

УТВЕРЖДЕНА

распоряжением АО «Кузбасс-пригород»

от «28» 03 2025 г. № 140

ПОЛИТИКА **информационной безопасности АО «Кузбасс-пригород»**

1. Общие положения

1.1. Настоящая Политика информационной безопасности АО «Кузбасс-пригород» (далее – Политика) представляет собой систематизированное изложение целей и задач обеспечения информационной безопасности, определяет характеристики информационной инфраструктуры АО «Кузбасс-пригород» и соответствующие ей основные угрозы информационной безопасности, а также основные мероприятия по обеспечению безопасности информационной инфраструктуры АО «Кузбасс-пригород», общие подходы к реализации отдельных мер (групп мер) защиты информации в информационных системах¹ и (или) информационно-телекоммуникационных сетях АО «Кузбасс-пригород».

1.2. Положения Политики направлены на обеспечение информационной безопасности информационной инфраструктуры АО «Кузбасс-пригород», в том числе на:

создание условий для безопасного функционирования информационных систем и (или) информационно-телекоммуникационных сетей АО «Кузбасс-пригород», информационной инфраструктуры АО «Кузбасс-пригород» в целом или ее отдельных компонентов²;

обеспечение эффективного функционирования и совершенствования системы управления информационной безопасностью АО «Кузбасс-пригород»;

минимизацию ущерба от возможных попыток нарушения информационной безопасности АО «Кузбасс-пригород».

1.3. Политика разработана на основе Стандарта ОАО «РЖД» СТО РЖД 18.002-2024 «Управление информационной безопасностью. Основные

¹ Термин «информационная система» используется как общее понятие для следующих терминов, используемых в нормативных правовых актах Российской Федерации, национальных стандартах, методических документах органов исполнительной власти, нормативных документах ОАО «РЖД»: «автоматизированная система», «автоматизированная система управления», «автоматизированная информационная система», «информационная система», «информационная система персональных данных» (СТО РЖД 18.002-2024, пункт 2.9).

² Под компонентом информационной инфраструктуры ОАО «РЖД» подразумевается любая ее часть – информационная система, информационно-телекоммуникационная сеть, элемент (комплекс элементов) информационной инфраструктуры (СТО РЖД 18.002-2024, пункт 2.8).

положения», с учетом требований законодательства Российской Федерации, нормативных правовых актов уполномоченных федеральных органов исполнительной власти, национальных стандартов Российской Федерации в области обеспечения информационной безопасности, международных стандартов в области информационной безопасности.

Политика не распространяется на деятельность по защите сведений, составляющих государственную тайну.

1.4. Политика предназначена для применения АО «Кузбасс-пригород». Положения Политики обязательны для исполнения работниками АО «Кузбасс-пригород».

Применение Политики сторонними организациями осуществляется на добровольной основе и оговаривается в договорах (соглашениях) с АО «Кузбасс-пригород».

2. Термины и определения

2.1. В Политике используются термины в соответствии со СТО РЖД 18.002-2024, а также следующие термины с соответствующими определениями.

2.1.1. Автоматизированное рабочее место –

программно-технический комплекс автоматизированной системы, предназначенный для автоматизации деятельности определенной категории пользователей³ или определенного вида деятельности (ГОСТ Р 59853-2021, раздел 2, пункт 3);

комплекс средств информационно-вычислительной техники и программного обеспечения, располагающийся непосредственно на рабочем месте специалиста и предназначенный для автоматизации его работы (Глоссарий ОСЖД Р 305-1, утвержденный I сессией Совещания Министров ОСЖД 13 – 16 июня 2023 г., раздел I, пункт 2).

2.1.2. **Идентификатор (учетная запись)** – строка символов, используемая для однозначной идентификации каждого субъекта доступа.

В АО «Кузбасс-пригород» могут применяться следующие типы идентификаторов (учетных записей):

временный – идентификатор (учетная запись), создаваемый на определенный промежуток времени, для выполнения конкретной задачи (например, для проведения обучения в техклассе, создаются на период прохождения обучения для каждого обучающегося);

общий (служебный) – идентификатор (учетная запись) для доступа к конкретным компонентам информационной инфраструктуры АО «Кузбасс-

³ Под пользователем подразумевается любой субъект доступа, являющийся физическим лицом.

пригород» определенного круга лиц для выполнения ими своих должностных обязанностей (например, сменные работники, диспетчеры, и т.п.);

персонифицированный – идентификатор (учетная запись) конкретного субъекта доступа информационного ресурса;

сервисный (технический) – идентификатор (учетная запись), используемый для осуществления логического доступа программными сервисами компонентов информационной инфраструктуры АО «Кузбасс-пригород», программными роботами и т.п.;

технологический (административный) – персонифицированный привилегированный идентификатор (учетная запись) конкретного работника для выполнения технологических операций (административных задач) на конкретном компоненте информационной инфраструктуры АО «Кузбасс-пригород».

2.1.3. Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов (Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», статья 2, пункт 2).

2.1.4. Информация конфиденциального характера – любая информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну.

2.1.5. Классификация – схема, в соответствии с которой объекты классификации подразделяются на категории с целью применения соответствующих защитных мер для этих категорий.

2.1.6. Контролируемая зона – пространство, в пределах которого осуществляется контроль над пребыванием и действиями лиц и (или) транспортных средств (ГОСТ Р 52863-2007, пункт 3.1.9).

2.1.7. Контур безопасности информации АО «Кузбасс-пригород» – часть информационной инфраструктуры АО «Кузбасс-пригород», для которой задан определенный класс (уровень) защищенности (категория значимости), на базе которой функционируют информационные системы АО «Кузбасс-пригород» не выше заданного класса (уровня) защищенности (категории значимости), и в рамках которой реализована единая номенклатура мер защиты информации и используются общие (или идентичные, типовые) средства защиты информации.

2.1.8. Машинный носитель – материальный носитель информации, предназначенный для записи и воспроизведения информации средствами вычислительной техники, а также сопрягаемыми с ними устройствами (внутренние и внешние жесткие диски, флеш-накопители, компакт-диски и иные устройства).

2.1.9. Мобильные технические средства – программно-аппаратные средства, предназначенные для повсеместного личного ношения людьми и способные выполнять прием, обработку, хранение и (или) передачу информации.

К мобильным техническим средствам относятся:

портативные вычислительные устройства (то есть устройства, основным назначением которых является сбор и (или) обработка информации, например: ноутбуки, нетбуки, планшеты, цифровые фото-видеокамеры, звукозаписывающие устройства и т.п.);

устройства связи с возможностью обработки информации (то есть устройства, основным назначением которых является передача информации, например: сотовые телефоны, смартфоны, смарт-часы, мобильные (карманные) маршрутизаторы, иные средства связи).

2.1.10. Носитель информации (материальный) – материальный объект, в том числе физическое поле, в котором информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин (ГОСТ Р 50922-2006, приложение А, пункт А.5).

2.1.11. Объект информатизации – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров (ГОСТ Р 51275-2006, пункт 3.1).

2.1.12. Подсистема защиты информации – часть информационной системы и (или) информационно-телекоммуникационной сети АО «Кузбасс-пригород», представляющая собой совокупность мер и средств контроля и управления (в том числе правовых мер, организационных мероприятий, технических, программных и программно-технических средств защиты информации и средств контроля эффективности защиты информации).

Термин «подсистема защиты информации» используется как общее понятие для следующих терминов, используемых в нормативных правовых актах Российской Федерации, национальных стандартах, методических документах органов исполнительной власти, нормативных документах АО «Кузбасс-пригород»: «подсистема безопасности», «подсистема защиты», «система безопасности», «система защиты».

2.1.13. Прикладное программное обеспечение – программное обеспечение, автоматизирующее бизнес-процессы АО «Кузбасс-пригород».

2.1.14. Сеть общетехнологического назначения – специализированная сеть передачи данных, предназначенная для обеспечения информационного взаимодействия автоматизированных рабочих мест работников АО «Кузбасс-пригород» с работниками железнодорожного транспорта, организации автоматизированного электронного документооборота, организации доступа и передачи информации в базы данных Главного вычислительного центра и его структурных подразделений на полигонах железных дорог и др. (адаптировано из Норм технологического проектирования цифровых телекоммуникационных сетей на федеральном железнодорожном транспорте (НТП ЦТКС-ФЖТ-2002), пункт 3.3.2.1).

2.1.15. Сеть оперативно-технологического назначения – специализированная сеть передачи данных, предназначенная для обеспечения функционирования систем диспетчерского управления и контроля в режиме реального времени (адаптировано из ГОСТ 33889-2016, пункт 44).

2.1.16. Системное программное обеспечение – комплекс программ, которые обеспечивают управление ресурсами средств вычислительной техники (процессор, оперативная память, устройства ввода-вывода, сетевое оборудование и пр.) и предоставление прикладному программному обеспечению сервисных функций, абстрагирующих детали аппаратной и микропрограммной реализации этих средств.

2.1.17. Съёмный машинный носитель (информации) – машинный носитель, используемый для хранения информации вне автоматизированного рабочего места (флеш-накопители, внешние жесткие диски, компакт-диски и иные устройства).

3. Сокращения

3.1. В Политике используются следующие сокращения:

АРМ	– автоматизированное рабочее место
ИБ	– информационная безопасность
ИИ	– информационная инфраструктура
ИС	– информационная система
ИТКС	– информационно-телекоммуникационная сеть
МНИ	– машинный носитель информации
ОРД	– организационно-правовой и (или) распорядительный документ
О	– программное обеспечение

СУИБ	– система управления информационной безопасностью
УБИ	– угроза безопасности информации
ФСБ России	– Федеральная служба безопасности Российской Федерации
ФСТЭК России	– Федеральная служба по техническому и экспортному контролю
ЦОД	– центр обработки данных

4. Цель и задачи обеспечения информационной безопасности АО «Кузбасс-пригород»

4.1. Основной целью обеспечения информационной безопасности (далее – ИБ) является защита информационных ресурсов (активов) АО «Кузбасс-пригород» от возможного нанесения им материального, физического или иного ущерба посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы ее обработки и передачи, а также минимизация рисков ИБ. Это непрерывный процесс, при котором меры защиты информации реализуются с учетом актуальных угроз безопасности информации (далее – УБИ) информационной инфраструктуры (далее – ИИ) АО «Кузбасс-пригород».

4.2. Основными задачами обеспечения ИБ являются обеспечение непрерывности и эффективности бизнес-процессов АО «Кузбасс-пригород», а также минимизация ущерба от возможных попыток нарушения ИБ АО «Кузбасс-пригород».

4.3. Для управления процессом обеспечения ИБ в АО «Кузбасс-пригород» функционирует система управления информационной безопасностью (далее – СУИБ), позволяющая решать следующие задачи:

4.3.1. выполнение в АО «Кузбасс-пригород» требований законодательства Российской Федерации и методических документов органов исполнительной власти, уполномоченных в области обеспечения ИБ, в том числе:

разработка организационно-правовых и методических документов по управлению ИБ в АО «Кузбасс-пригород»;

определение актуальных УБИ для информационных систем (далее – ИС) и (или) информационно-телекоммуникационных сетей (далее – ИТКС) АО «Кузбасс-пригород»;

реализация правовых, организационных и технических мер защиты информации в АО «Кузбасс-пригород»;

4.3.2. осуществление эффективного управления ИБ в ИИ АО «Кузбасс-пригород»,
в том числе:

своевременное выявление и реагирование на инциденты ИБ с использованием централизованно применяемых систем мониторинга и управления ИБ;

контроль (анализ) защищенности информации, содержащейся в ИИ АО «Кузбасс-пригород», с использованием централизованно применяемых систем контроля (анализа) защищенности;

минимизация последствий реализации актуальных УБИ в отношении ИИ АО «Кузбасс-пригород»;

обеспечение взаимоувязанного по времени, целям и задачам взаимодействия структурных подразделений АО «Кузбасс-пригород» по ИБ, сторонних организаций (в рамках выполнения ими договорных обязательств по ИБ), задействованных в процессах обеспечения ИБ;

4.3.3. обеспечение единой технической политики ИБ ИИ АО «Кузбасс-пригород»,
в том числе:

разработка, внедрение и сопровождение технического обеспечения управления ИБ;

категорирование объектов критической информационной инфраструктуры АО «Кузбасс-пригород»;

классификация компонентов ИИ АО «Кузбасс-пригород», формирование требований по безопасности информации, контроль и оценка соответствия компонентов ИИ и информационных активов⁴ АО «Кузбасс-пригород» требованиям по безопасности информации;

4.3.4. определение обязанностей работников АО «Кузбасс-пригород» по вопросам обеспечения ИБ, разработка, внедрение и ведение процессов повышения квалификации и осведомленности работников по вопросам ИБ;

4.3.5. обеспечение непрерывного совершенствования обеспечения ИБ ИИ АО «Кузбасс-пригород», в том числе:

анализ и оценка рисков нарушения ИБ для ИИ АО «Кузбасс-пригород»;

разработка планов долгосрочного и среднесрочного развития обеспечения ИБ АО «Кузбасс-пригород»;

⁴ Один из видов активов организации, в том числе различные виды информации, циркулирующие в информационных системах (служебная, управляющая, аналитическая, деловая и т.д.) на всех этапах жизненного цикла (генерация, хранение, обработка, передача, уничтожение) (СТО РЖД 18.002-2024, пункт 2.1).

5. Краткая характеристика информационной инфраструктуры АО «Кузбасс-пригород»

5.1. ИИ АО «Кузбасс-пригород» является территориально-распределенной. ИИ АО «Кузбасс-пригород» предполагает расположение ее компонентов на территориально удаленных друг от друга объектах размещения.

К объектам размещения могут относиться:

объекты информатизации Главного вычислительного центра и его структурных подразделений;

объекты информатизации участков производства АО «Кузбасс-пригород».

Объектами размещения также могут являться здания и помещения третьих лиц.

5.2. ИИ АО «Кузбасс-пригород» взаимодействует с сетями связи общего пользования, в том числе с сетью «Интернет», для обеспечения:

оказания услуг юридическим и физическим лицам;

взаимодействия ИС АО «Кузбасс-пригород» с ИС внешних организаций;

возможности ведения переписки посредством цифровых технологий;

взаимодействия с органами государственной власти, юридическими и физическими лицами.

5.3. Все создаваемые компоненты ИИ АО «Кузбасс-пригород» должны разрабатываться с учетом требований ИБ, установленных законодательством Российской Федерации, национальными и применимыми международными стандартами, нормативными документами АО «Кузбасс-пригород».

Развитие и модернизация ИИ АО «Кузбасс-пригород» должны осуществляться с учетом требований к безопасной разработке программного обеспечения (далее – ПО), содержащихся в нормативных правовых актах Российской Федерации, АО «Кузбасс-пригород».

5.4. При формировании требований ИБ в рамках создания (модернизации) компонентов ИИ АО «Кузбасс-пригород» должна учитываться необходимость защиты следующих основных активов ИИ АО «Кузбасс-пригород» (объектов защиты):

ИС и (или) ИТКС АО «Кузбасс-пригород», а также их сегментов;

информационных активов, содержащихся в ИС АО «Кузбасс-пригород»;

элементов ИИ АО «Кузбасс-пригород».

5.5. В качестве основных информационных активов АО «Кузбасс-пригород», подлежащих защите (объектов защиты), необходимо рассматривать:

информацию конфиденциального характера (включая, но не ограничиваясь: персональные данные, информацию, составляющую коммерческую тайну, а также поступающие в АО «Кузбасс-пригород» из

органов государственной власти документы с пометкой «Для служебного пользования»), служебную информацию;

технологическую информацию (информацию о структуре ИС и (или) ИТКС АО «Кузбасс-пригород», о конфигурации и параметрах настройки программных и программно-технических средств и т.п., за исключением информации конфиденциального характера);

общедоступную информацию АО «Кузбасс-пригород».

5.6. В качестве основных элементов ИИ АО «Кузбасс-пригород», подлежащих защите (объектов защиты), необходимо рассматривать:

технические и программно-технические средства обработки, хранения и передачи информации;

системное и прикладное ПО;

проводные и беспроводные линии (сети, каналы) связи, применяемые для связи компонентов ИС и (или) ИТКС между собой и с другими ИС и (или) ИТКС АО «Кузбасс-пригород» и иных организаций.

5.7. Состав объектов защиты должен уточняться по результатам регулярной инвентаризации (учета) активов ИИ АО «Кузбасс-пригород». Инвентаризация (учет) активов ИИ АО «Кузбасс-пригород», формирующихся в рамках Программы цифровизации проводится ответственным за информатизацию (цифровизацию) в АО «Кузбасс-пригород».

Для обеспечения инвентаризации (учета) активов ИИ АО «Кузбасс-пригород» необходимо:

идентифицировать владельцев всех основных активов ИИ АО «Кузбасс-пригород» и определить их ответственность за поддержание соответствующих мероприятий по управлению ИБ;

регламентировать порядок инвентаризации (учета) активов ИИ АО «Кузбасс-пригород»;

осуществлять проверки актуальности активов ИИ АО «Кузбасс-пригород» на регулярной основе.

Неучтенные активы ИИ АО «Кузбасс-пригород» могут быть отключены до принятия решения об их дальнейшей эксплуатации.

5.8. Для размещения информационных активов ИИ АО «Кузбасс-пригород» допускается использование вычислительных ресурсов сторонних организаций на основании заключенных договоров.

5.9. Работы и услуги по информационной безопасности, используемые и выполняемые подрядчиками, разработчиками, поставщиками в интересах АО «Кузбасс-пригород», могут пройти добровольное подтверждение соответствия в системе добровольной сертификации ОАО «РЖД» с областью сертификации «Информационная безопасность».

6. Основные угрозы безопасности информации информационной инфраструктуры АО «Кузбасс-пригород»

6.1. Наличие УБИ обуславливается множеством различных факторов, а их реализация возможна при определенных условиях, основным из которых для ИИ АО «Кузбасс-пригород» является наличие уязвимостей в активах АО «Кузбасс-пригород».

6.2. Для различных объектов защиты характерно действие различных факторов, определяющих возможность актуальности следующих видов УБИ:

6.2.1. угрозы, обусловленные внутренними факторами:

угрозы, обусловленные применяемыми информационными технологиями (облачными, суперкомпьютерными, мобильными, беспроводными технологиями, web- и грид-технологиями, технологиями виртуализации, больших данных (Big Data), предиктивного анализа, блокчейн-технологиями и др.);

угрозы, обусловленные используемой элементной базой (базовыми системами ввода-вывода (BIOS/UEFI) и иным микропрограммным обеспечением (firmware), операционными системами, системами управления базами данных, программами и устройствами обработки информации, машинными носителями информации (далее – МНИ), оперативной памятью, ИТКС, устройствами ввода-вывода информации, средствами установки и контроля за работой программ и механизмов, устройствами типа SoC⁵ и др.);

угрозы, обусловленные использованием средств защиты информации (средств идентификации и аутентификации, управления доступом, потоками информации, средств межсетевого экранирования, антивирусной защиты, контроля (анализа) защищенности, обнаружения (предотвращения) вторжений, регистрации событий ИБ, имитации деятельности субъектов доступа, создания доверенной программно-аппаратной среды и др.);

угрозы, обусловленные потенциально опасными действиями доверенных людей (ошибками, допущенными в ходе проектирования, разработки, интеграции компонентов в ИИ АО «Кузбасс-пригород», ошибками, допущенными в ходе эксплуатации компонентов ИИ АО «Кузбасс-пригород», действиями внутренних пользователей);

6.2.2. угрозы, обусловленные внешними факторами:

угрозы, связанные с проведением компьютерных атак (угрозы сбора и анализа сведений, неправомерного внедрения различных программных и (или) программно-аппаратных средств, обмана при взаимодействии с компонентами ИИ АО «Кузбасс-пригород», манипулирования временем и

⁵ SoC – System on Crystal (с англ. система на кристалле) – электронная схема, выполняющая функции целого устройства (например, компьютера).

состоянием компонентов ИИ АО «Кузбасс-пригород», злоупотребления функциональными возможностями компонентов ИИ АО «Кузбасс-пригород», расширения привилегий и распространения влияния в компонентах ИИ АО «Кузбасс-пригород», манипулирования ресурсами, структурами данных и пользователями ИС АО «Кузбасс-пригород», угрозы применения вероятностных техник в отношении защитного (криптографического) кодирования информации, получения физического доступа к компонентам ИИ АО «Кузбасс-пригород» и др.);

угрозы правового характера (угрозы негативного воздействия на бизнес-процессы из-за нарушения обязательных к применению требований и обеспечительных досудебных мер, угрозы негативных изменений в законодательстве стран присутствия, неспособности разрешения конфликта юрисдикций и др.);

техногенные угрозы (угрозы сбоев, отказа в работе технических устройств, возникновения ошибок в обработке программного кода процессором, перебоев электропитания, критического снижения качества услуг связи и др.);

стихийные угрозы (угрозы повреждения компонентов ИИ АО «Кузбасс-пригород» вследствие пожаров, наводнений, землетрясений, обвалов, лавин и др.).

6.3. Перечень УБИ, актуальных для конкретных компонентов ИИ АО «Кузбасс-пригород», должен определяться в соответствующих моделях угроз безопасности информации. В качестве исходных данных при определении актуальных УБИ должен использоваться Банк данных УБИ, ведение которого осуществляется ФСТЭК России, а также результаты анализа инцидентов ИБ конкретных компонентов ИИ или компонентов ИИ аналогичного типа.

6.4. При определении актуальных УБИ для компонентов ИИ АО «Кузбасс-пригород» необходимо руководствоваться требованиями законодательства Российской Федерации, методических документов ФСТЭК России, ФСБ России и нормативных документов ОАО «РЖД» в области обеспечения ИБ.

6.5. При определении актуальных УБИ в ИС и (или) ИТКС АО «Кузбасс-пригород», функционирующих на базе инфраструктуры ЦОД, должны учитываться УБИ, актуальные для инфраструктуры ЦОД.

7. Порядок обеспечения информационной безопасности информационной инфраструктуры АО «Кузбасс-пригород»

7.1. Обеспечение информационной безопасности ИИ АО «Кузбасс-пригород» должно включать:

регламентацию параметров настройки средств защиты информации;

сегментирование ИИ АО «Кузбасс-пригород» с учетом выполняемых бизнес-процессов и в соответствии с требованиями по безопасности информации;

применение встроенных механизмов защиты используемого системного и прикладного ПО, прошедших оценку соответствия требованиям по безопасности информации;

использование в ИИ АО «Кузбасс-пригород» средств защиты информации, прошедших оценку соответствия требованиям по безопасности информации, преимущественно российского производства;

использование централизованно применяемых средств аудита и мониторинга ИБ;

использование централизованно применяемых средств и систем контроля за действиями пользователей ИС и (или) ИТКС АО «Кузбасс-пригород», обнаружения вторжений, анализа и оценки защищенности;

применение средств криптографической защиты информации, прошедших оценку соответствия требованиям по безопасности информации.

7.2. Должны быть разработаны и применяться обязательные требования к процессу создания (разработки), оценки, эксплуатации и сопровождения компонентов ИИ АО «Кузбасс-пригород» в части мер защиты информации.

Обеспечение безопасности компонентов ИИ АО «Кузбасс-пригород» должно проводиться на всех этапах жизненного цикла компонентов ИИ АО «Кузбасс-пригород» и предусматривать выполнение следующих мероприятий.

7.2.1. Выбор применимых нормативных правовых актов и методических документов уполномоченных органов государственной власти, нормативных документов ОАО «РЖД», определяющих требования и рекомендации по безопасности информации.

7.2.2. Формирование требований по обеспечению безопасности информации в компонентах ИИ АО «Кузбасс-пригород», предусматривающее:

проведение информационного обследования компонентов ИИ АО «Кузбасс-пригород» в части вопросов защиты информации, в том числе, определения перечня защищаемой информации, необходимости обеспечения ее конфиденциальности, целостности и (или) доступности;

определение УБИ, реализация которых может привести к нарушению безопасности информации, с использованием сведений об УБИ, изложенных в Банке данных УБИ ФСТЭК России (<http://bdu.fstec.ru>) и иных источниках, опубликованных в сети «Интернет», и разработку на их основе модели угроз и нарушителя безопасности информации;

категорирование ИС и (или) ИТКС АО «Кузбасс-пригород» путем установления их соответствия критериям значимости, показатели которых устанавливаются Правительством Российской Федерации (в случае отнесения

этих ИС и (или) ИТКС к объектам критической информационной инфраструктуры, подлежащих категорированию);

классификацию компонентов ИИ АО «Кузбасс-пригород» по требованиям безопасности информации в соответствии с требованиями законодательства Российской Федерации в области обеспечения ИБ;

определение требований к подсистеме защиты информации, обрабатываемой в компоненте ИИ АО «Кузбасс-пригород», в том числе с учетом распределения ответственности за выполнение таких требований между ИС, функционирующей на базе общей инфраструктуры (комплекса элементов ИИ АО «Кузбасс-пригород», используемых более чем в одной ИС), и этой инфраструктурой (комплексом элементов ИИ АО «Кузбасс-пригород»).

7.2.3. Разработка (проектирование) подсистемы защиты информации компонента ИИ АО «Кузбасс-пригород», предусматривающая:

проектирование подсистемы защиты информации компонента ИИ АО «Кузбасс-пригород» с учетом сформированных требований по безопасности информации;

макетирование и тестирование подсистемы защиты информации компонента ИИ АО «Кузбасс-пригород». Необходимость проведения макетирования и тестирования подсистемы защиты информации компонента ИИ АО «Кузбасс-пригород» должна определяться совместно функциональным заказчиком и разработчиком подсистемы защиты информации.

При разработке (проектировании) подсистемы защиты информации компонента ИИ АО «Кузбасс-пригород» следует учитывать, что решения по подсистеме защиты информации ИС и (или) ИТКС АО «Кузбасс-пригород» могут предусматривать реализацию отдельных мер (групп мер) защиты информации на уровне общей инфраструктуры нескольких ИС и (или) элементов (комплекса элементов) ИИ АО «Кузбасс-пригород», а также предполагать модернизацию всей ИИ АО «Кузбасс-пригород».

Введение в постоянную эксплуатацию ИС АО «Кузбасс-пригород», в составе которой отсутствует подсистема защиты информации, не допускается.

Обеспечение защиты информации в ходе модернизации компонентов ИИ АО «Кузбасс-пригород» должно осуществляться в соответствии с требованиями, установленными при их создании.

7.2.4. Внедрение средств защиты информации, ПО, реализующего функции безопасности, иных технических средств и систем в соответствии с проектом подсистемы защиты информации компонента ИИ АО «Кузбасс-пригород».

7.2.5. Проведение оценки соответствия прикладного ПО компонента ИИ АО «Кузбасс-пригород» требованиям по безопасности информации (при необходимости).

7.2.6. Внедрение подсистемы защиты информации компонента ИИ АО «Кузбасс-пригород», предусматривающее:

- установку и настройку средств защиты информации;
- интеграцию с централизованно применяемыми в ОАО «РЖД» и АО «Кузбасс-пригород» системами мониторинга и управления ИБ;
- внедрение организационных мер защиты информации;
- предварительные испытания подсистемы защиты информации компонента ИИ АО «Кузбасс-пригород»;
- опытную эксплуатацию подсистемы защиты информации компонента ИИ АО «Кузбасс-пригород»;
- доработку проектных решений подсистемы защиты информации компонента ИИ АО «Кузбасс-пригород» (при необходимости);
- анализ уязвимостей компонента ИИ АО «Кузбасс-пригород» и принятие мер защиты информации по их устранению (компенсирующих мер защиты информации);
- приемочные испытания подсистемы защиты информации компонента ИИ АО «Кузбасс-пригород»;
- ввод подсистемы защиты информации компонента ИИ АО «Кузбасс-пригород» в постоянную эксплуатацию.

При реализации мер (групп мер) защиты информации в отдельных элементах (комплексах элементов) ИИ АО «Кузбасс-пригород» следует учитывать их техническую реализуемость для конкретных элементов (комплексов элементов) ИИ АО «Кузбасс-пригород».

Для защиты программно-технических средств компонентов ИИ АО «Кузбасс-пригород» должны быть обеспечены следующие условия:

- эксплуатация программно-технических средств компонентов ИИ АО «Кузбасс-пригород» в соответствии с эксплуатационной документацией;
- безопасность и отказоустойчивость программно-технических средств компонентов ИИ АО «Кузбасс-пригород»;
- защита конфигурационных данных (настроек) программно-технических средств компонентов ИИ АО «Кузбасс-пригород»;
- защита от сбоев программно-технических средств компонентов ИИ АО «Кузбасс-пригород»;
- организация контролируемой зоны для программно-технических средств компонентов ИИ АО «Кузбасс-пригород» (обеспечение границ контролируемой зоны);
- контроль физического доступа к программно-техническим средствам, средствам защиты информации, средствам обеспечения функционирования компонентов ИИ АО «Кузбасс-пригород», а также в помещения и сооружения, в которых они установлены;

защита собственных линий связи компонентов ИИ АО «Кузбасс-пригород» от несанкционированного доступа к ним (на предмет повреждений и др.);

размещение устройств вывода информации конфиденциального характера (в том числе мониторов, принтеров), исключающее возможность несанкционированного просмотра выводимой информации как из-за пределов контролируемой зоны, так и в ее пределах;

защита от внешних воздействий на программно-технические средства компонентов ИИ АО «Кузбасс-пригород»;

применение средств защиты информации и средств криптографической защиты информации в соответствии с требованиями эксплуатационной документации.

7.2.7. Определение соответствия компонента ИИ АО «Кузбасс-пригород» требованиям законодательства Российской Федерации, нормативных документов ОАО «РЖД» и АО «Кузбасс-пригород» в области обеспечения ИБ в соответствующей(-их) форме(-ах) (аттестация по требованиям безопасности информации, оценка эффективности принимаемых мер по обеспечению безопасности персональных данных, оценка соответствия требованиям по безопасности информации).

При этом:

7.2.7.1. аттестация по требованиям безопасности информации проводится в отношении:

ИС и (или) ИТКС АО «Кузбасс-пригород», в которых обрабатывается информация, составляющая коммерческую тайну, и (или) которые относятся к значимым объектам критической информационной инфраструктуры АО «Кузбасс-пригород»;

информационно-телекоммуникационной инфраструктуры ЦОД АО «Кузбасс-пригород», на базе которой функционируют ИС АО «Кузбасс-пригород», в которых обрабатывается информация, составляющая коммерческую тайну;

общей инфраструктуры нескольких ИС (комплекса элементов ИИ) АО «Кузбасс-пригород», на базе которой они функционируют, и в которых обрабатывается информация, составляющая коммерческую тайну;

7.2.7.2. оценка эффективности принимаемых мер по обеспечению безопасности персональных данных проводится в отношении ИС АО «Кузбасс-пригород», в которых обрабатываются персональные данные;

7.2.7.3. оценка соответствия требованиям по безопасности информации проводится в соответствии с требованиями законодательства Российской Федерации о техническом регулировании в отношении ИС и (или) ИТКС АО «Кузбасс-пригород», в которых не обрабатываются персональные данные и информация, составляющая коммерческую тайну.

До проведения соответствующей оценки компоненты ИИ АО «Кузбасс-пригород» могут вводиться в постоянную эксплуатацию, но без возможности обработки информации конфиденциального характера.

Запрещается вводить в постоянную эксплуатацию без проведения оценки соответствия требованиям законодательства Российской Федерации, нормативных документов ОАО «РЖД» и АО «Кузбасс-пригород» в области обеспечения ИБ ИС и (или) ИТКС, являющиеся значимыми объектами критической информационной инфраструктуры АО «Кузбасс-пригород».

7.2.8. Поддержание ИБ в ходе эксплуатации компонентов ИИ АО «Кузбасс-пригород», предусматривающее:

- планирование мероприятий по обеспечению безопасности в компоненте ИИ АО «Кузбасс-пригород», включающих в том числе создание подсистем защиты информации для компонентов ИИ АО «Кузбасс-пригород», введенных в эксплуатацию до утверждения Политики;

- анализ актуальности УБИ компонента ИИ АО «Кузбасс-пригород» и последствий от их реализации;

- управление (администрирование) подсистемой защиты информации компонента ИИ АО «Кузбасс-пригород»;

- управление конфигурацией компонента ИИ АО «Кузбасс-пригород», в том числе входящей в его состав подсистемы защиты информации;

- реагирование на инциденты ИБ в ходе эксплуатации компонента ИИ АО «Кузбасс-пригород»;

- обеспечение действий в нештатных ситуациях в ходе эксплуатации компонента ИИ АО «Кузбасс-пригород»;

- информирование и обучение (инструктаж) персонала;

- контроль обеспечения безопасности компонента ИИ АО «Кузбасс-пригород».

7.2.9. Обеспечение защиты информации при выводе из эксплуатации компонента ИИ АО «Кузбасс-пригород», предусматривающее:

- архивирование информации при необходимости ее дальнейшего использования в деятельности АО «Кузбасс-пригород»;

- уничтожение данных и остаточной информации с МНИ и (или) уничтожение МНИ;

- уничтожение данных об архитектуре и конфигурации компонента ИИ АО «Кузбасс-пригород»;

- архивирование или уничтожение эксплуатационной документации на компонент ИИ АО «Кузбасс-пригород», в том числе на входящую в его состав подсистему защиты информации, а также документов, определяющих правила и процедуры, реализуемые для обеспечения защиты информации в компоненте ИИ

АО «Кузбасс-пригород» в ходе эксплуатации (далее – ОРД по защите информации).

8. Обеспечение информационной безопасности работниками АО «Кузбасс-пригород»

8.1. Обязанности по обеспечению информационной безопасности должны быть доведены до работника АО «Кузбасс-пригород» при трудоустройстве под роспись до того момента, как работник будет допущен к использованию информационных ресурсов ОАО «РЖД» и АО «Кузбасс-пригород».

В должностной инструкции работника должна быть установлена его ответственность за нарушение ИБ.

8.2. Работник АО «Кузбасс-пригород», чьи должностные обязанности предусматривают обработку персональных данных, должен подписать обязательство о неразглашении персональных данных.

8.3. Все работники должны быть ознакомлены под роспись с перечнями информации конфиденциального характера, обрабатываемой в АО «Кузбасс-пригород», с установленными режимами ее защиты и с мерами ответственности за нарушение этих режимов.

8.4. Уполномоченные сотрудники АО «Кузбасс-пригород» в установленном в АО «Кузбасс-пригород» порядке имеют право проводить проверки:

выполнения действующих нормативных документов ОАО «РЖД» и АО «Кузбасс-пригород» по вопросам ИБ;

данных, находящихся на носителях информации;

порядка использования работниками информационных ресурсов ОАО «РЖД» и АО «Кузбасс-пригород»;

содержания служебной переписки;

выполняемых работниками действий на своих автоматизированных рабочих местах (далее – АРМ);

иные проверки в области обеспечения ИБ.

8.5. Все работники должны проходить обучение (инструктаж) в области обеспечения ИБ и конкретных процедур реализации мероприятий по безопасности, принятых в АО «Кузбасс-пригород», на регулярной основе.

9. Реализация документооборота в АО «Кузбасс-пригород» с учетом требований по безопасности информации

9.1. Порядок разработки, приемки, учета, хранения и уничтожения документов АО «Кузбасс-пригород», в том числе с использованием

электронного документооборота, и материальных носителей информации должны быть регламентированы.

9.2. На документах АО «Кузбасс-пригород», содержащих информацию, составляющую коммерческую тайну АО «Кузбасс-пригород», должен проставляться соответствующий гриф.

9.3. Должны быть установлены правила разграничения доступа работников к документам, содержащим информацию конфиденциального характера. В нормативных документах по организации документооборота в АО «Кузбасс-пригород» должны быть отражены правила и процедуры работы с документами АО «Кузбасс-пригород», а также особенности работы с документацией, содержащей информацию конфиденциального характера. Положения указанных нормативных документов АО «Кузбасс-пригород» должны быть доведены до сведения всех работников ОАО «РЖД», в том числе вновь принимаемых на работу, под роспись.

10. Использование электронных почтовых сервисов

10.1. При использовании средств электронной почты ОАО «РЖД» и АО «Кузбасс-пригород» должны быть выполнены:

разграничение внутренней (прием и передача информации между работниками структурных подразделений АО «Кузбасс-пригород») и внешней (прием и передача информации между АО «Кузбасс-пригород» и сторонними организациями) электронной почты ОАО «РЖД» и АО «Кузбасс-пригород»;

антивирусное сканирование почтовых сообщений, передаваемых и получаемых пользователями электронной почтовой системы ОАО «РЖД» и АО «Кузбасс-пригород»;

защита от спама и вирусов при получении почтовых сообщений из сети «Интернет»;

мониторинг и анализ информации, принимаемой и передаваемой посредством электронной почтовой системы ОАО «РЖД» и АО «Кузбасс-пригород», на предмет соответствия информационного обмена установленным в АО «Кузбасс-пригород» ограничениям;

использование разрешенных к применению в АО «Кузбасс-пригород» способов шифрования, в соответствии с Рекомендациями по использованию технологий передачи персональных данных в электронном виде по сетям связи, принятыми к руководству распоряжением ОАО «РЖД» от 16 марта 2018 г. № 508/р, при передаче по электронной почтовой системе ОАО «РЖД» и АО «Кузбасс-пригород» сообщений, содержащих персональные данные;

использование средств криптографической защиты информации при передаче по электронной почтовой системе ОАО «РЖД» и АО «Кузбасс-

пригород» сообщений, содержащих информацию, составляющую коммерческую тайну, а также поступающих в АО «Кузбасс-пригород» из органов государственной власти документов с пометкой «Для служебного пользования».

10.2. При использовании электронной почтовой системы ОАО «РЖД» и АО «Кузбасс-пригород» запрещается:

передача информации конфиденциального характера (информации, составляющей коммерческую тайну, персональных данных, а также поступающих в АО «Кузбасс-пригород» из органов государственной власти документов с пометкой «Для служебного пользования») в незащищенном виде;

использование в личных целях (электронная почта должна использоваться работниками АО «Кузбасс-пригород» только для выполнения служебных обязанностей);

настройка автоматической пересылки служебных сообщений на общедоступные почтовые сервисы.

10.3. Запрещается использование для пересылки служебной информации общедоступных электронных почтовых сервисов, файловых и облачных хранилищ, мессенджеров (WhatsApp, Telegram и др.).

11. Информирование и обучение персонала

11.1. Информирование персонала АО «Кузбасс-пригород» предусматривает доведение до работников информации о мероприятиях по обеспечению ИБ, правилах безопасной работы с информационными ресурсами АО «Кузбасс-пригород», в том числе связанных с использованием средств защиты информации. Информирование может проводиться одним из следующих способов:

информационная рассылка;

наглядная агитация.

11.2. Периодичность обучения всего персонала АО «Кузбасс-пригород» в области информационной безопасности регламентирована утверждаемым АО «Кузбасс-пригород» Перечнем требований к обязательным видам обучения руководителей и специалистов АО «Кузбасс-пригород», предусмотренных федеральными законами и иными нормативными правовыми актами Российской Федерации.

11.3. Работники структурных подразделений АО «Кузбасс-пригород», входящих в организационную структуру управления ИБ в соответствии со СТО РЖД 18.002-2024, должны проходить подготовку и повышение квалификации в образовательных организациях (специализированных учебных центрах) по программам обучения, согласованным с уполномоченными в

области обеспечения безопасности и технической защиты информации федеральными органами исполнительной власти, не реже одного раза в 5 лет, а также обучение (инструктаж) по порядку эксплуатации и администрированию применяемых в АО «Кузбасс-пригород» средств защиты информации.

11.4. Лица, ответственные за:

организацию обработки персональных данных в АО «Кузбасс-пригород»,
обеспечение безопасности персональных данных в информационных системах АО «Кузбасс-пригород»,

организацию обращения с информацией, составляющей коммерческую тайну, в АО «Кузбасс-пригород»,

ведение конфиденциального делопроизводства в АО «Кузбасс-пригород»,
должны проходить регулярное обучение с использованием Системы дистанционного обучения.

11.5. При подготовке работников АО «Кузбасс-пригород», осуществляющих эксплуатацию компонентов ИИ АО «Кузбасс-пригород», должно быть предусмотрено проведение практических занятий по правилам безопасной работы в ИС и (или) ИТКС, с элементами (комплексами элементов) ИИ АО «Кузбасс-пригород», а также по работе со средствами защиты информации.

11.6. Обучение также должно предусматривать на регулярной основе отработку действий (учения, тренировки) в нештатных ситуациях, в том числе:

в условиях ограничения доступа к информационным ресурсам АО «Кузбасс-пригород»;

по реагированию на инциденты ИБ;

по ликвидации последствий инцидентов ИБ.

12. Физический доступ

12.1. Доступ в помещения, в которых размещаются информационные ресурсы АО «Кузбасс-пригород», средства обработки информации (в том числе аттестованные АРМ для осуществления лицензируемых видов деятельности) и вспомогательное инженерное оборудование (устройства электропитания, кондиционирования, коммуникации и др.), должен контролироваться при помощи технических средств управления доступом или уполномоченными лицами и предоставляться только авторизованному персоналу АО «Кузбасс-пригород» или сторонних организаций.

12.2. Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие в нерабочее время, а также во время отсутствия в этих помещениях работающих в них работников АО «Кузбасс-пригород». Должен вестись учет выдачи ключей для доступа в эти помещения.

12.3. Окна и двери серверных помещений должны быть оборудованы металлическими решетками, охранной сигнализацией или другими средствами, препятствующими неконтролируемому проникновению посторонних лиц в указанные помещения.

12.4. Запрещается прием посетителей в помещениях, в которых в этот момент осуществляется обработка информации конфиденциального характера, за исключением случаев, когда это связано с непосредственным выполнением должностных обязанностей. При этом необходимо обеспечить соблюдение мер по недопущению ознакомления с информацией конфиденциального характера лиц, не имеющих прав на ознакомление с ней.

12.5. Для хранения документов и машинных носителей с информацией конфиденциального характера структурные подразделения АО «Кузбасс-пригород» должны быть снабжены сейфами, металлическими шкафами, шкафами или ящиками, оборудованными замками.

Также структурные подразделения АО «Кузбасс-пригород» должны быть обеспечены средствами уничтожения документов.

12.6. Места доступа, через которые неавторизованные лица могут попасть в помещения АО «Кузбасс-пригород», должны контролироваться и по возможности должны быть изолированы от средств обработки информации с целью предотвращения несанкционированного доступа. При невозможности такого размещения должны быть приняты меры к тому, чтобы оборудование не оставалось без контроля со стороны персонала, имеющего доступ к этому оборудованию.

12.7. При организации работы оборудования вне контролируемых зон, а также при транспортировке носителей информации за пределами территорий АО «Кузбасс-пригород» должны предприниматься меры для предотвращения несанкционированного доступа, повреждения или утери оборудования и носителей информации.

12.8. Все вспомогательные инженерные системы (электропитание, вентиляция и кондиционирование воздуха и др.) должны обеспечивать гарантированную и устойчивую работоспособность компонентов ИИ АО «Кузбасс-пригород».

12.9. В помещениях, в которых размещены технические средства ИИ АО «Кузбасс-пригород», должны быть предусмотрены меры защиты от пожара, затопления и других разрушающих природных и техногенных воздействий.

12.10. Необходимо на регулярной основе осуществлять контроль защищенности служебных кабинетов и помещений постоянного и временного пребывания должностных лиц АО «Кузбасс-пригород» от утечки информации по техническим каналам.

13. Обеспечение безопасности информационной инфраструктуры АО «Кузбасс-пригород» и ее компонентов

13.1. Общие положения обеспечения безопасности информационной инфраструктуры АО «Кузбасс-пригород» и ее компонентов

13.1.1. В ИИ АО «Кузбасс-пригород» должны быть реализованы меры защиты информации на следующих уровнях:

- защита периметра компонентов ИИ АО «Кузбасс-пригород»;
- защита ИТКС, контуров безопасности информации и сегментов ИИ АО «Кузбасс-пригород»;
- защита компонентов ИИ АО «Кузбасс-пригород», в том числе АРМ, мобильных технических средств;
- защита сегментов ИС и (или) ИТКС АО «Кузбасс-пригород».

13.1.2. Защита периметра компонентов ИИ АО «Кузбасс-пригород» должна предусматривать реализацию мер защиты информации, обеспечивающих взаимодействие компонентов ИИ АО «Кузбасс-пригород» с иными системами и сетями связи только через интерфейсы, для которых:

- межсетевыми экранами обеспечивается управление входящими и исходящими информационными потоками и сокрытие топологии сетей;
- средствами криптографической защиты информации обеспечивается защита информации при ее передаче по сетям связи общего пользования, в том числе по сети «Интернет»;

системами обнаружения вторжений обеспечивается обнаружение компьютерных атак;

реализуются другие меры защиты информации, обеспечивающие защиту от актуальных УБИ.

13.1.3. Защита ИТКС, контуров безопасности информации и сегментов ИИ АО «Кузбасс-пригород» должна предусматривать реализацию следующих мер защиты информации:

выделение отдельных уровней контуров безопасности информации, сегментов ИИ АО «Кузбасс-пригород», на базе которых функционируют ИС ОАО «РЖД», на основе классов (уровней) защищенности информации указанных ИС;

управление сетевыми потоками между созданными контурами и сегментами с помощью межсетевых экранов;

ограничение доступа к информации, передаваемой по каналам связи, не выходящим за пределы контролируемой зоны, с помощью механизмов виртуальных сетей, в том числе сегментация на разные виртуальные сети баз

данных ИС АО «Кузбасс-пригород» и технических (программных) средств приема и обработки запросов к этим базам данных;

использование средств криптографической защиты информации при передаче информации конфиденциального характера по сетям связи общего пользования, в том числе по сети «Интернет»;

обнаружение компьютерных атак из сетей, используемых для организации сетевого взаимодействия между сегментами.

13.1.4. Защита компонентов ИИ АО «Кузбасс-пригород», в том числе АРМ, мобильных технических средств должна предусматривать реализацию следующих мер защиты информации:

определение перечня АРМ и иных компонентов ИИ АО «Кузбасс-пригород», на которых происходит обработка информации конфиденциального характера; определение класса (уровня) защищенности информации;

создание подсистемы защиты информации на основе сегментного подхода (обеспечение ИБ типовых АРМ);

проведение оценки соответствия (аттестации) требованиям по безопасности информации.

13.1.5. Подключение к ИТКС АО «Кузбасс-пригород» должно производиться в установленном в АО «Кузбасс-пригород» порядке. Запрещается несанкционированное подключение к ИТКС АРМ, сетевого и любого другого оборудования.

Запрещается открытие и поддержка в ИТКС АО «Кузбасс-пригород» незарегистрированных, индивидуальных общедоступных ресурсов.

13.1.6. АРМ АО «Кузбасс-пригород» могут взаимодействовать с сетью «Интернет» в установленном в АО «Кузбасс-пригород» порядке.

13.1.7. В качестве мобильных технических средств в АО «Кузбасс-пригород» могут использоваться портативные вычислительные устройства и устройства связи с возможностью обработки информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и т.д.). Приобретение мобильных технических средств, возможность и порядок их использования в качестве АРМ и подключения к сети «Интернет» должны осуществляться в установленном в АО «Кузбасс-пригород» порядке.

13.1.8. Защита сегментов ИС АО «Кузбасс-пригород» должна предусматривать реализацию мер защиты информации, направленных на идентификацию и аутентификацию субъектов доступа, управление сеансами доступа, регистрацию событий безопасности, контроль доступа к сегментам ИС из внешних систем с помощью сертифицированных межсетевых экранов уровня веб-сервера (тип «Г»)⁶.

⁶ Требования к межсетевым экранам, утвержденные приказом ФСТЭК России от 9 февраля 2016 г. № 9.

13.1.9. При реализации мер защиты информации необходимо, по возможности, использовать имеющиеся в АО «Кузбасс-пригород» средства защиты информации.

При применении средств криптографической защиты информации должен быть организован их поэкземплярный учет в соответствии с требованиями законодательства Российской Федерации и эксплуатационной документации на применяемые средства.

В случае необходимости применения дополнительных средств защиты информации требуется предоставить соответствующее обоснование. Взаимодействие сетей общетехнологического, оперативно-технологического или иного назначения должно осуществляться только через специализированные узлы межсетевого взаимодействия.

Запрещается взаимодействие сетей оперативно-технологического назначения с сетями связи общего пользования и сетью «Интернет».

13.2. Организация сетей беспроводного доступа

13.2.1. Организация беспроводного доступа для предоставления гостевого доступа к ресурсам сети «Интернет» ограниченному количеству работников АО «Кузбасс-пригород», проведения демонстрационных показов, презентаций и иной общественной деятельности должна быть реализована в виде обособленной сети, физически отделенной от ИТКС АО «Кузбасс-пригород».

13.2.2. Запрещена передача информации конфиденциального характера по беспроводным каналам без применения соответствующих мер защиты информации, даже в пределах контролируемой зоны. При необходимости использования беспроводной сети такая сеть подлежит защите в соответствии с проектными решениями по созданию ее подсистемы защиты с проведением оценки соответствия требованиям по безопасности информации.

13.2.3. Защита информации, передаваемой по радиоканалам, должна осуществляться в соответствии с нормативными документами ОАО «РЖД» и АО «Кузбасс-пригород» по обеспечению ИБ беспроводного радиодоступа.

13.3. Управление доступом. Идентификация и аутентификация субъектов и объектов доступа

13.3.1. Управление доступом к информации и функциям ее обработки должно осуществляться в целях обеспечения и контроля доступа авторизованных субъектов доступа (пользователей и процессов и (или) устройств) к объектам доступа (ИС АО «Кузбасс-пригород», информационным ресурсам, операционным системам, системам управления

базами данных и др.), а также предотвращения доступа к ним неавторизованных субъектов доступа.

13.3.2. Разграничение доступа субъектов доступа к объектам доступа должно осуществляться средствами разграничения доступа сертифицированного ПО (в том числе операционных систем, а также средств защиты информации).

13.3.3. В ИИ АО «Кузбасс-пригород» должна быть предусмотрена реализация, как минимум, дискреционного и ролевого методов управления доступом.

Дискреционный метод управления доступом применяется для управления доступом субъектов доступа (пользователей и (или) групп пользователей) к объектам доступа, содержащим целевую информацию (например, объекты файловой системы, объекты баз данных, другие объекты системного и прикладного ПО).

Ролевой метод управления доступом применяется для управления доступом к механизмам управления компонентами ИС и их подсистемами защиты информации (средствами защиты информации в составе ПО).

13.3.4. При доступе к ИС АО «Кузбасс-пригород» должна осуществляться идентификация и аутентификация внутренних пользователей (работников АО «Кузбасс-пригород», или иных лиц, привлекаемых на договорной основе) и внешних пользователей (не являющихся работниками АО «Кузбасс-пригород»).

13.3.5. При назначении прав (привилегий, полномочий) идентификаторам (учетным записям) пользователей должен назначаться только тот минимальный набор прав (привилегий, полномочий), который необходим для выполнения ими своих должностных обязанностей (функций). Минимальные права (привилегии, полномочия) для идентификаторов (учетных записей) должны определяться ролевой моделью и ОРД по защите информации ИС.

13.3.6. Допуск пользователей к работе с информационными ресурсами АО «Кузбасс-пригород» должен быть регламентирован.

13.3.7. Для обеспечения возможности идентификации пользователей каждому пользователю информационных ресурсов АО «Кузбасс-пригород» должен присваиваться уникальный идентификатор (имя пользователя, логин), который позволяет однозначно идентифицировать пользователя.

13.3.8. Предоставление доступа к информационным ресурсам АО «Кузбасс-пригород» должно осуществляться только при успешном прохождении процедуры аутентификации (подтверждения заявленной личности) пользователя.

Аутентификация пользователей может осуществляться с использованием паролей или, в случае многофакторной (двухфакторной) аутентификации, комбинации паролей, аппаратных средств, средств электронной подписи, иных средств.

13.3.9. В случае производственной необходимости отдельным работникам АО «Кузбасс-пригород» (например, работникам, выполняющим функции администрирования компонентов ИИ АО «Кузбасс-пригород») могут быть созданы несколько уникальных идентификаторов (учетных записей) к одному и тому же ресурсу АО «Кузбасс-пригород» (например, с разными правами доступа для выполнения административных задач).

13.3.10. Временный идентификатор (учетная запись) может быть заведен для пользователя на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для проведения настройки, тестирования ПО, для организации гостевого доступа (посетителям, работникам сторонних организаций, стажерам и иным пользователям с временным доступом) и т.п.

13.3.11. В общем случае запрещено создавать и использовать общий (служебный) идентификатор (учетную запись) для группы пользователей. В случаях, когда это необходимо, ввиду особенностей бизнес-процесса или организации труда (например, посменное дежурство), должен вестись учет использования общего (служебного) идентификатора (учетной записи), который должен однозначно идентифицировать текущего владельца идентификатора (учетной записи) в каждый момент времени. Одновременное использование одного общего (служебного) идентификатора (учетной записи) разными пользователями запрещено.

При организации доступа к информационным ресурсам в классах обучения для каждого АРМ в классе должен использоваться отдельный общий (служебный) идентификатор (учетная запись).

13.3.12. Сервисные (технические) идентификаторы (учетные записи) должны быть персонифицированы для однозначной идентификации ответственного за данную учетную запись работника АО «Кузбасс-пригород».

13.3.13. С целью реализации правил управления доступом и для обеспечения возможности идентификации объектов и устройств объектам доступа и подключаемым устройствам также должны присваиваться идентификаторы (имена объектов доступа, имена или условные номера устройств). Для обеспечения возможности однозначной идентификации объектов доступа и устройств присваиваемые им идентификаторы (учетные записи) должны быть уникальными.

В ОРД по защите информации могут быть установлены порядок и правила аутентификации объектов доступа и (или) устройств.

13.3.14. Перед началом эксплуатации ПО должно быть обеспечено изменение аутентификационной информации (средств аутентификации), заданных производителями и (или) использованных внешними организациями при внедрении, настройке, модернизации.

13.3.15. Пользователи должны регулярно менять свою аутентификационную информацию. Периодичность смены паролей должна определяться в ОРД по защите информации. Передача пользователем своих средств аутентификации иным лицам запрещена.

13.3.16. Должен осуществляться на регулярной основе контроль функционирования средств идентификации и аутентификации. Периодичность контроля должна устанавливаться в ОРД по защите информации.

13.3.17. Процедуры регистрации и блокирования учетных записей пользователей должны применяться с соблюдением следующих правил:

использование уникальных идентификаторов (учетных записей) пользователей для однозначного определения и сопоставления личности с совершенными ею действиями;

использование общих (служебных) идентификаторов (учетных записей) только в случае, если это необходимо для выполнения задачи;

предоставление и блокирование прав должны быть санкционированы и документированы;

предоставление прав доступа к информационным ресурсам АО «Кузбасс-пригород» должно быть согласовано с владельцами данных ресурсов;

уровень предоставленных полномочий должен соответствовать производственной необходимости и не ставить под угрозу разграничение режимов работы;

назначенные пользователю права доступа должны быть документально зафиксированы;

доступ должен быть предоставлен с момента завершения процедуры регистрации;

должно быть обеспечено создание и поддержание формального списка всех субъектов доступа, зарегистрированных для работы с информационным ресурсом АО «Кузбасс-пригород»;

права доступа пользователей, сменивших должность, форму занятости или уволившихся из АО «Кузбасс-пригород», а также ушедших в отпуск по уходу за ребенком или в длительную командировку сроком более 6 месяцев, должны быть заблокированы в течение суток и при необходимости удалены в срок, не превышающий 3 месяца;

должен выполняться автоматический аудит учетных записей пользователей на наличие неиспользуемых, их блокировка;

учетные записи, используемые поставщиками для удаленной поддержки, должны включаться только на время выполнения работ;

должны отслеживаться удаленные учетные записи, используемые поставщиками во время выполнения работ;

повторное использование идентификатора (учетной записи) пользователя и (или) устройства должно быть запрещено в течение не менее чем трех лет;

учетная запись должна блокироваться на определенный период или до ее разблокировки администратором при установленном количестве неуспешных попыток ввода пароля;

учетные записи пользователей должны блокироваться при выявлении по результатам мониторинга (просмотра, анализа) журналов регистрации событий безопасности действий пользователей, которые отнесены к событиям нарушения ИБ.

13.3.18. Доступ работника к информационным ресурсам АО «Кузбасс-пригород» должен быть санкционирован работником, которому приказом по Обществу делегированы соответствующие полномочия), в котором числится, согласно штатному расписанию, данный работник, и владельцами соответствующих информационных ресурсов.

13.3.19. Должен осуществляться на регулярной основе пересмотр прав доступа пользователей к информационным ресурсам АО «Кузбасс-пригород».

13.3.20. Для предотвращения попыток подбора паролей пользователей должны быть настроены ограничения на количество неуспешных попыток входа в ИС АО «Кузбасс-пригород», после которого осуществляется блокировка учетной записи. Допустимое количество неуспешных попыток и время блокировки учетной записи должны быть определены в ОРД по защите информации на ИС.

13.3.21. В ИС АО «Кузбасс-пригород» должно быть настроено ограничение на максимально возможное количество сеансов доступа пользователей, при достижении которого механизмами управления доступом должно осуществляться блокирование новых или ранее открытых сеансов доступа.

13.3.22. В случае если работник покидает свое рабочее место, он обязан заблокировать доступ к эксплуатируемому им АРМ (заблокировать пользовательский сеанс в операционной системе), либо выключить его. Исключением являются ситуации, связанные с угрозой жизни и (или) здоровью работника, при которых рабочее место должно быть покинуто безотлагательно.

13.3.23. Организация информационного взаимодействия ИС АО «Кузбасс-пригород» с системами внешних организаций (внешними системами) допускается только на основании заключенных договоров (соглашений) с операторами (обладателями, владельцами) внешних систем в соответствии с

требованиями нормативных документов АО «Кузбасс-пригород» по предоставлению доступа к ИС АО «Кузбасс-пригород».

13.3.24. В случае необходимости передачи во внешнюю систему информации конфиденциального характера по отношению к такой системе АО «Кузбасс-пригород» должны быть предъявлены требования по обеспечению безопасности передаваемой информации и получено подтверждение выполнения предъявленных требований.

13.3.25. Порядок предоставления работникам АО «Кузбасс-пригород» удаленного доступа (то есть доступа для выполнения своих трудовых обязанностей вне места нахождения работодателя, с использованием ИТКС, в том числе сетей связи общего пользования и сети «Интернет») к информационным ресурсам АО «Кузбасс-пригород» должен быть регламентирован.

13.4. Управление паролями

13.4.1. Идентификатор и пароль пользователя являются учетными данными, на основании которых работнику АО «Кузбасс-пригород» предоставляются права доступа и протоколируются производимые им в системе действия.

13.4.2. Пароли пользователей должны формироваться и использоваться с учетом следующих требований:

пароли должны содержать не менее 14 символов для администраторов и 12 символов для остальных пользователей;

пароли должны быть уникальными для каждой системы и случайными;

пароли не должны являться именами собственными, не должны содержать информацию личного характера (например: имя, фамилию, дату рождения, месяц, логин, название организации в любых словоформах), а также основываться на словах естественного языка;

пароль не должен содержать более двух следующих друг за другом одинаковых символов, наборы повторяющихся символов;

запрещено использовать пустые пароли;

пароль в обязательном порядке должен содержать символы из следующих подмножеств:

буквы в верхнем регистре (A – Z);

буквы в нижнем регистре (a – z);

цифры (0 – 9);

специальные символы и знаки препинания (~ + \$ & # @ % и т.п.);

первичный пароль при создании пользователя должен генерироваться автоматически на основе псевдослучайных последовательностей;

пароли должны регулярно меняться. Срок действия паролей пользователей не должен превышать 90 дней;

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

пароли не должны использоваться для процессов автоматического входа в систему, за исключением паролей сервисных (технических) учетных записей;

должно быть обеспечено хранение паролей с использованием хеш-сумм, сформированных с помощью криптографических хэш-функций;

должно быть запрещено хранение паролей пользователей в атрибутах их учетных записей.

13.4.3. Должна быть предусмотрена защита парольной информации в процессе ее ввода от возможного использования лицами, не имеющими на это полномочий (например, вводимые символы пароля могут отображаться условными знаками «*»).

13.4.4. Хранение парольной информации в электронном виде должно осуществляться в форме значений хеш-функций, рассчитываемых, преимущественно, с использованием российских криптоалгоритмов.

13.4.5. Работник АО «Кузбасс-пригород» обязан обеспечивать конфиденциальность парольной информации. С этой целью работнику запрещается:

сообщать свой пароль кому-либо;

указывать пароль в сообщениях электронной почты;

хранить пароли, записанные на бумаге, в легкодоступном месте;

использовать один и тот же пароль для доступа к различным информационным ресурсам АО «Кузбасс-пригород».

13.4.6. В отдельных ситуациях (отпуск, командировка, болезнь и т.п.) допускается использование паролей отсутствующих работников. Пароли для доступа к информационным ресурсам АО «Кузбасс-пригород», записанные на бумажном носителе, должны храниться в запечатанном конверте в закрывающемся на ключ шкафу (сейфе) уполномоченного работника АО «Кузбасс-пригород». Порядок хранения и выдачи паролей, а также ответственный за вскрытие конверта с паролем, использование и обеспечение конфиденциальности пароля должен определяться руководителем АО «Кузбасс-пригород». Плотность бумаги конверта должна исключать прочтение текста вложения, помещенного в конверт, без вскрытия конверта.

По возвращению к месту работы работник обязан незамедлительно произвести внеплановую смену пароля, поместить новый пароль в конверт и сдать его на хранение.

13.5. Использование программного обеспечения

13.5.1. Используемое в АО «Кузбасс-пригород» ПО, в том числе в составе программно-аппаратных комплексов, должно быть включено в Единый реестр российских программ для электронных вычислительных машин и баз данных или в Единый реестр программ для электронных вычислительных машин и баз данных из государств – членов Евразийского экономического союза, за исключением Российской Федерации.

При отсутствии необходимого ПО в указанных Единых реестрах возможность использования такого ПО, его приобретения должны осуществляться в установленном порядке.

13.5.2. Используемое лицензионное ПО должно быть включено в перечень разрешенного к использованию в ОАО «РЖД».

13.5.3. Для удаления, изменения, дополнения, обновления программной конфигурации на рабочих местах пользователей должны привлекаться соответствующие специалисты. Самостоятельно вносить изменения в конфигурацию аппаратно-программных средств рабочих мест или устанавливать дополнительное ПО запрещено.

13.5.4. Для выполнения своих служебных обязанностей каждый работник АО «Кузбасс-пригород» обеспечивается доступом к соответствующим информационным ресурсам.

13.5.5. Доступ к сети «Интернет» предоставляется работникам АО «Кузбасс-пригород» в целях выполнения ими своих служебных обязанностей, требующих непосредственного подключения к внешним информационным ресурсам.

АО «Кузбасс-пригород» вправе блокировать или ограничивать доступ пользователей к Интернет-ресурсам, содержание которых не имеет отношения к исполнению служебных обязанностей, а также к ресурсам, содержание и направленность которых запрещены законодательством Российской Федерации.

13.5.6. Контроль за установкой и конфигурированием ПО, проверка ПО на уязвимости должны быть реализованы в установленном порядке в соответствии с методическими документами ФСТЭК России⁷.

13.5.7. Запрещается использовать иностранное ПО на значимых объектах критической информационной инфраструктуры АО «Кузбасс-пригород».

ПО, предназначенное для обеспечения безопасности значимых объектов критической информационной инфраструктуры АО «Кузбасс-пригород», а

⁷ Методика тестирования обновлений безопасности программных, программно-аппаратных средств, утвержденная ФСТЭК России 28 октября 2022 г., Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств, утвержденная ФСТЭК России 28 октября 2022 г., Руководство по организации процесса управления уязвимостями в органе (организации), утвержденное ФСТЭК России 17 мая 2023 г.

также ПО, предназначенное для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на инциденты ИБ и (или) обмена информацией об инцидентах ИБ на объектах критической информационной инфраструктуры АО «Кузбасс-пригород», должно соответствовать требованиям законодательства Российской Федерации, в том числе требованиям, установленным ФСТЭК России и (или) ФСБ России в пределах их полномочий, что должно быть подтверждено соответствующим документом (сертификатом).

13.5.8. Не допускается эксплуатация ПО, в котором присутствуют известные уязвимости высокого и критического уровня опасности⁸.

Не допускается обработка информации конфиденциального характера с помощью ПО, в котором присутствуют известные уязвимости среднего и более высокого уровня опасности.

13.5.9. Применяемые в ИИ АО «Кузбасс-пригород» средства защиты информации, в том числе криптографические, должны пройти оценку соответствия требованиям по безопасности информации.

13.5.10. Запрещается использовать программные средства исследования (сканирования) компонентов ИИ АО «Кузбасс-пригород» и нападения на них, перехвата, искажения и уничтожения информации, другие программные продукты, имеющие свойства и функциональные возможности нанесения ущерба компонентам ИИ.

13.5.11. Запрещается использовать программные средства, применение которых требует открытия дополнительных общедоступных портов доступа, ресурсов, применения дополнительных открытых протоколов обмена информацией, и другие программные продукты, снижающие защищенность компонентов ИИ АО «Кузбасс-пригород», если иное не определено отдельным нормативным документом АО «Кузбасс-пригород» или проектным решением.

13.6. Защита машинных носителей информации

13.6.1. Доступ к МНИ предоставляется только тем лицам, которым он необходим для выполнения своих должностных обязанностей.

13.6.2. Перед использованием МНИ необходимо провести их проверку средствами антивирусной защиты.

13.6.3. Все МНИ, используемые в АО «Кузбасс-пригород» для обработки информации конфиденциального характера (съёмные МНИ; портативные вычислительные устройства со встроенными МНИ; МНИ, встроенные в корпус

⁸ В соответствии с пунктом 5.2.18 ГОСТ Р 56545-2015 Защита информации. Уязвимости ИС. Правила описания уязвимостей.

вычислительной техники и т.д.), подлежат учету, включающему присвоение им регистрационных (учетных) номеров.

13.6.4. Все используемые для работы в ИС АО «Кузбасс-пригород» съемные МНИ должны быть зарегистрированы в установленном порядке. Использование личных съемных МНИ должно быть исключено.

13.6.5. Хранение съемных МНИ, используемых для обработки информации конфиденциального характера, должно осуществляться в сейфах (металлических шкафах) либо помещаться в запираемые ящики столов, шкафы.

В случае если на съемном МНИ хранятся только персональные данные в зашифрованном с использованием средств криптографической защиты информации, виде, допускается хранение таких МНИ вне запираемых ящиков столов, шкафов (сейфов).

13.6.6. При необходимости отправки МНИ в ремонт или вывода из эксплуатации, в том числе для передачи в другое структурное подразделение АО «Кузбасс-пригород», хранящаяся на нем информация конфиденциального характера должна быть уничтожена в установленном порядке. Уничтожение информации на МНИ должно исключать возможность восстановления защищаемой информации.

Если уничтожение информации на МНИ невозможно, то такие МНИ должны быть уничтожены.

Уничтожение МНИ должно производиться путем механического нарушения целостности, не позволяющего произвести считывание или восстановление информации (надлом, физическое деформирование и т.п.).

Также должны быть обеспечены регистрация и контроль действий по уничтожению защищаемой информации и уничтожению МНИ.

13.7. Антивирусная защита

13.7.1. В АО «Кузбасс-пригород» должны применяться централизованные средства антивирусной защиты.

Средства антивирусной защиты должны быть установлены, настроены и функционировать на всех допускающих такую установку программно-технических средствах обработки информации до начала использования этих средств в ИИ АО «Кузбасс-пригород».

Для программно-технических средств обработки информации, для которых отсутствует техническая возможность установки средств антивирусной защиты, должны разрабатываться компенсирующие меры, направленные на защиту от вредоносного ПО (например, предусматривающие использование средств антивирусной защиты, установленных на других программно-технических средствах по вычислительной сети).

13.7.2. Необходимость установки средств антивирусной защиты на сетевом оборудовании (коммутационное оборудование, межсетевые экраны и пр.) и для отдельных технологий (веб-сервер, почтовый сервер и пр.) в зависимости от предъявляемых требований по безопасности информации должна определяться в техническом проекте на подсистему защиты информации.

13.7.3. Должно быть обеспечено проведение на регулярной основе проверки всех программно-технических средств на наличие вредоносного ПО (в том числе вирусов).

13.7.4. Должна осуществляться антивирусная проверка всех поступающих на АРМ пользователей и отправляемых с него файлов вне зависимости от того, каким образом они поступили или каким образом они отправляются (в том числе через съемные МНИ). Пользователям должно быть запрещено отключать проверку съемных МНИ.

13.7.5. Пользователям запрещается отключать установленные на программно-технических средствах обработки информации средства антивирусной защиты. Допускается отключение администраторами средств антивирусной защиты только для регламентных или восстановительных работ, при этом на время таких работ должны быть реализованы компенсирующие меры.

13.7.6. Средства антивирусной защиты должны иметь все последние обновления, полученные из доверенных источников. Обновления должны устанавливаться с заданной периодичностью.

13.7.7. К использованию в ИИ АО «Кузбасс-пригород» должны допускаться только лицензионные сертифицированные на соответствие требованиям по безопасности информации средства антивирусной защиты.

13.8. Обеспечение целостности и доступности

13.8.1. Реализация мер по контролю целостности позволяет своевременно обнаруживать несанкционированную модификацию компонентов ИИ АО «Кузбасс-пригород», обеспечить правильность функционирования средств защиты информации и целостность обрабатываемой информации.

Для обеспечения контроля целостности должно быть предусмотрено:

применение функций контроля целостности средств защиты информации. В определенных случаях по согласованию с уполномоченным сотрудником АО «Кузбасс-пригород» допускается использование встроенных механизмов контроля целостности используемых в ИС АО «Кузбасс-пригород» операционных систем, а также прикладного ПО;

отсутствие в ИИ АО «Кузбасс-пригород» средств разработки и тестирования (отладки) либо выделение их в отдельный сегмент. Доступ из этого сегмента к защищаемой в ИИ АО «Кузбасс-пригород» информации должен быть запрещен или (при необходимости) ограничен с помощью однонаправленных шлюзов (или аналогичных устройств), а также строго контролироваться;

ведение не менее двух копий программных средств (например, дистрибутивов, лицензионных ключей, параметров настройки) для обеспечения возможности восстановления работоспособности этих средств в случае нарушения их функционирования;

применение средств защиты информации, блокирующих несанкционированные модификацию или удаление защищаемых ресурсов;

применение средств сравнения для контроля соответствия ПО (защищаемых ресурсов) с их эталонными копиями и восстановление в случае нарушения целостности;

применение средств подсчета и сравнения контрольных сумм;

применение средств электронной подписи;

ведение протоколирования в системных журналах, синхронизация по дате и времени.

13.8.2. В ИИ АО «Кузбасс-пригород» должно быть обеспечено хранение информации с необходимым резервированием (с использованием программно-аппаратных способов доступности данных) путем создания:

13.8.2.1. набора независимых серверов (узлов), работающих совместно для повышения доступности служб и приложений – кластеров. Существует несколько типов кластеров, из которых можно выделить следующие:

кластер высокой доступности;

кластер распределения (балансировки) нагрузки;

вычислительный кластер;

13.8.2.2. систем резервного копирования (предназначенных для автоматизированного выполнения операций резервного копирования и восстановления данных в случае сбоя), включая:

создание удаленных синхронных копий (синхронная репликация);

создание резервных копий по расписанию (полным, инкрементальным, дифференциальным или иным методом, обеспечивающим создание резервной копии);

13.8.2.3. серверов «горячего» резерва.

13.8.3. В рамках обеспечения доступности корпоративных сервисов (доменов, служб каталогов, почтовых систем, систем хранения файлов и т.п.) должна быть обеспечена их доступность в режиме 24x7, быстрое восстановление в случае аппаратного либо программного сбоя без потери данных.

13.8.4. При необходимости, по согласованию с уполномоченным сотрудником АО «Кузбасс-пригород», для функционирования ИС АО «Кузбасс-пригород» возможно использование ЦОД сторонних организаций.

13.9. Обеспечение работоспособности информационной инфраструктуры АО «Кузбасс-пригород» в нештатных ситуациях

13.9.1. При обеспечении работоспособности значимых объектов критической информационной инфраструктуры АО «Кузбасс-пригород» в нештатных ситуациях необходимо руководствоваться Требованиями к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, утвержденными приказом ФСТЭК России от 21 декабря 2017 г. № 235, и Требованиями по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденными приказом ФСТЭК России от 25 декабря 2017 г. № 239.

13.9.2. С целью подготовки персонала к действиям по оперативному восстановлению компонент ИИ АО «Кузбасс-пригород» в случаях возникновения нештатных ситуаций должны быть определены:

перечень возможных видов нештатных ситуаций;

лица, ответственные за организацию и координацию действий в нештатных ситуациях;

основные задачи, решаемые в случае возникновения нештатных ситуаций, и соответствующие требования к действиям, осуществляемым при решении этих задач, планы действий при возникновении инцидентов ИБ и иных нештатных ситуаций.

13.9.3. Управление инцидентами ИБ должно быть реализовано в установленном порядке.

О происшедших инцидентах (событиях), относящихся к ИБ, должны быть оперативно оповещены подразделения ОАО «РЖД», отвечающие за вопросы ИБ. Указанную информацию можно также сообщить на «горячую линию» для работников ОАО «РЖД» по вопросам ИБ.

13.9.4. Процедуры (регламенты) выявления и реагирования на инциденты ИБ должны включать:

регистрацию инцидента ИБ, включая сбор и накопление доказательной базы, в том числе документированной информации, используемой при расследовании инцидента ИБ, а также направление (при необходимости) информации об инциденте ИБ в Национальный координационный центр по компьютерным инцидентам в порядке, предусмотренном Порядком информирования ФСБ России о компьютерных инцидентах, реагирования

на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденном приказом ФСБ России от 19 июня 2019 г. № 282;

сдерживание инцидента ИБ, включая локализацию мест (сегментов сети, отдельных серверов и др.) возникновения инцидента ИБ;

устранение инцидента ИБ;

выявление последствий инцидента ИБ;

устранение последствий инцидента ИБ;

принятие мер по предотвращению повторного возникновения инцидента ИБ, включая анализ каждого инцидента, выявление и устранение его причин, отслеживание и прогнозирование появления новых уязвимых мест в ИИ АО «Кузбасс-пригород», а также новых УБИ.

13.9.5. Для повышения эффективности и снижения затрат на выявление и реагирование на инциденты ИБ может быть создан собственный ситуационный центр по ИБ.

14. Аудит информационной безопасности

14.1. Аудит ИБ должен включать в себя:

проведение инвентаризации информационных ресурсов АО «Кузбасс-пригород»;

оценку текущего уровня защищенности информационных ресурсов АО «Кузбасс-пригород»;

выявление и локализацию уязвимостей информационных ресурсов АО «Кузбасс-пригород»;

анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении информационных ресурсов АО «Кузбасс-пригород»;

выработку рекомендаций по совершенствованию СУИБ за счет внедрения новых и повышения эффективности существующих мер защиты информации.

14.2. Аудит может быть внутренним (проводимым АО «Кузбасс-пригород» своими силами или с привлечением на договорной основе сторонней организации) или внешним (проводимым внешними независимыми аудиторскими организациями).

14.3. При проведении инвентаризации информационных ресурсов АО «Кузбасс-пригород» должны осуществляться:

мониторинг ИИ АО «Кузбасс-пригород» в целях получения актуальной информации о составе технических средств, ПО и средств защиты информации;

контроль соответствия состава программно-технических средств, ПО и средств защиты информации сведениям, приведенным в эксплуатационной

документации, и принятие мер, направленных на устранение выявленных недостатков;

контроль сроков действия сертификатов соответствия на средства защиты информации, соответствия условий эксплуатации средств защиты информации требованиям эксплуатационной документации, и принятие мер, направленных на устранение выявленных недостатков.

14.4. Должны осуществляться выявление (поиск), анализ и устранение уязвимостей, проверка правильности установки и настройки средств защиты информации, программно-технических средств и ПО, а также корректности работы средств защиты информации при их взаимодействии с программно-техническими средствами и ПО.

Должны быть предусмотрены мероприятия, направленные на устранение возможности использования выявленных уязвимостей (например, установка обновлений, выполнение настроек средств защиты информации, изменение режима обработки информации и порядка использования ИС и (или) ИТКС АО «Кузбасс-пригород», и т.п.).

14.5. Должны быть определены события ИБ, подлежащие регистрации, состав и содержание информации о событиях ИБ, включаемой в записи регистрации о событиях ИБ, и сроки их хранения. Перечень событий ИБ, подлежащих регистрации, должен пересматриваться не реже, чем один раз в год, а также по результатам контроля (мониторинга) за выполнением требований по безопасности информации.

14.6. При проведении мероприятий по обеспечению безопасности информации в ИС и (или) ИТКС АО «Кузбасс-пригород» должны предусматриваться работы по их интеграции с централизованно применяемыми в ОАО «РЖД» системами мониторинга и управления ИБ.

14.7. Аудит ИБ должен предусматривать автоматический непрерывный мониторинг событий ИБ, а также проведение администраторами (в рамках деятельности по текущему администрированию) просмотра и анализа результатов такого мониторинга, выявления инцидентов ИБ и реагирования на них.

Мониторинг должен проводиться для всех событий, подлежащих регистрации.

Мониторинг событий ИБ с целью выявления инцидентов ИБ должен осуществляться с использованием централизованно применяемых в ОАО «РЖД» и АО «Кузбасс-пригород» систем мониторинга и управления ИБ.

Все локальные средства мониторинга (в случае применения), которые применяются в отдельных ИС и (или) ИТКС АО «Кузбасс-пригород» или на отдельных объектах размещения программно-технических средств АО

«Кузбасс-пригород», должны быть интегрированы с системами мониторинга и управления ИБ.

15. Обеспечение информационной безопасности интеллектуальной собственности сторонних организаций и физических лиц

15.1. Обеспечение информационной безопасности интеллектуальной собственности сторонних организаций и физических лиц при реализации АО «Кузбасс-пригород» своей деятельности является одним из аспектов обеспечения ИБ. Осуществление такой защиты важно в случае:

использования полученных информационных материалов (в том числе размещения на официальном сайте АО «Кузбасс-пригород»);

проведения конкурсов на выполнение работ в интересах АО «Кузбасс-пригород»;

использования ПО и др.

15.2. Для информации, передаваемой в АО «Кузбасс-пригород», которая может являться объектом интеллектуальной собственности до момента ее регистрации, должны предъявляться требования по ее безопасности, аналогичные требованиям по безопасности информации конфиденциального характера в АО «Кузбасс-пригород».

15.3. При заключении договоров (соглашений) АО «Кузбасс-пригород» со сторонними организациями в договоры (соглашения) должны в обязательном порядке включаться положения по охране интеллектуальной собственности сторон и ответственности сторон за нарушения данных положений.

16. Обеспечение безопасности информации при передаче ее органам государственной власти, правоохранительным органам и сторонним организациям

16.1. Предоставление информации органам государственной власти, правоохранительным органам и сторонним организациям должно выполняться с соблюдением действующего законодательства Российской Федерации.

16.2. Обмен информацией с федеральными органами государственной власти возможен по Единой автоматизированной системе документооборота (ЕАСД) с оформлением документов в адрес соответствующего органа власти посредством системы Межведомственного электронного документооборота (МЭДО).

16.3. При использовании для обмена информацией незащищенных каналов связи, а также сетей связи общего пользования, в том числе сети «Интернет», для обеспечения безопасности передаваемой информации должны

использоваться средства криптографической защиты информации, прошедшие оценку соответствия требованиям по безопасности информации.

При невозможности использования средств криптографической защиты информации необходимо использовать соответствующие организационные и технические меры защиты информации, позволяющие нейтрализовать актуальные УБИ, например, передачу документов на бумажном носителе (почтовым отправлением или курьером).

17. Планирование мероприятий по обеспечению информационной безопасности

17.1. В АО «Кузбасс-пригород» должны разрабатываться планы мероприятий по обеспечению ИБ, в которых должны быть определены:

перечень мероприятий по обеспечению ИБ;

для каждого мероприятия ответственные за его реализацию работники АО «Кузбасс-пригород»;

для каждого мероприятия сроки его реализации и результат.

17.2. Для значимых объектов критической информационной инфраструктуры АО «Кузбасс-пригород» и ИС АО «Кузбасс-пригород», аттестованных по требованиям безопасности информации, планы мероприятий по обеспечению ИБ должны разрабатываться в обязательном порядке, в соответствии с законодательством Российской Федерации в области обеспечения ИБ.

17.3. Ежегодно должны готовиться отчеты о выполнении планов мероприятий по обеспечению ИБ. Каждый пункт плана с истекшим сроком реализации должен быть закрыт отчетным документом о его выполнении, либо ходатайством о переносе срока его реализации, либо ходатайством об исключении данного пункта из плана.

18. Контроль выполнения требований Политики

18.1. Общий контроль состояния ИБ АО «Кузбасс-пригород» осуществляет главный инженер АО «Кузбасс-пригород», ответственный за обеспечение ИБ в АО «Кузбасс-пригород», в том числе за обнаружение, предупреждение и ликвидацию последствий компьютерных атак, и реагирование на компьютерные инциденты.

18.2. Текущий контроль соблюдения Политики осуществляет уполномоченный сотрудник АО «Кузбасс-пригород». Контроль осуществляется путем проведения мониторинга и анализа инцидентов ИБ АО «Кузбасс-пригород», а также в рамках иных контрольных мероприятий.

18.3. Координацию работ по выполнению требований Политики в части реагирования на компьютерные инциденты, обнаружения, предупреждения и ликвидации компьютерных атак на ИИ АО «Кузбасс-пригород» и информационные активы АО «Кузбасс-пригород» осуществляет главный инженер АО «Кузбасс-пригород».

18.4. Ответственность за нарушение Политики возлагается на каждого работника АО «Кузбасс-пригород», допустившего такое нарушение своим действием или бездействием, совершенным в рамках возложенных на него должностных обязанностей.

Содержание

1. Общие положения	1
2. Термины и определения.....	2
3. Сокращения.....	5
4. Цель и задачи обеспечения информационной безопасности АО «Кузбасс-пригород»	6
5. Краткая характеристика информационной инфраструктуры АО «Кузбасс-пригород»	8
6. Основные угрозы безопасности информации информационной инфраструктуры АО «Кузбасс-пригород».....	10
7. Порядок обеспечения информационной безопасности информационной инфраструктуры АО «Кузбасс-пригород».....	11
8. Обеспечение информационной безопасности работниками АО «Кузбасс-пригород»	17
9. Реализация документооборота в АО «Кузбасс-пригород» с учетом требований по безопасности информации.....	17
10. Использование электронных почтовых сервисов.....	18
11. Информирование и обучение персонала	19
12. Физический доступ.....	20
13. Обеспечение безопасности информационной инфраструктуры АО «Кузбасс-пригород» и ее компонентов.....	22
13.1. Общие положения обеспечения безопасности информационной инфраструктуры АО «Кузбасс-пригород» и ее компонентов.....	242
13.2. Организация сетей беспроводного доступа.....	24
13.3. Управление доступом. Идентификация и аутентификация субъектов и объектов доступа.....	24
13.4. Управление паролями	29
13.5. Использование программного обеспечения.....	31
13.6. Защита машинных носителей информации.....	32
13.7. Антивирусная защита	33
13.8. Обеспечение целостности и доступности.....	34
13.9. Обеспечение работоспособности информационной инфраструктуры АО «Кузбасс-пригород» в нештатных ситуациях.....	36
14. Аудит информационной безопасности	37
15. Обеспечение информационной безопасности интеллектуальной собственности сторонних организаций и физических лиц.....	39
16. Обеспечение безопасности информации при передаче ее органам государственной власти, правоохрнительным органам и сторонним организациям.....	39

17. Планирование мероприятий по обеспечению информационной безопасности	40
18. Контроль выполнения требований Политики	40