ОТКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО
«РОССИЙСКИЕ ЖЕЛЕЗНЫЕ ДОРОГИ»
(ОАО «РЖД»)

РАСПОРЯЖЕНИЕ

26 января 2023 г. Москва №152/р

Об утверждении Порядка предоставления доступа к информационным системам ОАО «РЖД»

1. Утвердить прилагаемый Порядок предоставления доступа к информационным системам ОАО «РЖД» (далее – Порядок).

2. Руководителям подразделений аппарата управления, филиалов и структурных подразделений ОАО «РЖД»:

обеспечить выполнение Порядка;

организовать ознакомление работников с Порядком под роспись, а также изучение ими Порядка.

3. Признать утратившим силу распоряжение ОАО «РЖД» от 28 ноября 2011 г. № 2546р «О порядке предоставления доступа к информационным системам ОАО «РЖД».

Генеральный директор –
председатель правления ОАО «РЖД» О.В.Белозёров

Исп. Кайсаров А.Р., ЦИБ
(499) 262-31-96

УТВЕРЖДЕН
распоряжением ОАО «РЖД»
от «26» 01 2023 г. № 152 /р

ПОРЯДОК
предоставления доступа к информационным системам ОАО «РЖД»

I. Общие положения

1. Настоящий Порядок устанавливает единую процедуру предоставления доступа к информационным системам ОАО «РЖД» (далее – доступ к ИС) работникам подразделений аппарата управления, филиалов и структурных подразделений ОАО «РЖД» (далее – подразделения ОАО «РЖД») и сторонних организаций, а также индивидуальным предпринимателям и их работникам.

2. Уполномоченные работники подразделений ОАО «РЖД», участвующие в согласовании/утверждении заявок на предоставление доступа к ИС, обязательно используют при предоставлении доступа к ИС электронную подпись.

3. Подключение к информационным системам ОАО «РЖД» в режиме «информационная система ОАО «РЖД» – автоматизированная система внешней организации», а также подключение технологического оборудования (стоек, терминалов, банкоматов и т.п.) осуществляется на основании проекта технических решений подключения, утвержденного в соответствии с требованиями Стандарта ОАО «РЖД» «Автоматизированные системы и программные средства ОАО «РЖД». Порядок согласования и утверждения документов, разрабатываемых при создании и модификации автоматизированных систем и программных средств» СТО РЖД 04.001.4-2021, утвержденного распоряжением ОАО «РЖД» от 29 апреля 2021 г. № 951/р.

4. В настоящем Порядке используются следующие основные термины и понятия:

1) АС ОЗ – система, предназначенная для автоматизации процесса создания, согласования и утверждения заявок на подключение пользователей к информационным системам ОАО «РЖД», а также для хранения заявок и прилагаемых к ним материалов в течение установленного времени;

2) АСУ ЕСПП – система, предназначенная для управления инцидентами и работами по их устранению, включая регистрацию инцидентов и нарядов на соответствующие работы, а также для контроля выполнения этих работ;

3) бизнес-роль – совокупность прав доступа к ИС, обеспечивающих выполнение работниками подразделений ОАО «РЖД» своих должностных обязанностей;

4) внешний пользователь – работник сторонней организации (в том числе хозяйственного общества с прямым или косвенным участием ОАО «РЖД») или индивидуальный предприниматель и его работник, которому предоставляется доступ к ИС;

5) внутренний пользователь – работник подразделения ОАО «РЖД», которому предоставляется доступ к ИС;

6) ВП АС ОЗ – обособленный раздел АС ОЗ, предназначенный для подготовки и оформления заявок внешних пользователей в целях их рассмотрения и согласования вместе с прилагаемыми к ним материалами;

7) доступ к информационной системе – возможность ознакомления со сведениями, находящимися в информационной системе, и/или использования обеспечивающих их обработку информационных технологий и технических средств, в том числе в рамках единого технологического процесса на всем жизненном цикле информационной системы (разработка, внедрение, сопровождение, модификация и вывод из эксплуатации);

8) заявка – сформированный в АС ОЗ запрос на предоставление доступа к ИС;

9) зона ответственности подразделения ОАО «РЖД», осуществляющего эксплуатацию информационной системы, – область функционирования информационной системы, где данное подразделение несет ответственность за ее работоспособность;

10) информация ограниченного доступа – информация, доступ к которой ограничен федеральными законами;

11) обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации;

12) организация внешнего пользователя – сторонняя организация или индивидуальный предприниматель и его работник, которой (-ому) предоставляется доступ к ИС;

13) ответственный за оформление заявок – работник подразделения ОАО «РЖД», оформляющий доступ к ИС пользователей данного подразделения;

14) права доступа – совокупность правил, определяющих условия и регламент доступа к ИС;

15) АС ОЗ БР – раздел АС ОЗ, предназначенный для автоматизации процесса подключения внутренних пользователей к информационным системам ОАО «РЖД»;

16) распорядитель информационной системы – подразделение ОАО «РЖД» или внешняя организация, реализующие полномочия обладателя информации по предоставлению доступа к ИС в соответствии с требованиями настоящего Порядка, а также других организационно-правовых или распорядительных документов ОАО «РЖД»;

17) руководитель подразделения ОАО «РЖД» – начальник (заместитель начальника) подразделения ОАО «РЖД», имеющий право подписи исходящих документов;

18) СПД – корпоративная транспортная инфраструктура передачи данных, предназначенная для обмена информацией между подключенными к ней пользователями, а также для обеспечения доступа к ИС пользователей;

19) ЦУДИС – сетевой узел, предназначенный для обеспечения информационной безопасности информационных систем ОАО «РЖД» при централизованном сетевом взаимодействии и информационном обмене с внешними организациями по выделенным каналам связи и/или по информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»).

5. Подключения пользователей к информационным системам ОАО «РЖД» подразделяются на следующие типы:

1) информационный – для получения справочных сведений из информационной системы;

2) технологический – для обмена данными с информационной системой в процессе производственной деятельности;

3) обеспечивающий – для сопровождения и обеспечения эффективного функционирования информационной системы.

6. В случае отсутствия возможности использования внутренними пользователями АС ОЗ заявка на предоставление доступа к ИС, составленная по форме согласно приложениям № 1 и 2, вместе с сопроводительным письмом, в котором указываются цель подключения и основание для предоставления доступа к ИС, направляется в адреса Главного вычислительного центра (информационно-вычислительного центра), распорядителя информационной системы и Департамента информатизации (службы корпоративной информатизации железной дороги).

В случае отсутствия возможности использования внешними пользователями ВП АС ОЗ заявка на предоставление доступа к ИС, составленная по форме согласно приложениям № 1 и 2, схема подключения, составляется по форме согласно приложению № 2, вместе с сопроводительным

письмом, в котором указывается цель подключения и основание для предоставления доступа к ИС, направляются в ОАО «РЖД».

7. Ответственными за предоставление доступа к ИС являются:

1) руководитель подразделения ОАО «РЖД», инициирующего подключение внутреннего пользователя к информационной системе – за достоверность внесенных в заявку сведений и соответствие данных о подключаемом внутреннем пользователе сведениям, содержащимся в Единой корпоративной автоматизированной системе управления трудовыми ресурсами (ЕК АСУТР);

2) руководитель подразделения ОАО «РЖД», являющегося распорядителем информационной системы – за согласование заявки на предоставление доступа к ИС, а также за принятие решения о целесообразности и возможности предоставление доступа к ИС и к информации в информационной системе;

3) администратор информационной системы – за своевременность подключения к информационной системе (отключения от информационной системы) и соответствие прав доступа, предоставляемых внутреннему и внешнему пользователям, правам, указанным в заявке;

4) начальник службы корпоративной информатизации железной дороги – за утверждение заявки на предоставление доступа к ИС в зоне ответственности информационно-вычислительного центра;

5) работник Департамента информатизации, назначаемый приказом по данному подразделению ОАО «РЖД», – за утверждение заявки на предоставление доступа к ИС в зоне ответственности Главного вычислительного центра.

II. Организация доступа к ИС внутренних пользователей

8. Основанием для предоставления доступа к ИС внутреннему пользователю являются должностные обязанности (трудовые функции), установленные распорядительными и организационно-правовыми документами ОАО «РЖД» (должностные инструкции, приказ о распределении обязанностей, положение о подразделении и пр.).

9. Для предоставления внутреннему пользователю доступа к ИС, в которой обрабатываются персональные данные, необходимо одновременное наличие:

1) приказа о назначении внутреннего пользователя на должность;

2) документа, в котором закреплены трудовые обязанности, в том числе функции по обработке персональных данных;

3) подписанного внутренним пользователем обязательства о неразглашении персональных данных.

10. Доступ к ИС обеспечивается путем подключения персональных электронно-вычислительных машин (далее – ПЭВМ) внутренних пользователей к СПД.

11. Предоставление внутреннему пользователю доступа к ИС осуществляется на основании заявок, оформляемых в АС ОЗ.

Заявка на предоставление доступа к ИС заполняется в АС ОЗ ответственным за оформление заявок в подразделении ОАО «РЖД» или самим внутренним пользователем. При оформлении заявки указывается цель и тип подключения, при этом тип подключения выбирается исходя из цели подключения.

В зависимости от обрабатываемой в информационной системе информации к заявке прикрепляются соответствующие основания для предоставления доступа к ИС, предусмотренные пунктами 8 и 9 настоящего Порядка.

В случае необходимости в поле комментария к заявке могут указываться дополнительные сведения, требуемые для корректной работы и/или настройки программного обеспечения.

12. Руководитель подразделения внутреннего пользователя подтверждает необходимость подключения, согласовывая заявку в АС ОЗ с применением электронной подписи. Делегирование полномочий руководителя подразделения ОАО «РЖД» в части согласования заявок в АС ОЗ внутренних пользователей данного подразделения допускается только работнику этого подразделения на основании приказа по данному подразделению. Применение электронной подписи указанным работником в этом случае является обязательным.

13. Распорядитель информационной системы в порядке согласования заявки в АС ОЗ с учетом представленных оснований принимает решение о целесообразности и возможности предоставления доступа к ИС внутреннему пользователю.

Распорядитель информационной системы по согласованию с Департаментом управления информационной безопасностью и Департаментом информатизации при необходимости может делегировать право согласования в АС ОЗ заявок внутренних пользователей структурным подразделениям дорожного уровня в зоне ответственности соответствующих информационно-вычислительных центров.

14. В Главном вычислительном центре (информационно-вычислительном центре) заявки на предоставление доступа к ИС рассматриваются соответствующими подразделениями (уполномоченными работниками), которые обеспечивают:

1) физическое подключение ПЭВМ внутреннего пользователя к СПД, если ранее ПЭВМ не была подключена, или подтверждение факта ее физического подключения;

2) организацию (при необходимости) работы по установке автоматизированного рабочего места информационной системы на ПЭВМ внутреннего пользователя;

3) предоставление и обеспечение безопасности доступа к ИС.

15. Департамент информатизации (службой корпоративной информатизации железной дороги) утверждает заявки на предоставление доступа к ИС внутренним пользователям.

16. Срок рассмотрения соответствующими подразделениями ОАО «РЖД» заявок на доступ к ИС внутренних пользователей не должен превышать 3 рабочих дней.

17. В случае наличия ошибок (неточностей) или отсутствия оснований для предоставления доступа к ИС внутреннему пользователю к информационным системам при оформлении в АС ОЗ заявки, а также при нарушении порядка ее согласования доступ к ИС не предоставляется, о чем работник, принявший решение об отказе в предоставлении доступа к ИС, уведомляет инициатора заявки путем оформления замечания в АС ОЗ.

18. Срок действия заявки на предоставление внутреннему пользователю доступа к ИС – 2 года с даты ее утверждения.

19. Внутренние пользователи при работе в информационных системах ОАО «РЖД» обязаны соблюдать требования, изложенные в приложении № 4.

III. Порядок предоставления доступа к ИС внутренним пользователям в зоне ответственности Главного вычислительного центра

20. Предоставление доступа к ИС внутренним пользователям в зоне ответственности Главного вычислительного центра осуществляется в следующем порядке:

1) оформленные в АС ОЗ заявки направляются в Главный вычислительный центр;

2) в Главном вычислительном центре заявки согласовываются администратором информационной системы, администратором безопасности и начальником отдела безопасности информационных ресурсов и направляются на рассмотрение распорядителю информационной системы;

3) согласованные распорядителем информационной системы заявки направляются на утверждение в Департамент информатизации;

4) утвержденные в Департаменте информатизации заявки направляются в Главный вычислительный центр для исполнения.

21. Предоставление внутренним пользователям доступа к ИС, подключаемым через информационно-вычислительный центр, осуществляется в следующем порядке:

1) оформленные в АС ОЗ заявки направляются в информационно-вычислительный центр;

2) в информационно-вычислительном центре заявки согласовываются администратором информационной системы, администратором безопасности и начальником подразделения информационной безопасности и направляются для согласования в соответствующий региональный центр безопасности – структурное подразделение ОАО «РЖД»;

3) согласованные в региональном центре безопасности заявки направляются на согласование в Главный вычислительный центр;

4) согласованные в Главном вычислительном центре заявки направляются распорядителю информационной системы;

5) согласованные распорядителем информационной системы заявки направляются на утверждение в Департамент информатизации;

6) утвержденные в Департаменте информатизации заявки направляются в Главный вычислительный центр (информационно-вычислительный центр) для исполнения.

IV. Порядок предоставления доступа к ИС внутренним пользователям в зоне ответственности информационно-вычислительных центров

22. Предоставление внутренним пользователям доступа к ИС в зоне ответственности информационно-вычислительных центров осуществляется в следующем порядке:

1) оформленные в АС ОЗ заявки направляются в соответствующий информационно-вычислительный центр;

2) в информационно-вычислительном центре заявки согласовываются администратором информационной системы, администратором безопасности и начальником подразделения информационной безопасности и направляются на согласование распорядителю информационной системы;

3) согласованные распорядителем информационной системы заявки направляются на согласование в соответствующий региональный центр безопасности;

4) согласованные в региональном центре безопасности заявки направляются на утверждение в соответствующую службу корпоративной информатизации железной дороги;

5) утвержденные в службе корпоративной информатизации железной дороги заявки направляются в соответствующий информационно-вычислительный центр (Главный вычислительный центр) для исполнения.

V. Порядок предоставления доступа к ИС внутренним пользователям в зоне ответственности иных подразделений ОАО «РЖД», самостоятельно осуществляющих эксплуатацию информационных систем ОАО «РЖД»

23. Предоставление внутренним пользователям доступа к ИС в зоне ответственности подразделений ОАО «РЖД», за исключением информационных систем, находящихся в зонах ответственности Главного вычислительного центра или информационно-вычислительных центров, осуществляется в следующем порядке:

1) оформленные в АС ОЗ заявки направляются в соответствующее подразделение ОАО «РЖД», осуществляющее эксплуатацию информационной системы;

2) заявки согласовываются администратором информационной системы, ответственным за обеспечение информационной безопасности, руководителем подразделения ОАО «РЖД» как распорядителя информационной системы и направляются на утверждение в Департамент информатизации;

3) утвержденные в Департаменте информатизации заявки направляются в подразделение ОАО «РЖД», осуществляющее эксплуатацию информационной системы, для исполнения.

VI. Предоставление доступа к ИС внутренним пользователям на основании бизнес-ролей

24. Предоставление доступа к ИС внутренним пользователям на основании бизнес-ролей осуществляется с использованием АС ОЗ БР.

25. Уполномоченный руководителем подразделения ОАО «РЖД» работник заполняет размещенную в АС ОЗ БР форму бизнес-роли. Заполнению подлежат все обязательные поля формы бизнес-роли, за исключением дополнительных, заполняемых при необходимости.

Заполненная форма бизнес-роли направляется на согласование в соответствии с указанными в бизнес-роли информационными системами:

при наличии в бизнес-роли информационных систем, находящихся в зоне ответственности Главного вычислительного центра, – в Главный вычислительный центр;

при наличии в бизнес-роли информационных систем, находящихся в зоне ответственности информационно-вычислительных центров, – в соответствующий информационно-вычислительный центр.

26. В Главном вычислительном центре (информационно-вычислительном центре) согласование бизнес-роли осуществляется администраторами всех информационных систем, указанных в бизнес-роли.

После согласования всеми администраторами информационных систем Главного вычислительного центра (информационно-вычислительного центра) бизнес-роль автоматически направляется на согласование распорядителям всех информационных систем, указанных в бизнес-роли.

27. Каждый распорядитель информационной системы в процессе согласования принимает решение о целесообразности и возможности предоставления доступа к ИС.

После согласования распорядителями информационных систем бизнес-роль автоматически направляется на согласование в Департамент управления информационной безопасностью (соответствующий региональный центр безопасности).

28. Согласованная в Департаменте управления информационной безопасностью (региональном центре безопасности) бизнес-роль направляется на утверждение в Департамент информатизации (службу корпоративной информатизации железной дороги).

29. В случае отклонения бизнес-роли хотя бы одним из участников согласования в АС ОЗ БР ей присваивается статус «Отклонена» и предоставление доступа к ИС на основании данной бизнес-роли не осуществляется.

30. При назначении работника на должность, указанную в утвержденной бизнес-роли, из ЕК АСУТР в АС ОЗ БР передаются соответствующие данные и АС ОЗ БР автоматически формирует наряд в Главный вычислительный центр (информационно-вычислительный центр) на подключение ПЭВМ внутреннего пользователя ко всем информационным системам, указанным в утвержденной бизнес-роли.

Предоставление доступа к ИС на основании бизнес-роли, содержащим информацию ограниченного доступа, без получения из ЕК АСУТР подтверждения права на обработку такой информации запрещается.

31. Срок предоставления внутреннему пользователю доступа ко всем информационным системам, указанным в утвержденной бизнес-роли, – один рабочий день со дня поступления в АС ОЗ БР данных из ЕК АСУТР.

Срок действия права доступа к ИС, предоставленного внутреннему пользователю на основании бизнес-роли, – до наступления кадрового события, предусмотренного пунктом 47 настоящего Порядка.

32. В случае производственной необходимости подключения ПЭВМ внутреннего пользователя к информационным системам, не указанным в утвержденной бизнес-роли, или расширения прав ранее предоставленного

доступа к ИС предоставление соответствующего доступа к ИС осуществляется в соответствии с разделами II-V настоящего Порядка.

VII. Особенности организации и предоставления доступа к сети «Интернет» внутренним пользователям

33. Подключение внутренних пользователей к сети «Интернет» осуществляется работниками Главного вычислительного центра (информационно-вычислительного центра), которые устанавливают на ПЭВМ внутреннего пользователя средства защиты информации, а также производят их необходимую настройку в соответствии с нормативными документами ОАО «РЖД» в области информационной безопасности.

34. Предоставление внутренним пользователям доступа к сети «Интернет» в зоне ответственности Главного вычислительного центра осуществляется в следующем порядке:

1) оформленные в АС ОЗ заявки направляются в Главный вычислительный центр;

2) в Главном вычислительном центре заявки согласовываются администратором безопасности и начальником подразделения информационной безопасности;

3) согласованные в Главном вычислительном центре как распорядителе информационной системы заявки направляются на утверждение в Департамент информатизации;

4) утвержденные в Департаменте информатизации заявки направляются в Главный вычислительный центр для исполнения.

35. Предоставление внутренним пользователям доступа к сети «Интернет» в зоне ответственности информационно-вычислительного центра осуществляется в следующем порядке:

1) оформленные в АС ОЗ заявки направляются в информационно-вычислительный центр;

2) в информационно-вычислительном центре заявки согласовываются администратором безопасности и начальником отдела безопасности информационных ресурсов;

3) согласованные в информационно-вычислительном центре как распорядителе информационной системы заявки направляются на согласование в региональный центр безопасности;

4) согласованные в региональном центре безопасности заявки направляются на утверждение в службу корпоративной информатизации железной дороги;

5) утвержденные службой корпоративной информатизации железной дороги заявки направляются в информационно-вычислительный центр для исполнения.

VIII. Организация и предоставление доступа к ИС внешним пользователям

36. Основанием для предоставления доступа к ИС внешним пользователям является договор (соглашение) между организацией внешнего пользователя и ОАО «РЖД» об электронном обмене данными, в котором указываются перечень информационных систем, доступ к которым необходим внешним пользователям, состав передаваемой информации, порядок приостановления или прекращения доступа к ИС внешних пользователей, требования по обеспечению безопасности информации в соответствии с организационно-правовыми документами ОАО «РЖД» в области информационной безопасности, а также следующие обязательства организации внешнего пользователя:

1) обеспечивать конфиденциальность информации, составляющей коммерческую тайну ОАО «РЖД», не передавать полученную информацию третьим лицам без письменного согласия ОАО «РЖД»;

2) обеспечивать конфиденциальность персональных данных, обрабатываемых при исполнении договора (соглашения), а также соблюдать меры по обеспечению их безопасности при обработке, предусмотренные статьей 19 Федерального закона «О персональных данных» (в случае предоставления в рамках договора (соглашения) доступа к ИС, в которых обрабатываются персональные данные);

3) незамедлительно информировать ОАО «РЖД» о допущенном организацией внешнего пользователя либо ставшем ей известном факте разглашения или об угрозе разглашения, о незаконном получении или незаконном использовании третьими лицами информации, составляющей коммерческую тайну ОАО «РЖД»;

4) возместить убытки ОАО «РЖД» в случае разглашения организацией внешнего пользователя информации, составляющей коммерческую тайну ОАО «РЖД», а также в других случаях нарушения внешним пользователем требований информационной безопасности, в том числе безопасности персональных данных;

5) обеспечить средства электронно-вычислительной техники, подключаемые к информационным системам, антивирусной защитой и защитой от несанкционированного доступа в соответствии с организационно-правовыми документами ОАО «РЖД» в области информационной безопасности.

37. Проекты договоров (соглашений) об электронном обмене данными согласовываются с распорядителями информационных систем, Главным вычислительным центром (информационно-вычислительным центром в случае предоставления доступа к ИС в зоне его ответственности) и с Департаментом управления информационной безопасностью (региональным центром безопасности – в случае предоставления доступа к ИС в зоне ответственности информационно-вычислительного центра).

38. Предоставление внешним пользователям доступа к ИС осуществляется на основании утвержденных заявок, оформленных с использованием ВП АС ОЗ.

В случае наличия у организации внешнего пользователя доступа к АС ЭТРАН, предоставленного в соответствии с настоящим Порядком, заявка на ВП АС ОЗ может оформляться с использованием указанной информационной системы в рамках технологии взаимодействия АС ЭТРАН и ВП АС ОЗ.

39. До начала оформления заявки на предоставление доступа к ИС организация внешнего пользователя представляет в Главный вычислительный центр (информационно-вычислительный центр) электронную копию действующего заключенного договора (соглашения) об электронном обмене данными, а также копию типовой схемы предоставления доступа к ИС внешним пользователям, оформленной, согласованной и утвержденной в соответствии с приложением № 3.

40. При необходимости использования схемы предоставления доступа к ИС внешних пользователей, отличной от типовой, организация внешнего пользователя согласовывает ее с Главным вычислительным центром (информационно-вычислительным центром).

После указанного согласования схема согласовывается с Департаментом управления информационной безопасностью (региональным центром безопасности) и утверждается Департаментом информатизации.

41. Предоставление внешним пользователям доступа к ИС в зоне ответственности Главного вычислительного центра (информационно-вычислительных центров) осуществляется в следующем порядке:

1) заявки на предоставление доступа к ИС, оформленные на ВП АС ОЗ или в письменном виде согласно абзацу второму пункта 6 настоящего Порядка, направляются в Главный вычислительный центр (информационно-вычислительный центр) подразделением ОАО «РЖД», инициирующим данное подключение (заключение договора или соглашения об электронном обмене данными);

2) в Главном вычислительном центре (информационно-вычислительном центре) заявки согласовываются администратором информационной системы,

администратором безопасности и начальником отдела безопасности информационных ресурсов (начальником подразделения информационной безопасности) и направляются на рассмотрение распорядителю информационной системы;

3) согласованные распорядителем информационной системы заявки направляются:

для информационных систем в зоне ответственности информационно-вычислительных центров – на согласование в региональный центр безопасности и утверждение в службу корпоративной информатизации железной дороги;

для информационных систем в зоне ответственности Главного вычислительного центра – на утверждение в Департамент информатизации.

Утвержденные Департаментом информатизации (службой корпоративной информатизации железной дороги) заявки направляются в Главный вычислительный центр (информационно-вычислительный центр) для исполнения.

42. Предоставление внешним пользователям доступа к ИС в зоне ответственности иных подразделений ОАО «РЖД», самостоятельно осуществляющих эксплуатацию информационных систем ОАО «РЖД», осуществляется в следующем порядке:

1) заявки на предоставление доступа к ИС, оформленные на ВП АС ОЗ или в письменном виде согласно абзацу второму пункта 6 настоящего Порядка, направляются в подразделение ОАО «РЖД», осуществляющее эксплуатацию информационной системы;

2) заявки согласовываются администратором информационной системы, ответственным за обеспечение информационной безопасности, и направляются на согласование распорядителю информационной системы;

3) согласованные распорядителем информационной системы заявки направляются на утверждение в Департамент информатизации;

4) утвержденные в Департаменте информатизации заявки направляются в подразделение ОАО «РЖД», осуществляющее эксплуатацию информационной системы, для исполнения.

43. Срок действия заявки на предоставление внешнему пользователю доступа к ИС – один год с даты ее утверждения, но не более срока действия заключенного договора (соглашения) об электронном обмене данными.

44. Доступ к ИС внешних пользователей осуществляется через ЦУДИС согласно схеме предоставления доступа к ИС, утвержденной в соответствии с пунктами 39 и 40 настоящего Порядка.

45. Доступ к ИС внешних пользователей, содержащей информацию, обладателем которой ОАО «РЖД» не является, возможен только при наличии письменного согласия обладателя данной информации.

46. Предоставление внешним пользователям доступа к сети «Интернет» через СПД не допускается.

IX. Отключение пользователей и продление срока доступа к ИС

47. В случае кадрового события, связанного с увольнением работника ОАО «РЖД», переводом его в другое подразделение ОАО «РЖД», назначением на новую должность, переводом на другую работу для замещения временно отсутствующего работника, убытием в отпуск на срок более 6 месяцев, приостановкой трудового договора, ответственным за оформление заявок в подразделении ОАО «РЖД» в АС ОЗ не позднее следующего дня после кадрового события формируется заявка на отключение работника от информационных систем, к которым ему ранее был предоставлен доступ на основании заявки в АС ОЗ.

В случае указанного кадрового события в отношении работника, которому ранее был предоставлен доступ к ИС на основании бизнес-роли, в соответствии с информацией, поступившей из ЕК АСУТР в АС ОЗ БР, автоматически инициируется процедура отключения рабочего места данного пользователя.

48. По окончании срока действия заявки, оформленной в АС ОЗ (ВП АС ОЗ), внутренний (внешний) пользователь отключается в автоматическом режиме от информационных систем, к которым ему был предоставлен доступ на основании указанной заявки.

49. В случае расторжения или окончания срока действия договора (соглашения) об электронном обмене данными между ОАО «РЖД» и внешней организацией подразделение ОАО «РЖД», заключившее указанный договор (соглашение), в течение суток после получения такой информации направляет письмом в Главный вычислительный центр (информационно-вычислительный центр) соответствующее уведомление, с указанием срока прекращения доступа к ИС.

Главный вычислительный центр (информационно-вычислительный центр) на основании поступившего уведомления направляет утвержденные заявки в АС ОЗ на блокировку доступа к ИС и отключение всех внешних пользователей указанной организации от информационных систем с учетом указанного в уведомлении срока прекращения доступа к ИС.

50. Продление срока доступа к ИС пользователя осуществляется на основании заявки, своевременно оформленной, согласованной и утвержденной в соответствии с настоящим Порядком.

51. Несоблюдение требований настоящего Порядка, а также правил работы внутренних пользователей в информационных системах, указанных в приложении № 4, является основанием для отключения внутреннего пользователя от всех информационных систем.

52. Невыполнение хотя бы одним внешним пользователем обязанностей, изложенных в договоре (соглашении) об электронном обмене данными, заключенным между ОАО «РЖД» и организацией внешнего пользователя, является основанием для отключения всех внешних пользователей данной организации от всех информационных систем, к которым им был предоставлен доступ.

53. Администраторы соответствующих информационных систем несут ответственность за несвоевременное отключение пользователей от информационных систем на основании согласованных заявок на блокировку доступа к ИС.

Проверку своевременности отключения пользователей от информационных систем осуществляют соответствующие администраторы безопасности информационных систем Главного вычислительного центра (информационно-вычислительных центров).

54. Контроль за организацией доступа к ИС внутренних и внешних пользователей, а также внутренних пользователей к сети «Интернет», обеспечением информационной безопасности при осуществлении электронного обмена данными осуществляют Департамент управления информационной безопасностью (региональные центры безопасности), Удостоверяющий центр Главного вычислительного центра (подразделения информационной безопасности информационно-вычислительных центров) в пределах своих полномочий.

55. Случаи невыполнения требований настоящего Порядка, предусматривающие персональную ответственность работников ОАО «РЖД», подлежат рассмотрению подразделением внутреннего пользователя в установленном ОАО «РЖД» порядке с привлечением при необходимости работников Департамента управления информационной безопасностью (региональных центров безопасности) и Главного вычислительного центра (информационно-вычислительных центров).

56. Работники ОАО «РЖД», виновные в невыполнении требований настоящего Порядка, несут ответственность в соответствии с законодательством Российской Федерации.

X. Хранение заявок (бизнес-ролей) на предоставление доступа к ИС

57. Оформленные заявки (бизнес-роли) на предоставление доступа к ИС и копии схем предоставления доступа к ИС хранятся в Главном вычислительном центре (информационно-вычислительных центрах) в течение одного года после отключения пользователя от информационных систем.

58. При предоставлении доступа к ИС, содержащим сведения, составляющие коммерческую тайну ОАО «РЖД», заявки с прилагаемыми материалами (бизнес-роли) хранятся в Главном вычислительном центре (информационно-вычислительных центрах) в течение 3 лет после отключения пользователя от указанных информационных систем.

Приложение № 1
к Порядку предоставления
доступа к информационным
системам ОАО «РЖД»

УТВЕРЖДАЮ
От Департамента информатизации

_____ И.О.Фамилия
(подпись)
«__»_____ 20__ г.

З А Я В К А
от «___» _____ 20__ г. № _____
на предоставление доступа к информационной системе ОАО «РЖД» (ИС)

_____
(наименование организации пользователя)

Информационная система			
Раздел ИС, АРМ и т.п.			
Тип подключения (ненужное зачеркнуть)	технологическое	информационное	обеспечивающее
Основание для подключения – дата и номер договора (распоряжения, приказа и т.п.), дата и номер сопроводительного письма. Цель подключения.			
Полное наименование организации юридического лица или структурного подразделения ОАО «РЖД», филиала ОАО «РЖД».			
Юридический адрес организации пользователя			
Подразделение пользователя			
Должность пользователя			
Фамилия И.О. пользователя, табельный номер		№	
Фактический адрес пользователя			
Номер телефона и адрес электронной почты пользователя			
Наличие на ПЭВМ пользователя специального системного и			

прикладного ПО	
Антивирусное ПО на ПЭВМ пользователя	
Заявка действительна по	
Рабочее время и дни доступа к ИС	
Позиции, заполняемые ГВЦ (ИВЦ)	
Протокол	
Ограничение полномочий (ИР, папка, база данных и т.п.)	
Права пользователя	
Наличие на ПЭВМ пользователя открытых портов и их назначение	

С правами и обязанностями внутренних пользователей при работе в информационных системах ОАО «РЖД» ознакомлен «__»___ 20__ г. _____И.О.Фамилия
(подпись)

Руководитель организации (подразделения) пользователя _____И.О.Фамилия
(подпись)

Начальник подразделения – распорядителя ИС _____И.О.Фамилия
(подпись)

Администратор ИС ГВЦ ОАО «РЖД» (ИВЦ) _____И.О.Фамилия
(подпись)

Администратор безопасности ГВЦ ОАО «РЖД» (ИВЦ) _____И.О.Фамилия
(подпись)

Начальник отдела безопасности информационных ресурсов ГВЦ ОАО «РЖД» (ИВЦ) _____И.О.Фамилия
(подпись)

Приложение № 2
к Порядку предоставления
доступа к информационным
системам ОАО «РЖД»

СОГЛАСОВАНО
Начальник_____
регионального центра безопасности

_____ И.О.Фамилия
(подпись)
«__»_____ 20__ г.

УТВЕРЖДАЮ
Начальник службы корпоративной
информатизации_____
железной дороги

_____ И.О.Фамилия
(подпись)
«__»_____ 20__ г.

ЗАЯВКА
от «___» _____ 20__ г. № _____
на предоставление доступа к информационной системе
ОАО «РЖД» (ИС)

Информационная система			
Раздел ИС, АРМ и т.п.			
Тип подключения (ненужное зачеркнуть)	технологическое	информационное	обеспечивающее
Основание для подключения – дата и номер договора (распоряжения, приказа и т.п.), дата и номер сопроводительного письма. Цель подключения.			
Полное наименование организации юридического лица или структурного подразделения ОАО «РЖД», филиала ОАО «РЖД».			
Юридический адрес организации пользователя			
Подразделение пользователя			
Должность пользователя			
Фамилия И.О. пользователя, табельный номер		№	
Фактический адрес пользователя			
Номер телефона и адрес электронной почты пользователя			
Наличие на ПЭВМ пользователя			

специального системного и прикладного ПО	
Антивирусное ПО на ПЭВМ пользователя	
Заявка действительна по	
Рабочее время и дни доступа к ИС	
Позиции, заполняемые ГВЦ (ИВЦ)	
Протокол	
Ограничение полномочий (ИР, папка, база данных и т.п.)	
Права пользователя	
Наличие на ПЭВМ пользователя открытых портов и их назначение	

С правами и обязанностями внутренних пользователей при работе в информационных системах ОАО «РЖД» ознакомлен «__»___ 20__ г. _____И.О.Фамилия
(подпись)

Руководитель организации (подразделения) пользователя _____И.О.Фамилия
(подпись)

Начальник подразделения – распорядителя ИС _____И.О.Фамилия
(подпись)

Администратор ИС ИВЦ _____И.О.Фамилия
(подпись)

Администратор безопасности ИВЦ _____И.О.Фамилия
(подпись)

Начальник подразделения информационной безопасности ИВЦ _____И.О.Фамилия
(подпись)

Приложение № 3
к Порядку предоставления
доступа к информационным
системам ОАО «РЖД»

СОГЛАСОВАНО
от Департамента управления
информационной безопасностью

_____ И.О.Фамилия
(подпись)
«__»_____ 20__ г.

УТВЕРЖДАЮ
от Департамента информатизации

_____ И.О.Фамилия
(подпись)
«__»_____ 20__ г.

ТИПОВАЯ СХЕМА

предоставления доступа к информационной системе ОАО «РЖД» (ИС)

(_____(железной дороги)
(наименование железной дороги)

_____
(наименование организации пользователя)

(Схема подключения ПЭВМ пользователя с указанием разделов ИС, АРМ и т.п.)

В схеме указываются: рабочая станция и ПЭВМ пользователей, подключение к ИВЦ или к ГВЦ, средства защиты информации (СЗИ), тип канала связи (СПД, сеть «Интернет» или др.), используемое активное сетевое и иное оборудование, через которое осуществляется подключение, а также СЗИ, используемые для защиты подключений (антивирусное программное обеспечение, средства защиты от НСД, средства обнаружения вторжений и др.).

Руководитель организации
(подразделения) пользователя _____ _____ «__»_____ 20___ г.
(подпись) (И.О.Фамилия)

М.П.

ПРИ ПОДКЛЮЧЕНИИ
ЧЕРЕЗ ИВЦ
от регионального центра
безопасности _____ _____ «__»_____ 20___ г.
(подпись) (И.О.Фамилия)

Администратор ИС ГВЦ
ОАО «РЖД» (ИВЦ) _____ _____ «__»_____ 20___ г.
(подпись) (И.О.Фамилия)

Администратор безопасности
ГВЦ ОАО «РЖД» (ИВЦ) _____ _____ «__»_____ 20___ г.
(подпись) (И.О.Фамилия)

Начальник УДЦ ГВЦ ОАО «РЖД»
_____ _____ «__»_____ 20___ г.
(подпись) (И.О.Фамилия)

Исп. (И.О.Фамилия)
(код города, телефон, эл. почта)

Приложение № 4
к Порядку предоставления
доступа к информационным
системам ОАО «РЖД»

Права и обязанности внутренних пользователей при работе в информационных системах ОАО «РЖД»

1. Внутренний пользователь при работе в информационных системах ОАО «РЖД» имеет право:

1) использовать информационные системы ОАО «РЖД» для более эффективного и качественного выполнения своих должностных обязанностей;

2) повышать уровень профессиональной квалификации с использованием доступных сетевых ресурсов и информационных систем ОАО «РЖД»;

3) использовать доступные информационные производственные приложения (корпоративные WEB-сайты, сетевые ресурсы и т.п.), расположенные в СПД;

4) обмениваться производственной информацией с внутренними и внешними пользователями информационных систем ОАО «РЖД» в соответствии с нормативными документами ОАО «РЖД»;

2. Внутренний пользователь при работе в ИС ОАО «РЖД» обязан:

1) сохранять в тайне свои пароли (ключевые носители) доступа к ПЭВМ, а также к информаицонным системам ОАО «РЖД»;

2) незамедлительно осуществить замену пароля (ключевого носителя) для доступа к ПЭВМ или информационной системе ОАО «РЖД» в соответствии с требованиями нормативных документов ОАО «РЖД» в случае его компрометации;

3) обеспечивать блокирование ПЭВМ парольной экранной заставкой во время перерывов в работе с информационной системой ОАО «РЖД»;

4) обеспечивать с помощью установленного антивирусного программного обеспечения проверку используемых съемных носителей информации на наличие вредоносных программ;

5) незамедлительно отключать ПЭВМ от СПД и сообщать об этом в ЕСПП при подозрении на появление вредоносных программ на ПЭВМ, автоматически не выявленных и не обезвреженных системой антивирусной защиты, или получение неправомерного доступа к ПЭВМ третьими лицами;

6) незамедлительно сообщать в ЕСПП в случае полного или частичного прекращения работы антивирусного программного обеспечения;

7) соблюдать условия обеспечения конфиденциальности обрабатываемой информации и защиты информационной системы ОАО «РЖД» от несанкционированного доступа;

8) обращаться в ЕСПП при обнаружении некорректной работы программного обеспечения на ПЭВМ.

3. Внутреннему пользователю при работе в информационной системе ОАО «РЖД» запрещается:

1) допускать использование ПЭВМ иными лицами, за исключением работников, осуществляющих обслуживание ПЭВМ, работников Департамента безопасности ОАО «РЖД» (регионального центра безопасности) и Департамента управления информационной безопасностью ОАО «РЖД», осуществляющих функции в соответствии с нормативными документами ОАО «РЖД»;

2) осуществлять несанкционированное подключение к ПЭВМ и сетевому оборудованию внешних устройств, в том числе устройств телекоммуникации и обработки информации;

3) использовать ПЭВМ в непроизводственных целях;

4) передавать информацию конфиденциального характера по незащищенным каналам сети передачи данных ОАО «РЖД»;

5) отключать «агента безопасности» либо вносить изменения в его настройки, а также самостоятельно устанавливать любые программные продукты на ПЭВМ или разрешать это кому-либо, за исключением работников, осуществляющих обслуживание ПЭВМ;

6) использовать ПЭВМ с частично или полностью неработающим антивирусным программным обеспечением, а также некорректной работой программного обеспечения;

7) использовать на ПЭВМ сменные носители информации, в том числе внешние средства хранения информации, без предварительной проверки на наличие вредоносных программ;

8) предоставлять сетевой доступ к своему ПЭВМ другим внутренним и внешним пользователям.

4. Внутреннему пользователю при работе в сети «Интернет» запрещается:

1) публиковать свои адреса (электронной почты, IP-адреса и т.п.), а также адреса других работников ОАО «РЖД» на общедоступных ресурсах сети «Интернет» (форумы, конференции и т.п.);

2) использовать общедоступные электронные почтовые системы и иные службы обмена сообщениями в личных целях, а также для распространения любой информации;

3) передавать сведения, создающие угрозу безопасности и обороноспособности государства, здоровью и безопасности людей, интересам ОАО «РЖД»;

4) запускать на ПЭВМ исполняемые файлы, полученные из сети «Интернет» (файлы с расширением exe, com, bat, scr, reg и т.п.);

5) обращаться к потенциально опасным ресурсам сети «Интернет».