВЕРЖДЕНО
приказом Росжелдора
от 31.10.2017 № 423

Журнал

учета обращений субъектов персональных данных о выполнении их законных прав, при обработке персональных данных в государственных информационных системах Федерального агентства железнодорожного транспорта

Ответственный _____

(Должность)

(Подпись)

(ФИО)

Начат: « ___ » _____ 20__ г.
Окончен: « ___ » _____ 20__ г.

На ___ листах

УТВЕРЖДЕНО
приказом Росжелдора
от 31.10.2017 № 423

**Регламент предоставления прав доступа к информации ограниченного доступа,
не содержащей государственную тайну, обрабатываемой в государственных
информационных системах Федерального агентства железнодорожного
транспорта**

1. Выдача пользователям учетных записей и паролей для доступа к средствам вычислительной техники государственных информационных систем Федерального агентства железнодорожного транспорта осуществляется администратором государственной информационной системы или администратором информационной безопасности.

2. Полная плановая смена паролей в государственных информационных системах проводится не реже одного раза в месяц пользователями самостоятельно. Правила смены и формирования паролей описаны в «Инструкции по организации парольной защиты в государственных информационных системах Федерального агентства железнодорожного транспорта».

3. Настройка прав доступа к информационным ресурсам государственных информационных систем осуществляется администратором информационной безопасности в зависимости от должностных обязанностей государственного гражданского служащего или работника подведомственной организации, и прав на обработку персональных данных, прописанных в «Перечне лиц, допущенных к автоматизированной обработке персональных данных, обрабатываемых в государственных информационных системах Федерального агентства железнодорожного транспорта».

4. Администратор информационной безопасности осуществляет контроль за предоставленными правами на доступ к защищаемой информации с целью исключения возможных нарушений, а также контроль над работой средств защиты информации, ограничивающих права пользователей.

5. Отзыв или перенастройка прав доступа работников в случае увольнения или изменения их должности и функциональных обязанностей, также возлагается на администратора информационной безопасности.

**Инструкция
по организации антивирусной защиты
в государственных информационных системах
Федерального агентства железнодорожного транспорта**

1. Общие положения

1.1. Инструкция по организации антивирусной защиты (далее – Инструкция) определяет требования к организации защиты государственных информационных систем в центральном аппарате Федерального агентства железнодорожного транспорта (Росжелдор) от разрушающего воздействия компьютерных вирусов.

1.2. К использованию в Росжелдоре допускаются только сертифицированные лицензионные антивирусные средства.

1.3. Установка и настройка средств антивирусного контроля и защиты на серверах и автоматизированных рабочих местах (далее – АРМ) государственных информационных систем осуществляется администратором информационной безопасности.

2. Применение средств антивирусного контроля

2.1. Антивирусный контроль всех дисков и файлов рабочих станций должен проводиться 1 раз в сутки в автоматическом режиме.

2.2. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, лентах, CD - ROM и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее получения. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

2.3. Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

2.4. Установка (изменение) системного и прикладного программного обеспечения осуществляется в соответствии с Перечнем разрешенного к использованию программного обеспечения.

2.5. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка на защищаемых серверах и АРМах

государственных информационных систем персональных данных администратором информационной безопасности.

3. Действия при обнаружении вирусов

3.1. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) государственный гражданский служащий Росжелдора вместе с администратором информационной безопасности должен провести внеочередной антивирусный контроль своего АРМа.

3.2. В случае обнаружения при проведении антивирусной проверки файлов, зараженных компьютерными вирусами, необходимо:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов, владельца зараженных файлов, а также смежные отделы/управления, использующие эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов вместе администратором информационной безопасности.

4. Ответственность

4.1. Ответственность за организацию антивирусного контроля и защиты в Росжелдоре, в соответствии с требованиями настоящей Инструкции возлагается на администратора информационной безопасности.

4.2. Ответственность за проведение мероприятий антивирусного контроля и защиты в Росжелдоре, и соблюдение требований настоящей Инструкции возлагается на администратора информационной безопасности и всех пользователей государственных информационных систем персональных данных Росжелдора.

4.3. Периодический контроль состояния антивирусной защиты, а также соблюдения установленного порядка антивирусного контроля и выполнения требований настоящей Инструкции осуществляется администратором информационной безопасности.

**Инструкция
по организации парольной защиты
в государственных информационных системах
Федерального агентства железнодорожного транспорта**

1. Общие положения

1.1. Первоначально личные пароли доступа к средствам вычислительной техники государственных информационных систем пользователям выдаются администратором информационной безопасности.

1.2. Полная плановая смена паролей в государственных информационных системах проводится не реже одного раза в месяц пользователями самостоятельно.

2. Правила формирования пароля

2.1. Пароль не может содержать имя учетной записи пользователя или какую-либо его часть.

2.2. Пароль должен состоять не менее чем из 8 символов.

2.3. В пароле должны присутствовать символы трех категорий из числа следующих четырех:

- прописные буквы английского алфавита от А до Z;
- строчные буквы английского алфавита от а до z;
- десятичные цифры (от 0 до 9);
- символы, не принадлежащие алфавитно-цифровому набору (например, !, \$, #, %).

2.4. Запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а также имена и даты рождения свои и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе.

2.5. Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов.

2.6. Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.).

2.7. Запрещается использовать один и тот же пароль несколько раз.

3. Правила ввода пароля

3.1. Ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан.

3.2. Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамерами и др.).

4. Правила хранения пароля

4.1. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах.

4.2. Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

5. Обязанности работников

5.1. Лица, использующие паролирование, обязаны:

- четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по паролированию;
- своевременно сообщать администратору информационной безопасности об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

**Инструкция пользователя
государственной информационной системы персональных данных
Федерального агентства железнодорожного транспорта**

1. Общие положения

1.1. Пользователь, обрабатывающий персональные данные (далее – Пользователь), осуществляет обработку персональных данных в государственной информационной системе Федерального агентства железнодорожного транспорта (Росжелдор), обрабатывающей персональные данные.

1.2. Пользователем является каждый государственный служащий Росжелдора, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, персональным данным и средствам защиты информации.

1.3. Пользователь несет персональную ответственность за свои действия.

1.4. Пользователь в своей работе руководствуется настоящей инструкцией, политикой в отношении обработки персональных данных и другими локальными актами Росжелдора по обеспечению защиты персональных данных, а также руководящими и нормативными документами ФСТЭК России.

1.5. Методическое руководство по работе пользователя (в части информационной безопасности) осуществляется администратором информационной безопасности.

2. Должностные обязанности Пользователя

2.1. Пользователь обязан:

2.1.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних локальных актов Росжелдора по защите персональных данных.

2.1.2. Выполнять на автоматизированном рабочем месте только те процедуры, которые определены для него в Перечне лиц, допущенных к автоматизированной обработке персональных данных, обрабатываемых в государственных информационных системах Федерального агентства железнодорожного транспорта.

2.1.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету и хранению персональных данных, обеспечению безопасности персональных данных, а также руководящих и организационно-распорядительных документов.

2.1.4. Соблюдать инструкции антивирусной и парольной защиты.

2.1.5. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, жалюзи на окнах должны быть закрыты.

2.1.6. Обо всех выявленных нарушениях, связанных с информационной безопасностью в Росжелдоре, а также для получения консультаций по вопросам информационной безопасности, необходимо обращаться к администратору информационной безопасности.

2.1.7. Для получения консультаций по вопросам работы и настройке элементов государственных информационных систем, обрабатывающих персональные данные, необходимо обращаться к администратору данных систем.

2.1.8. При отсутствии визуального контроля над автоматизированным рабочим местом, доступ к компьютеру должен быть немедленно заблокирован.

2.1.9. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в рамках возложенных на него функций.

2.2. Пользователям запрещается:

2.2.1.1. Разглашать защищаемую информацию третьим лицам.

2.2.1.2. Копировать защищаемую информацию на внешние носители без разрешения своего руководителя.

2.2.1.3. Самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.

2.2.1.4. Несанкционированно открывать общий доступ к папкам на своем рабочем месте.

2.2.1.5. Подключать к автоматизированному рабочему месту и корпоративной информационной сети личные внешние носители и мобильные устройства.

2.2.1.6. Отключать (блокировать) средства защиты информации.

2.2.1.7. Обработать на автоматизированном рабочем месте информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к персональным данным.

2.2.1.8. Сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам государственных информационных систем, обрабатывающих персональные данные.

2.2.1.9. Привлекать посторонних лиц для производства ремонта или настройки автоматизированного рабочего места, без согласования администратора информационной безопасности.

УТВЕРЖДЕНО
приказом Росжелдора
от 31.10.2017 № 423

**Согласие субъекта персональных данных
на обработку персональных данных**

В соответствии с требованиями части 4 статьи 9 Федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных»,

Я, _____,
(фамилия, имя, отчество)

документ удостоверяющий личность _____ № _____,
(вид документа)

выдан _____,
(кем и когда)

зарегистрированный(ая) по адресу: _____,

даю свое согласие Федеральному агентству железнодорожного транспорта, зарегистрированному по адресу: 105064, г. Москва, ул. Старая Басманная, д. 11/2 стр. 1 на обработку своих персональных данных, на следующих условиях:

1. Данное согласие дается на обработку персональных данных, как без использования средств автоматизации, так и с их использованием.

2. В ходе обработки с персональными данными могут быть совершены следующие действия: сбор, запись, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, удаление, уничтожение.

3. Обработка персональных данных может осуществляться исключительно в моих интересах, а также в целях обеспечения соблюдения законов и иных нормативных правовых актов.

Мне гарантируется конфиденциальность моих персональных данных при их обработке, за исключением, если мои персональные данные обезличены и (или) являются общедоступными.

Передача моих персональных данных третьим лицам возможна в моих интересах в рамках межведомственного взаимодействия, а также в иных, предусмотренных законом случаях.

Данное согласие действует со дня его подписания до дня отзыва в письменной форме.

Я оставляю за собой право отозвать свое согласие посредством составления соответствующего письменного заявления, которое может быть направлено мной в адрес Федерального агентства железнодорожного транспорта по почте заказным письмом с уведомлением о вручении, либо вручено лично под расписку уполномоченному представителю Федерального агентства железнодорожного транспорта.

Настоящим подтверждаю, что ознакомлен(а) с положениями Федерального закона от 27 июля 2006 г. N 152-ФЗ «О персональных данных», права и обязанности в области защиты персональных данных мне разъяснены.

" ____ " _____ 20 ____ г.

(подпись)

(фамилия, инициалы)

УТВЕРЖДЕНО
приказом Росжелдора
от 31.10.2017 № 423

**Обязательство о соблюдении режима защиты персональных данных
в центральном аппарате Федерального агентства железнодорожного
транспорта**

Я, _____,

работая в должности _____

в Федеральном агентстве железнодорожного транспорта, обязуюсь:

1. Не разглашать, не раскрывать публично, а также соблюдать установленный Политикой в отношении обработки персональных данных в центральном аппарате Федерального агентства железнодорожного транспорта, порядок передачи третьим лицам сведений, составляющих персональные данные субъектов персональных данных, которые мне будут доверены или станут известны по работе.

2. Выполнять относящиеся ко мне требования Политики в отношении обработки персональных данных, приказов, распоряжений, инструкций и других локальных нормативных актов по обеспечению конфиденциальности персональных данных субъектов персональных данных и соблюдению правил их обработки.

3. В случае попытки посторонних лиц получить от меня сведения, составляющие персональные данные субъекта персональных данных, немедленно сообщить ответственному за организацию обработки и обеспечение безопасности персональных данных.

4. В случае моего увольнения, все носители, содержащие персональные данные субъектов персональных данных (документы, копии документов, дискеты, диски, магнитные ленты, распечатки на принтерах, черновики и пр.), которые находились в моем распоряжении в связи с выполнением мною служебных обязанностей во время работы у работодателя, передать руководителю структурного подразделения или другому работнику по указанию руководителя структурного подразделения.

5. Об утрате или недостатке документов, или иных носителей, содержащих персональные данные субъектов персональных данных (удостоверений, пропусков и т.п.), ключей от хранилищ, сейфов (металлических шкафов) и о других фактах, которые могут привести к разглашению персональных данных субъектов персональных данных, а также о причинах и условиях возможной утечки сведений немедленно сообщить руководителю структурного подразделения.

Я ознакомлен под роспись с Политикой в отношении обработки персональных данных в центральном аппарате Федерального агентства железнодорожного транспорта.

Мне известно, что нарушение мною обязанностей по защите персональных данных субъектов персональных данных может повлечь дисциплинарную, гражданско-правовую, уголовную и иную ответственность в соответствии с законодательством Российской Федерации.

« ____ » _____ 20__ г.

Подпись

ФИО

Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в центральном аппарате Федерального агентства железнодорожного транспорта

1. Назначение и область действия

1.1. Порядок резервирования и восстановления работоспособности технических средств, программного обеспечения, баз данных и систем защиты информации в центральном аппарате Федерального агентства железнодорожного транспорта (далее – Порядок) определяет действия, связанные с функционированием государственных информационных систем (далее – ГИС) Федерального агентства железнодорожного транспорта (Росжелдор), меры и средства поддержания непрерывности работы и восстановления работоспособности ГИС.

1.2. Целью настоящего документа является превентивная защита элементов ГИС от предотвращения потери защищаемой информации, определение мер защиты от потери информации, определение действий восстановления в случае потери информации.

1.3. Действие настоящего Порядка распространяется на всех пользователей, имеющих доступ к ресурсам ГИС, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

- системы жизнеобеспечения ГИС;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

1.4. Ответственными работниками за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, назначаются:

- работники, обрабатывающие персональные данные;
- руководители подразделений Росжелдора, в которых производится обработка персональных данных;
- работники ответственные за организацию обработки и обеспечение безопасности персональных данных, обрабатываемых в информационных системах Росжелдора.

2. Порядок реагирования на инцидент

2.1. В настоящем Порядке под инцидентом понимается любое происшествие, связанное со сбоем в функционировании элементов ГИС, а также потерей защищаемой информации.

2.2. Происшествие, вызывающее инцидент, может произойти:

- в результате непреднамеренных действий пользователей;
- в результате преднамеренных действий пользователей и третьих лиц;
- в результате нарушения правил эксплуатации технических и программных средств ГИС;
- в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

2.3. В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование работники предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с непосредственным руководителем. По необходимости, иерархия согласования может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

3. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов

3.1. Техническими мерами для обеспечения непрерывной работы и восстановления является использование систем для предотвращения потери информации (включающих программные и технические средства), таких как:

- системы жизнеобеспечения ГИС;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

3.2. Системы жизнеобеспечения ГИС включают:

- пожарные сигнализации и системы пожаротушения;
- системы резервного питания.

3.3. Все помещения, в которых размещаются элементы ГИС и средства защиты, должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

3.4. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ГИС: ПЭВМ, сетевое и коммуникационное оборудование должны подключаться к сети электропитания через источники бесперебойного питания.

3.5. Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках.

3.6. Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердых носителях (жесткий магнитный диск, лазерный диск, флэшку).

3.7. Резервное копирование и хранение данных должно осуществляться на периодической основе:

- для обрабатываемых персональных данных – не реже 1 раза в неделю;

- для технологической информации – не реже 1 раза в месяц;
- эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты) – каждый раз при внесении изменений в эталонные копии (выход новых версий).

3.8. Носители должны храниться в негорючем шкафу или помещении, оборудованном системой пожаротушения.

Регламент проведения технического обслуживания в центральном аппарате Федерального агентства железнодорожного транспорта

1. Общие положения

1.1. В настоящем Регламенте проведения технического обслуживания (далее – Регламент) излагаются порядок и правила выполнения работ по техническому обслуживанию (далее – ТО) оборудования и программного обеспечения, находящегося в эксплуатации в центральном аппарате Федерального агентства железнодорожного транспорта (далее - Росжелдор).

1.2. ТО вычислительной техники и периферийного оборудования направлено на обеспечение постоянной готовности оборудования к использованию по прямому назначению и предотвращение преждевременного выхода его из строя.

1.3. При выполнении ТО оборудования должны дополнительно использоваться эксплуатационные документы на изделия (Приложения №№ 1-4 к Регламенту), входящие в состав аппаратных комплексов.

2. Организация работ

2.1. ТО проводится на оборудовании, имеющем инвентарные номера.

2.2. Поддержание работоспособности вычислительной техники, установленного лицензионного программного обеспечения, осуществляется работниками отдела информатизации федерального казенного учреждения «Управление служебных зданий федеральных органов исполнительной власти в области транспорта» (ФКУ УСЗ) или специалистами обслуживающей организации по вызовам или в соответствии с графиком проведения плановых профилактических работ.

2.3. Количество внеплановых выездов по устранению неполадок в работе оборудования и программного обеспечения не ограничено.

2.4. Время реакции на внеплановые вызовы не должно превышать 2 часа.

2.5. Восстановление работоспособности неисправного оборудования не должно превышать 8 часов, с момента получения заявки, исключение составляют работы требующие замены деталей, механизмов или блоков устройств.

2.6. Допуск к обслуживаемому оборудованию осуществляется в присутствии ответственного лица, за которым закреплено оборудование.

2.7. Факт выполнения ТО оборудования фиксируется в паспорте технического средства и в акте выполненных работ.

2.8. В случае выявления дефектов оборудования (печатающие, множительные устройства, мониторы, источники бесперебойного питания, сканеры, факсимильные аппараты), которые не могут быть устранены на площадке пользователя, техническое средство (с согласия материально-ответственного лица) должно быть изъято для ремонта в лабораторных условиях после составления акта

изъятия технического средства (согласно Приложению 2 к Регламенту). После выполнения ремонтных работ составляется акт возврата технического средства (Приложение № 3 к Регламенту). Акты изъятия и возврата технического средства составляются в двух экземплярах и хранятся у лица, за которым закреплена техника.

Все действия по ремонту и обслуживанию системных блоков компьютеров проводятся на рабочем месте. Изъятие системных блоков компьютеров для проведения ремонтов и ТО в лабораторных условиях организаций, заключивших договоры или контракты на обслуживание вычислительной техники и не имеющих лицензии по технической защите конфиденциальной информации, запрещается.

2.9. Доставка оборудования в ремонт и обратно на рабочее место осуществляется обслуживающей организацией или работниками ФКУ УСЗ.

2.10. Ремонт оборудования, на которое не истек гарантийный срок, производится с учетом условий гарантийного соглашения.

2.11. Плановое ТО организационной и копировальной техники (принтеры, копировальное оборудование, сканеры, факсы и т.д.) осуществляется 4 раза в год в каждом квартале. Норма времени на проведение планового ТО одной единицы организационной и копировальной техники составляет 2 часа.

2.12. Плановое ТО вычислительной техники производится 4 раза в год в каждом квартале. Норма времени на проведение планового ТО одной единицы вычислительной техники составляет 4 часа.

3. Специалистам обслуживающих организаций запрещается

3.1. Несанкционированное копирование, какой-либо информации, находящейся на компьютере (носителе информации), при проведении ремонта, профилактики, ТО компьютера учреждения.

3.2. Осуществлять какие-либо действия (операции), не требующиеся для осуществления ремонта, профилактики или ТО.

3.3. Изменять перечень прикладного и системного программного обеспечения.

3.4. Вносить какие-либо изменения в установленное программное обеспечение (кроме восстановительных работ).

3.5. Вносить изменения в пароли, учетные записи, системные настройки и т.п., что может привести к неправильной работе компьютера.

3.6. Выносить за пределы помещения обслуживаемой организации носители информации любого типа и в любом состоянии, принадлежащие обслуживаемой организации.

4. Состав работ по видам ТО персональных компьютеров

4.1. Входной контроль

- Внешний осмотр;
- Проверка соответствия конфигурации оборудования заявленной в документах (спецификация к договору, акты передачи);
- Проверка работоспособности устройств средствами операционной системы;
- Настройка операционной системы и программного обеспечения;

– Установка оборудования.

4.2. Плановое ТО

- Внешний осмотр;
- Очистка от пыли внутренних объемов системного блока (при отсутствии пломбы на гарантийное обслуживание);
- Техническая профилактика, смазка и чистка движущихся элементов персональных компьютеров;
- Очистка от пыли видеомониторов, регулировка и настройка;
- Проведение дефрагментации накопителей на жестких магнитных дисках;
- Проверка работоспособности устройств средствами операционной системы, при необходимости – соответствующие восстановления и настройка;
- Проверка состояния файловой системы с помощью утилит Windows;
- Полное тестирование всех устройств персонального компьютера;
- Полная проверка дисковой памяти на наличие вирусов;
- Проверка работоспособности программ (операционная система Windows, MS Office, архиваторы, антивирусные программы, драйверы периферийных устройств и др.), при необходимости – соответствующие восстановления и настройка;
- Контроль кабельных соединений.

4.3. Внеплановое ТО

- Проведение диагностики и локализация неисправностей;
- Выполнение необходимых действий перечисленных в п. 4.2 для устранения неисправности.

5. Состав работ по видам ТО принтеров

5.1. Входной контроль

- Внешний осмотр;
- Проверка соответствия конфигурации оборудования заявленной в документах (спецификация к договору, акты передачи);
- Установка оборудования;
- Проверка работоспособности устройств средствами операционной системы (печать пробной страницы).

5.2. Плановое ТО

- Внешний осмотр;
- Печать пробной страницы;
- Проверка работоспособности драйверов принтера при необходимости – соответствующие восстановления и настройка;
- Чистка, смазка, настройка (при необходимости);
- Замена картриджа (при необходимости);
- Замена изношенных или вышедших из строя деталей;
- Внешний осмотр и контроль кабельных соединений.

5.3. Внеплановое ТО

- Проведение диагностики и локализация неисправностей;

- Выполнение необходимых действий, перечисленных в п. 5.2 для устранения неисправности;
- Печать пробной страницы.

6. Состав работ по видам ТО сканеров

6.1. Входной контроль

- Внешний осмотр;
- Проверка соответствия конфигурации оборудования заявленной в документах (спецификация к договору, акты передачи);
- Установка оборудования;
- Сканирование пробной страницы.

6.2. Плановое ТО

- Сканирование пробной страницы;
- Проверка работоспособности драйверов сканера при необходимости – соответствующие восстановления и настройка;
- Чистка, настройка (при необходимости);
- Внешний осмотр и контроль кабельных соединений (сканирование пробной страницы).

6.3. Внеплановое ТО

- Проведение диагностики и локализация неисправностей;
- Выполнение необходимых действий, перечисленных в п. 6.2 для устранения неисправности;
- Сканирование пробной страницы.

7. Состав работ по видам ТО копировальной техники

7.1. Входной контроль

- Внешний осмотр;
- Проверка соответствия конфигурации оборудования заявленной в документах (спецификация к договору, акты передачи);
- Установка оборудования;
- Копирование пробной страницы.

7.2. Плановое ТО

- Копирование пробной страницы;
- Чистка, смазка, настройка (при необходимости);
- Замена картриджа и или других элементов переноса изображения (при необходимости);
- Замена изношенных или вышедших из строя деталей;
- Внешний осмотр и контроль кабельных соединений (копирование пробной страницы).

7.3. Внеплановое ТО

- Проведение диагностики и локализация неисправностей;
- Выполнение необходимых действий, перечисленных в п. 7.2 для устранения неисправности;

- Копирование пробной страницы.

8. Состав работ по видам технического обслуживания источников бесперебойного питания (далее – ИБП)

8.1. Входной контроль

- Внешний осмотр;
- Проверка соответствия конфигурации оборудования заявленной в документах (спецификация к договору, акты передачи);
- Установка оборудования.

8.2. Внеплановое техническое обслуживание

- Диагностика ИБП встроенными средствами (при их наличии);
- Проверка работоспособности ИБП под нагрузкой;
- Замена вышедших из строя аккумуляторов на аналогичные.

Все выше перечисленные действия выполняются как в комплексе, так и по отдельности по мере необходимости.

После проведения ТО, лица ответственные за вычислительную, оргтехнику и работник обслуживающей организации, выполнивший обслуживание, делают соответствующие записи в паспорте технического средства (Приложения №№ 1-4 к Регламенту) и акте выполненных работ.

Приложение № 1
к Регламенту

Паспорт технического средства (для вычислительной техники)

Наименование _____

Закреплен за

Кабинет _____ Ф.И.О. _____

Структурное подразделение _____

Серийный № _____ инв.№ _____

Жесткий диск _____ Гб, ОЗУ _____ Гб

Процессор тип _____ рабочая частота _____ кол-во (CPU) _____

CD-ROM тип _____ название _____

Иные устройства

Монитор Название _____ диагональ _____ тип _____

Серийный № _____ инв.№ _____

Установленное программное обеспечение

№	Наименование программного обеспечения	Дата установки или изменения

Плановое обслуживание технического средства

№	Дата	Наименование работ	Ф.И.О. обслуживающего лица	Подпись обслуживающего лица	Ф.И.О. ответственного лица	Подпись ответственного лица

Внеплановое обслуживание технического средства

№	Дата	Наименование работ	Ф.И.О. обслуживающего лица	Подпись обслуживающего лица	Ф.И.О. ответственного лица	Подпись ответственного лица

Акт изъятия технического средства

для проведения ремонта или технического обслуживания в лабораторных условиях

Наименование оборудования _____

Инвентарный/серийный номера _____ / _____

Описание оборудования _____

_____Описание неисправности и причины возникновения _____

Ответственное лицо, за которым закреплена техника

Ф.И.О., Подпись / _____ / _____ дата _____

Лицо, совершившее процедуру изъятия техники

Ф.И.О., Подпись / _____ / _____ дата _____

Акт возврата технического средства, изъятого
для проведения ремонта или технического обслуживания в лабораторных
условиях

Наименование оборудования _____

Инвентарный/серийный номера

_____ / _____

Описание оборудования _____

Описание неисправности и причины возникновения _____

Произведенные работы _____

Ответственное лицо, за которым закреплена техника

Ф.И.О., Подпись / _____ / _____ дата _____

Лицо, совершившее процедуру изъятия техники

Ф.И.О., Подпись / _____ / _____ дата _____

Паспорт технического средства (для оргтехники)

Наименование _____

Закреплен за

Кабинет _____ Ф.И.О. _____

Структурное подразделение _____

Серийный № _____ инв.№ _____

Описание

Плановое обслуживание технического средства

№	Дата	Наименование работ	Ф.И.О. обслуживающе го лица	Подпис ь обслуж ивающе го лица	Ф.И.О. ответствен ного лица	Подпись ответствен ного лица

Внеплановое обслуживание технического средства

№	Дата	Наименование работ	Ф.И.О. обслуживающе	Подпис ь	Ф.И.О. ответствен	Подпись ответствен

			го лица	обслуж ивающе го лица	ного лица	ного лица

**Правила
осуществления внутреннего контроля соответствия обработки персональных
данных требованиям к защите персональных данных
в Федеральном агентстве железнодорожного транспорта**

1. Настоящие правила определяют основания и порядок проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным действующим законодательством (далее – внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных).

2. Внутренний контроль соответствия обработки персональных данных требованиям защиты персональных данных в Федеральном агентстве железнодорожного транспорта (Росжелдор) осуществляется в форме проверок условий обработки персональных данных.

3. Проверки осуществляются администратором информационной безопасности Росжелдора, которой назначается приказом руководителя Росжелдора.

4. В проведении проверки в Росжелдоре не может участвовать должностное лицо, прямо или косвенно заинтересованное в ее результатах.

5. Основанием для проведения внеплановой проверки является информация о нарушениях требований по обработке персональных данных, поступившая в Росжелдор от правоохранительных органов, иных государственных органов, органов местного самоуправления и их должностных лиц, граждан Российской Федерации, иностранных граждан и лиц без гражданства.

6. Проведение проверки организуется лицом, ответственным за защиту персональных данных, в течение трех рабочих дней с момента поступления в Росжелдор соответствующей информации.

7. При проведении проверок должны быть полностью, объективно и всесторонне установлены:

- порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

- порядок и условия применения средств защиты информации;

- эффективность принимаемых мер по обеспечению безопасности персональных данных;

- состояние учета машинных носителей персональных данных;

- соблюдение правил доступа к персональным данным;

- наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;

- мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- осуществление мероприятий по обеспечению целостности персональных данных.

8. Администратор информационной безопасности имеет право:

- получать от проверяемого структурного подразделения Росжелдора необходимые для осуществления проверки документы, дополнительную письменную и устную информацию о соблюдении законодательства о персональных данных;

- принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

- вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

- вносить предложения о привлечении к ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

9. Срок проведения проверки не должен превышать 20 календарных дней со дня начала проверки.

Срок проверки может быть продлен лицом, принявшим решение о ее проведении, на основании обращения администратора информационной безопасности, но не более чем на 10 дней.

10. По результатам проведения проверки оформляется справка с изложением результатов проверки, выводами, предложениями и мерами, необходимыми для устранения выявленных нарушений. Справка подписывается администратором информационной безопасности и направляется руководителю Росжелдора.

**Перечень разрешенного к использованию программного обеспечения
в государственных информационных системах
Федерального агентства железнодорожного транспорта**

1. Общие положения

1.1. Настоящий документ устанавливает перечень разрешенного к установке программного обеспечения (далее – ПО) в центральном аппарате Федерального агентства железнодорожного транспорта (Росжелдор), необходимого и достаточного для осуществления государственными гражданскими служащими Росжелдора своих должностных обязанностей, а также обеспечения определенных классов защищенности государственных информационных систем и уровней защищенности персональных данных, обрабатываемых в государственных информационных системах Росжелдора.

1.2. Требования, установленные настоящим документом, обязательны для выполнения всеми работниками Росжелдора.

1.3. Установка программ отсутствующих в разделе 2 настоящего документа запрещена.

1.4. Установка подлежит только необходимому для работы ПО, установка всего перечня не обязательна.

2. Перечень разрешенного к использованию ПО

2.1. Перечень разрешенного к использованию ПО на серверном оборудовании:

2.1.1. В государственной информационной системе «Информационная система обеспечения финансово-экономической деятельности Федерального агентства железнодорожного транспорта»:

- Microsoft Windows Server;
- Internet Explorer;
- 7-Zip;
- Kontur.Diag;
- Microsoft Office;
- Microsoft SQL Server;
- Mozilla Firefox;
- PL/SQL Developer;
- Агент администрирования Kaspersky Security Center;
- КриптоПро CSP;
- ПАРУС-Бюджет 8;
- ПАРУС-Сведение отчетности Онлайн;
- Формирование и исполнение ФБ ГРБС;

- FusionInventory Agent;
- Kaspersky Endpoint Security;
- Zabbix Agent;
- .NET Framework;
- 1С:Предприятие. Бухгалтерский учет 7 (сетевая версия)
- 1С:Предприятие. Оперативный учет 7 (сетевая версия)
- 1С:Предприятие. Расчет 7 (сетевая версия)
- 1С:Предприятие 8
- HASP Device Drivers;
- HASP License Manager;
- SecretNet 7.

2.1.2. В государственной информационной системе «Система электронного документооборота Федерального агентства железнодорожного транспорта»:

- CentOS;
- Nginx;
- Microsoft Windows;
- .NET Framework;
- CodeGear InterBase 2009;
- KDS Tools 2009;
- Adobe Reader;
- КриптоПро JCP;
- Java;
- Borland Delphi 6;
- Postgre SQL;
- JBoss-portal;
- Логика СЭД;
- FusionInventory Agent;
- Kaspersky Endpoint Security;
- Zabbix Agent;
- SecretNet 7;
- PostgreSQL.

2.1.3. В государственной информационной системе «Официальный сайт Федерального агентства железнодорожного транспорта (www.roszeldor.ru)»:

- CentOS;
- MySQL;
- Nginx;
- PHP;
- FusionInventory Agent;
- Kaspersky Endpoint Security;
- Zabbix Agent;
- SecretNet 7.

2.1.4. В государственной информационной системе «Электронная почтовая система Федерального агентства железнодорожного транспорта»:

- CentOS;

- Zimbra Collaboration Open Source.

2.2. Перечень разрешенного к использованию ПО на рабочих станциях пользователей:

2.2.1. В государственной информационной системе «Информационная система обеспечения финансово-экономической деятельности Федерального агентства железнодорожного транспорта»:

- Microsoft Windows;
- Microsoft Office;
- .NET Framework;
- 7-Zip;
- Internet Explorer;
- Формирование и исполнение ФБ ГРБС;
- 1С:Предприятие. Бухгалтерский учет 7 (сетевая версия);
- 1С: Предприятие: Расчет 7 (сетевая версия);
- 1С Предприятие 7;
- 1С: Предприятие 8;
- 1С:Базы данных;
- ПАРУС Бюджет;
- ПАРУС-Бюджет 8;
- Печать НДС с PDF417.

2.2.2. В государственной информационной системе «Система электронного документооборота Федерального агентства железнодорожного транспорта»:

- Microsoft Windows;
- Microsoft Office;
- Adobe Acrobat Reader;
- Microsoft Firefox;
- Java;
- KDS Tools 2009;
- КриптоПро CSP.

2.2.3. В государственной информационной системе «Официальный сайт Федерального агентства железнодорожного транспорта (www.roszeldor.ru)»:

- Internet Explorer 9 и выше;
- Google Chrome 40 и выше;
- Mozilla Firefox 35 и выше;
- Яндекс.Браузер 14 и выше;
- Opera 10.1 и выше;
- Safari 3.2 и выше.

2.2.4. В государственной информационной системе «Электронная почтовая система Федерального агентства железнодорожного транспорта»:

- Mozilla Firefox;
- Zimbra Desktop.

2.2.5. Прочее:

- Агент администрирования Kaspersky Security Center;
- FusionInventory Agent;

- Kaspersky Endpoint Security;
- Zabbix Agent;
- SecretNet 7;
- CDBurnerXP;
- MPC-NC;
- КриптоАРМ;
- ABBY FineReader;
- Партионная почта;
- Microsoft Office Visio Viewer;
- Драйвера и утилиты, необходимые для работы оборудования;
- doPDF.

2.2.5.1. В связи с необходимостью использования информационных систем Росжелдора:

2.2.5.1.1. Автоматизированная система управления объектами федерального имущества, закрепленного за подведомственными Росжелдору организациями (АСУ Имущество):

- VMware Horizon Client.

2.2.5.1.2. Информационная системы ведения перечней железнодорожных станций:

- Microsoft Windows;
- ASP.NET;
- Internet Explorer;
- Microsoft Silverlight;
- Adobe Acrobat Reader;
- Microsoft Office;
- LibreOffice.

2.2.5.1.3. Информационная система обеспечения предоставления государственных услуг Федерального агентства железнодорожного транспорта:

- Adobe Acrobat Reader;
- Microsoft Office;
- Mozilla Firefox;
- КриптоПро CSP 3.6 или выше;
- КриптоПро Browser Plugin;
- Re:Doc;
- VipNet Client.

2.2.5.1.4. Информационная система пономерного учета грузовых вагонов:

- Microsoft Windows;
- ASP.NET;
- Internet Explorer;
- Microsoft Silverlight;
- Adobe Acrobat Reader;
- Microsoft Office;
- LibreOffice.

2.2.5.1.5. Справочная правовая система Федерального агентства железнодорожного транспорта:

- Microsoft Windows;
- ГАРАНТ аэро (Клиент);
- ИС «Кодекс: 6 поколение» Интранет;
- Консультант Плюс.

2.2.5.1.6. Информационная система пономерного учета пассажирских вагонов локомотивной тяги:

- Microsoft Windows;
- ASP.NET;
- Internet Explorer;
- Microsoft Silverlight;
- Adobe Acrobat Reader;
- Microsoft Office;
- LibreOffice.

2.2.5.1.7. Система видеоконференцсвязи центрального аппарата Федерального агентства железнодорожного транспорта:

- Mozilla Firefox.

2.2.5.1.8. Информационная система пономерного учета локомотивов:

- Microsoft Windows;
- ASP.NET;
- Internet Explorer;
- Microsoft Silverlight;
- Adobe Acrobat Reader;
- Microsoft Office;
- LibreOffice.

2.2.5.1.9. Автоматизированная система управления образовательными организациями Федерального агентства железнодорожного транспорта (АСУ ВУЗ Росжелдора):

- VMware Horizon Client.

2.2.5.2. В связи с необходимостью использования сторонних информационных систем:

2.2.5.2.1. Информационно-аналитическая система регулирования на транспорте (АСУ ТК):

- Microsoft Windows XP/Vista/7 и выше;
- Google Chrome 44 и выше;
- Internet Explorer 11 и выше;
- Mozilla Firefox 40 и выше;
- Microsoft Office.

2.2.5.2.2. Государственная автоматизированная информационная система «Управление» (ГАС «Управление»):

- Microsoft Windows 2000 Professional (SP4);
- Microsoft Windows XP Professional (SP2);
- Microsoft Windows Vista;

- Microsoft Windows 7;
- Microsoft Windows 8;
- Internet Explorer версии 9.0 или выше;
- Crypto Pro Fox версии 24 или выше;
- Microsoft Office версии 2000 или выше;
- Adobe Acrobat Reader версии 9 или выше;
- Adobe Flash Player версии 19 или выше;
- Rostelecom Плагин пользователя систем электронного правительства;
- КриптоПро CSP версии 3.6.1 или выше;
- КриптоПро ЭЦП Browser Plug-in версии 1.5.

2.2.5.2.3. Облачная система электронного документооборота Министерства транспорта Российской Федерации (ОСЭД Минтранса):

- Mozilla Firefox.

2.2.5.2.4. Портал государственных программ Российской Федерации:

- Mozilla Firefox.

2.2.5.2.5. Федеральная государственная информационная система «Федеральный портал государственной службы и управленческих кадров» (Портал госслужбы):

- Специальное программное обеспечение «Справки БК»;
- Microsoft Windows XP Professional Russian SP 3 или Windows 7;
- NET Framework 3.5 или 4.5;
- Microsoft Internet Explorer 8.0 и выше;
- Mozilla Firefox 2.0 и выше;
- VipNet Client;

2.2.5.2.6. Портал ССТУ.рф:

– Специальное программное обеспечение универсальное автоматизированное рабочее место для проведения общероссийского дня приема граждан;

- VipNet Client
- Microsoft Windows XP SP3 (32-разрядная)/Vista SP2 (32/64-разрядная)/Windows 7 (32/64-разрядная).

2.2.5.2.7. Система управления финансового документооборота (СУФД):

- КриптоПро 3.0 и выше;
- Континент АП 3.4 и выше;
- Java 6 update 14;
- Internet Explorer 7 и выше;
- Mozilla Firefox 3.6 и выше.

2.2.5.2.8. Федеральная государственная информационная система досудебного (внесудебного) обжалования (ФГИС ДО):

- Internet Explorer;
- КриптоПро CSP;
- КриптоПро ЭЦП Browser Plug-in.

2.2.5.2.9. Федеральная государственная информационная система территориального планирования (ФГИС ТП):

- Opera;
- Google Chrome;
- Mozilla Firefox;
- Apple Safari;
- Яндекс.Браузер;
- Internet Explorer;
- Microsoft Silverlight;

2.2.5.2.10. Федеральная государственная информационная система «Федеральный реестр государственных и муниципальных услуг (функций)» (ФРГУ):

- Microsoft Windows XP;
- Windows Vista;
- Windows 7;
- Ubuntu Linux 11.04 Gnome и выше (GTK 2.2.1, ATK 1.2.0, glib 2.2.1, Pango 1.2.1, Freetype 2.1.3);
- Mozilla Firefox 11 и выше.

2.2.5.2.11. Государственная интегрированная информационная система управления общественными финансами «Электронный бюджет» (ГИИС «Электронный бюджет»):

- Internet Explorer 10.0 и выше;
- Microsoft Windows Vista/7/8/8.1;
- КриптоПро CSP;
- Континент TLS Клиент;
- Jinn-Client;
- КУБ: Модуль для работы с электронной подписью;
- VipNet Client.

УТВЕРЖДЕНО
приказом Росжелдора
от 31.10.2017 № 423

**План мероприятий по обеспечению контроля защиты государственных информационных систем и персональных данных в центральном аппарате
Федерального агентства железнодорожного транспорта**

Название контрольного мероприятия	Периодичность проведения	Исполнитель
Контроль над соблюдением режима обработки персональных данных	Ежемесячно	Администратор информационной безопасности
Контроль над соблюдением режима защиты государственных информационных систем и персональных данных	Ежедневно	Администратор информационной безопасности
Контроль над выполнением антивирусной защиты	Еженедельно	Администратор информационной безопасности
Контроль над соблюдением режима защиты при подключении к сетям общего пользования и (или) международного обмена	Еженедельно	Администратор информационной безопасности
Проведение контрольных проверок на предмет выявления изменений в режиме обработки персональных данных	Ежегодно	Администратор информационной безопасности
Контроль обновления программного обеспечения	Еженедельно	Администратор информационной безопасности
Организация анализа и пересмотра имеющихся угроз безопасности информации, обрабатываемой в государственных информационных системах, а также предсказание появления новых, еще неизвестных угроз	Ежегодно	Администратор информационной безопасности
Поддержание в актуальном состоянии нормативно-организационных документов	Ежеквартально	Администратор информационной безопасности
Контроль выполнения работниками центрального аппарата Федерального	Еженедельно	Руководитель подразделения

агентства железнодорожного транспорта инструкций по защите персональных данных		
Контроль знания и выполнения работниками требований локальных нормативных актов центрального аппарата Федерального агентства железнодорожного транспорта по защите персональных данных на автоматизированных рабочих местах и локально-вычислительных сетях путем выборочного опроса работников	Ежеквартально	Администратор информационной безопасности

УТВЕРЖДЕНО
приказом Росжелдора
от 31.10.2017 № 423

Журнал

учета мероприятий по контролю обеспечения защиты государственных информационных систем и персональных данных в центральном аппарате Федерального агентства железнодорожного транспорта

Ответственный за обеспечение безопасности информации _____

Начат: «__» _____ 20__ г.
Окончен: «__» _____ 20__ г.

На ___ листах

УТВЕРЖДЕНО
приказом Росжелдора
от 31.10.2017 № 423

Журнал

выдачи съемных носителей информации для работы в государственных информационных системах и обработки персональных данных в центральном аппарате Федерального агентства железнодорожного транспорта

Ответственный _____
(Должность) (Подпись) (ФИО)

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

На _____ листах

УТВЕРЖДЕНО
приказом Росжелдора
от 31.10.2017 № 423

Журнал

поэкземплярного учета средств защиты информации в центральном аппарате
Федерального агентства железнодорожного транспорта

Ответственный за обеспечение безопасности информации _____

Начат: «___» _____ 20__ г.
Окончен: «___» _____ 20__ г.

На ___ листах

