МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
(РОСЖЕЛДОР)

ПРИКАЗ

_____ **Москва** **№** _____

Об утверждении организационно-распорядительных документов по вопросам защиты информации, необходимых для обеспечения информационной безопасности Федерального агентства железнодорожного транспорта

Во исполнение Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказов ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации (СКЗИ) с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30 августа 2002 г. № 282, методического документа «Меры защиты информации в государственных информационных системах», утвержденного ФСТЭК России 11 февраля 2014 г., в соответствии с п.п. 9.9 Положения о Федеральном агентстве железнодорожного транспорта, утвержденного постановлением Правительства Российской Федерации от 30 июля 2004 г. № 397 **п р и к а з ы в а ю:**

1. Утвердить:

1.1. Концепцию информационной безопасности центрального аппарата Федерального агентства железнодорожного транспорта;

1.2. Политику информационной безопасности локальной вычислительной сети центрального аппарата Федерального агентства железнодорожного транспорта;

1.3. Политику использования сети «Интернет» и электронной почты в информационно-телекоммуникационной сети центрального аппарата Федерального агентства железнодорожного транспорта;

1.4. Регламент реагирования на инциденты информационной безопасности в центральном аппарате Федерального агентства железнодорожного транспорта;

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

1.6. Порядок использования средств криптографической защиты информации в центральном аппарате Федерального агентства железнодорожного транспорта;

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

1.8. Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи в центральном аппарате Федерального агентства железнодорожного транспорта;

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

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

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

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

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

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

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

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

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

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

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

1.20. Инструкция администратора государственных информационных систем центрального аппарата Федерального агентства железнодорожного транспорта;

1.21. Инструкция администратора информационной безопасности государственных информационных систем Федерального агентства железнодорожного транспорта;

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

1.23. Инструкция по порядку учета и хранению машинных носителей конфиденциальной информации (персональных данных) в государственных информационных системах центрального аппарата Федерального агентства железнодорожного транспорта;

1.24. Журнал учета съемных носителей информации в государственных информационных системах центрального аппарата Федерального агентства железнодорожного транспорта;

2. Признать утратившим силу приказ Росжелдора от 16 октября 2017 г. № 395 «Об утверждении Требований и мер по обеспечению безопасного режима эксплуатации средств криптографической защиты информации и назначении администратора безопасности».

3. Признать утратившим силу приказ Росжелдора от 31 октября 2016 г. № 423 «Об утверждении документов, регламентирующих мероприятия по обеспечению информационной безопасности в Федеральном агентстве железнодорожного транспорта».

4. Контроль за исполнением настоящего приказа возложить на заместителя руководителя Росжелдора, курирующего вопросы цифровой трансформации Росжелдора.

Руководитель И.Ю. Коваль

Казаков Андрей Сергеевич, ОИВ
(499) 550-34-36 доб. 1011

УТВЕРЖДЕНО
приказом Росжелдора
от _____ № _____

Концепция информационной безопасности центрального аппарата Федерального агентства железнодорожного транспорта (Росжелдора)

1. Общие положения

Концепция информационной безопасности центрального аппарата Федерального агентства железнодорожного транспорта (далее – Концепция) отражает согласованную систему взглядов на задачи обеспечения информационной безопасности на объектах информатизации Росжелдора и является основополагающим руководящим документом, регулирующим вопросы создания системы обеспечения информационной безопасности и определяющим стратегию ее развития.

Концепция представляет собой систематизированное изложение целей, задач, принципов построения, требований и подходов по обеспечению и управлению информационной безопасностью на объектах информатизации Росжелдора.

Система обеспечения информационной безопасности Росжелдора представляет собой совокупность принципов, требований, подходов и методов к обеспечению информационной безопасности, реализуемых в виде совокупности нормативной, методической, организационно-распорядительной, проектной и иной документации, а также в виде совокупности реализованных правовых, организационных и программно-технических мер по обеспечению информационной безопасности на объектах информатизации Росжелдора.

Положения Концепции распространяются на все объекты информатизации и информационные системы, в отношении которых на Росжелдор возложены обязанности собственника информационных ресурсов или функции оператора.

Положения Концепции не распространяются на вопросы защиты сведений, составляющих государственную тайну.

2. Цели и задачи обеспечения информационной безопасности Росжелдора и основные пути их достижения (решения задач системы защиты)

Основной целью обеспечения информационной безопасности (далее – ИБ) на объектах информатизации Росжелдора является обеспечение надежной защиты субъектов информационных отношений (интересы которых затрагиваются при создании и функционировании объектов информатизации) от возможного нанесения им ощутимого ущерба посредством случайного или преднамеренного несанкционированного вмешательства в процесс обработки циркулирующей в них информации и ее незаконного использования.

Задачами, решаемыми для достижения указанной цели обеспечения ИБ в Росжелдоре, являются:

1) определение принципов и технологий обеспечения ИБ, управления ею, а также способов их реализации;

2) определение подходов к выбору механизмов обеспечения информационной безопасности;

3) прогнозирование, своевременное выявление и устранение угроз ИБ Росжелдора, причин и условий, способствующих нанесению ущерба, нарушению нормального функционирования и развития объектов информатизации Росжелдора на основе применения правовых, организационных и программно-технических мер и средств обеспечения ИБ;

4) создание условий для максимально возможной локализации наносимого ущерба от реализации угроз, а также ослабление негативного влияния последствий нарушения ИБ;

5) минимизация времени восстановления после осуществления угроз, обеспечение наличия всех необходимых средств для ограничения последствий вредоносных воздействий и своевременного возобновления нормальной деятельности объектов информатизации;

6) защита прав Росжелдора, его работников, иных субъектов информационных отношений в случаях неправомерного использования или злоупотребления информационными ресурсами;

7) создание механизмов контроля текущего состояния защищенности информационных систем (далее – ИС) объектов информатизации Росжелдора и совершенствования организационно-технических мер защиты;

8) определение принципов и подходов по совершенствованию организационно-технических мер и механизмов обеспечения ИБ;

9) применение сформулированных выше положений на объектах информатизации Росжелдора.

3. Принципы обеспечения информационной безопасности

Обеспечение ИБ на объектах информатизации Росжелдора должно осуществляться на основе следующих принципов:

1) законность при выборе и реализации мер и средств обеспечения ИБ;

2) неукоснительное соблюдение требований законодательства Российской Федерации, требований государственных регулирующих органов, требований нормативных правовых и технических документов Росжелдора в области обеспечения ИБ;

3) комплексность методов, средств и мероприятий, включая законодательные и нормативно-правовые, организационно-административные, инженерно-технические, программно-аппаратные, направленных на предупреждение, пресечение и ликвидацию последствий угроз ИБ;

4) своевременность мер, направленных на обеспечение ИБ (должны носить упреждающий характер, предполагающий постановку задач по ИБ на основе анализа и прогнозирования угроз, опирающихся на модели угроз и модели нарушителей ИБ, а также разработку эффективных мер предупреждения посягательств на

информационные ресурсы Росжелдора);

5) адекватность противодействия возникающим угрозам (меры и средства обеспечения информационной безопасности должны быть адекватны и соответствовать существующим угрозам ИБ);

6) обоснованность и экономическая целесообразность (должно быть обеспечено соответствие возможных потерь от реализации угроз ИБ стоимости принимаемых мер и используемых средств защиты (по критерию «эффективность – стоимость»), а также сохранение финансовых инвестиций в средства защиты);

7) непрерывность функционирования (деятельность по обеспечению ИБ должна представлять собой непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла информационных ресурсов и систем на протяжении всего времени их функционирования);

8) принцип управляемости (все процессы обеспечения ИБ должны быть управляемыми, т.е. должна существовать возможность мониторинга и измерения процессов и компонентов, возможность своевременного выявления нарушений ИБ и принятия соответствующих мер реагирования на инциденты);

9) принцип преемственности и непрерывности совершенствования (должно обеспечиваться постоянное совершенствование мер и средств защиты на основе преемственности организационных и технических решений, анализа функционирования систем защиты с учетом изменений в методах и средствах получения информации нарушителем);

10) перспективность (реализация механизмов обеспечения ИБ должна осуществляться с учетом общих мировых тенденций и лучшего практического опыта в области обеспечения ИБ);

11) осведомленность (все работники объектов информатизации Росжелдора, а также третьи лица, использующие его информационные ресурсы, должны быть осведомлены о требованиях ИБ и ответственности за их нарушение).

При выборе программно-технических решений по обеспечению ИБ предпочтение отдается решениям, обеспечивающим соблюдение основных принципов ИБ, а также удовлетворяющих следующим критериям:

1) поддержка национальных, международных промышленных стандартов;

2) поддержка наивысшей степени интеграции с существующими программно-аппаратными платформами и используемыми средствами обеспечения безопасности информации;

3) унификация разработчиков и поставщиков используемых продуктов;

4) унификация средств и интерфейсов управления подсистемами ИБ;

5) минимизация стоимости внедрения и эксплуатации;

6) наличие сертификатов соответствия требованиям по безопасности информации.

Принципы обеспечения ИБ обуславливают необходимость применения определенных методов и технологий защиты. Определение способов реализации этих принципов путем применения конкретных программно-технических средств защиты информации и системы организационных мероприятий является предметом актов

Росжелдора, разрабатываемых на основе Концепции.

4. Описание объекта информатизации

4.1. Назначение, цели создания и эксплуатации объектов информатизации

Информационно-техническая поддержка деятельности Росжелдора осуществляется информационными системами объектов информатизации Росжелдора.

К таким объектам относятся объекты внедрения государственных информационных систем (далее – ГИС), в отношении которых Росжелдор выполняет функции оператора.

Целями создания и эксплуатации ИС (объектов информатизации) Росжелдора являются:

1) повышение эффективности деятельности Росжелдора на основе полного и оперативного обеспечения информационных потребностей работников Росжелдора при выполнении ими функциональных задач;

2) исполнение требований законодательства Российской Федерации;

3) повышение эффективности решения задач транспортной безопасности путем создания системы информационного обеспечения решений данных задач.

Создание и применение ИС объектов информатизации Росжелдора позволяет реализовать:

1) повышение качества управления всеми процессами деятельности Росжелдора;

2) повышение качества контроля за движением материальных и финансовых ресурсов Росжелдора;

3) сокращение финансовых и временных затрат на поддержку внутреннего и внешнего документооборота;

4) повышение оперативности и обоснованности планирования расходов Росжелдора;

5) повышение качества информационного обеспечения решения задач обеспечения транспортной безопасности и иных задач Росжелдора.

Основные задачи, решаемые на объектах информатизации Росжелдора, которые необходимо учитывать при обеспечении ИБ:

1) сбор, систематизация, распределение, обработка и отображение в соответствующих формах информации, необходимой для решения задач деятельности Росжелдора;

2) обеспечение подсистемы управления, эксплуатации и технической поддержки функционирования Росжелдора.

4.2. Структура, состав и размещение основных элементов объектов информатизации, информационные связи с другими объектами

На объектах информатизации Росжелдора циркулирует информация разных категорий. В ряде ИС объектов информатизации Росжелдора предусмотрено взаимодействие с внешними (государственными и коммерческими, российскими и зарубежными) организациями по коммутируемым и выделенным каналам с использованием специальных средств передачи информации.

Комплекс технических средств ИС объектов информатизации Росжелдора включает средства обработки данных (автоматизированные рабочие места (далее – АРМ), сервера приложений, сервера БД, почтовые сервера и т.п.), средства обмена данными с возможностью выхода в глобальные сети (кабельная система, мосты, шлюзы и т.д.), а также средства хранения (в т.ч. архивирования) данных.

К основным особенностям функционирования ИС объектов информатизации, являющихся государственными информационными системами Росжелдора, относятся:

1) объединение в единую систему большого количества разнообразных технических средств обработки и передачи информации;

2) разнообразие решаемых задач и категории обрабатываемой информации (данных), сложные режимы автоматизированной обработки информации, связанные с выполнением информационных запросов различных пользователей;

3) объединение в единых базах данных информации различного назначения, принадлежности и категорий;

4) непосредственный доступ к вычислительным и информационным ресурсам большого числа различных категорий пользователей (источников и потребителей информации) и обслуживающего персонала;

5) наличие каналов взаимодействия с внешним миром (источниками и потребителями информации);

6) необходимость непрерывного функционирования.

Технические средства обработки информации ИС объектов информатизации Росжелдора размещаются:

1) в ЛВС Росжелдора;

2) на территории Росжелдора без подключения к ЛВС;

3) в защищенных центрах обработки данных (ЦОД) ГИС;

4) на территории иных объектов информатизации, органов государственной власти, подведомственных Росжелдору организаций и пр.

4.3. Категории информационных ресурсов, подлежащих защите

На объектах информатизации Росжелдора обрабатываются следующие категории информации:

1) открытая информации;

2) информация ограниченного доступа;

3) персональные данные (ПДн);

4) служебная информация ограниченного распространения (служебная тайна, информация «для служебного пользования»).

4.4. Категории пользователей, режимы использования и уровни доступа к информации

В ИС объектов информатизации Росжелдора имеется значительное число категорий пользователей и обслуживающего персонала, которые могут иметь различные полномочия по доступу к ИС объектов информатизации Росжелдора:

1) пользователи (работники подразделений Росжелдора, использующие в своей повседневной деятельности информацию, циркулирующую в ИС Росжелдора, работники иных органов государственной власти – пользователи ГИС, физические лица – пользователи ГИС);

2) ответственные за наполнение баз данных ИС (ввод, корректировка, удаление данных), в том числе юридические и физические лица, являющиеся «поставщиками» информации в ГИС;

3) администраторы ГИС;

4) администраторы (работники сервисных/эксплуатирующих организаций), осуществляющие обслуживание технических средств вычислительной техники;

5) администраторы ИБ (средств защиты информации).

Для каждой категории пользователей и обслуживающего персонала на объектах информатизации Росжелдора должны быть предусмотрены соответствующие режимы доступа и использования информации (по времени, решаемым задачам, порядку ознакомления, модификации данных и т.п.).

Каждой категории пользователей ИС назначаются уровни доступа к информации (на чтение, запись, изменение и т.д.) необходимые и достаточные для выполнения ими их должностных обязанностей.

4.5. Интересы лиц, затрагиваемых при эксплуатации объектов информатизации

При эксплуатации объектов информатизации затрагиваются интересы следующих лиц:

1) Росжелдора, как собственника информационных ресурсов и оператора ИС;

2) органов государственной власти, являющихся пользователями ГИС;

3) подведомственные организации Росжелдора, обеспечивающие эксплуатацию объектов информатизации;

4) работников структурных подразделений Росжелдора, как пользователей ИС Росжелдора в соответствии с их должностными обязанностями;

5) юридических лиц, сведения о которых накапливаются, хранятся и обрабатываются в ИС Росжелдора;

6) юридических лиц, задействованных в процессе создания и эксплуатации объектов информатизации (разработчики, обслуживающий персонал, оказывающий услуги на основании договоров; лица, привлекаемые для оказания услуг в области безопасности информационных технологий и др.).

Перечисленные субъекты информационных отношений заинтересованы

в обеспечении конфиденциальности, целостности и доступности обрабатываемой информации, а также в обеспечении бесперебойного функционирования ИС.

Лица, привлекаемые Росжелдором для проведения работ на объектах информатизации (в т.ч. со средствами защиты информации), осуществляют свою деятельность на основании Государственных контрактов (договоров), неотъемлемой частью которых является регламентация требований по обеспечению безопасности информации.

В требованиях определены задачи и функции привлекаемых лиц на всех стадиях проведения работ и порядок взаимодействия всех занятых в этой работе лиц, подразделений и специалистов.

С привлеченными лицами в обязательном порядке заключается соглашение о конфиденциальности, в котором указываются обязанности сторон по неразглашению информации, ставшей им известной в ходе проведения работ.

5. Уязвимость основных элементов объектов информатизации

Наиболее доступными и уязвимыми элементами ИС объектов информатизации Росжелдора являются автоматизированные рабочие места (далее – АРМ) пользователей ИС. Именно с них могут быть предприняты многочисленные попытки несанкционированного доступа и попытки совершения несанкционированных действий (случайных и умышленных). С АРМ пользователей осуществляется управление процессами обработки информации (в том числе на серверах), запуск программного обеспечения, ввод и корректировка данных. На АРМ могут размещаться важные данные и ПО, предназначенное для обработки информации. Нарушения конфигурации аппаратно-программных средств АРМ и неправомерное вмешательство в процессы их функционирования могут приводить к нарушению целостности и доступности информации, невозможности своевременного решения важных задач и выходу из строя отдельных АРМ и ИС в целом.

Также уязвимыми являются такие элементы ИС объектов информатизации Росжелдора как файловые серверы, серверы баз данных и серверы приложений, в том числе входящие в состав ЦОД ГИС. Такие элементы в первую очередь могут быть использованы для получения доступа к защищаемой информации и оказания влияния на работу различных подсистем ИС. При этом могут предприниматься попытки как удаленного (с АРМ) так и непосредственного (с консоли сервера) воздействия на работу серверов и их средств защиты.

Сетевое оборудование, каналы и средства связи также нуждаются в защите. Они могут быть использованы нарушителями для реструктуризации и дезорганизации работы сети, перехвата передаваемой информации, анализа трафика и реализации других способов вмешательства в процессы обмена данными.

6. Перечень основных опасных воздействующих факторов и значимых угроз информационной безопасности

Для обоснования необходимости применения тех или иных мер защиты информации в ИС объектов информатизации Росжелдора используются модели угроз ИБ и модели нарушителя ИБ, применительно к различным ИС. При этом каждой актуальной угрозе ИБ ставится в соответствие одно или несколько требований по обеспечению ИБ, а каждое такое требование реализуется одним или несколькими механизмами защиты (техническими средствами или организационными мероприятиями). В конечном итоге это позволяет уменьшить вероятность реализации угрозы ИБ, либо снизить возможный ущерб Росжелдору и иным субъектам информационных отношений.

При определении требований по безопасности информации для ИС объектов информатизации Росжелдора необходимо учитывать, что в отношении них существуют угрозы ИБ, являющиеся как следствием возможных проявлений воздействий внешней среды (пожар, затопление и пр.), так и связанные с человеческим фактором (целенаправленные или случайные).

Особое внимание при определении требований по ИБ для объектов информатизации должно уделяться угрозам ИБ, связанным с целенаправленным воздействием человеческого фактора.

Основными угрозами ИБ в ИС объектов информатизации Росжелдора являются:

нарушение конфиденциальности (разглашение, утечка) информации ограниченного доступа (персональных данных и информации «для служебного пользования»);

нарушение доступности информации (дезорганизация работы ИС), блокирование информации, нарушение технологических процессов, срыв своевременного решения задач;

нарушение целостности (искажение, подмена, уничтожение) информационных, программных и других информационных ресурсов объектов информатизации Росжелдора, а также фальсификация (подделка) документов.

Основными источниками угроз ИБ являются:

1) внешние источники:

деятельность сторонних организаций;

стихийные бедствия и природные явления (пожар, ураган, наводнение и др.);

деятельность злоумышленников;

2) внутренние источники:

непреднамеренные ошибки пользователей и администраторов;

непреднамеренные и умышленные нарушения пользователями ИС установленных требований ИБ при сборе, обработке, передаче и уничтожении информации;

возникновения технических проблем и ошибок конфигурации программного обеспечения;

отказы и сбои в работе оборудования.

Модели угроз и нарушителей предназначены для:

1) проведения классификации возможных угроз ИБ на основе общей классификации угроз безопасности информации;

2) выявления основных факторов риска и уязвимых мест для отдельных объектов информатизации и их элементов;

3) выявления возможных категорий потенциальных нарушителей безопасности информации для объектов информатизации;

4) определения способов доступа различных категорий нарушителей к защищаемой информации.

При анализе потенциальных угроз информации, обрабатываемой в ИС объектов информатизации, необходимо учитывать следующие характеристики:

1) тип ИС (локальная, распределенная);

2) объект оказания нарушителем воздействия на ИС (аппаратное обеспечение, операционная система, сетевое оборудование, каналы связи, системные сервисы, функциональные модули ИС, съемные носители информации и т.п.);

3) характер угрозы (случайная или преднамеренная);

4) длительность реализации угрозы;

5) вероятность реализации угрозы;

6) тяжесть последствий реализаций угрозы (величина потерь).

При анализе потенциальных нарушителей безопасности ИС необходимо учитывать следующие характеристики:

1) причины, мотивы и цели действий нарушителя;

2) тип нарушителя (внешний, внутренний);

3) уровень квалификации нарушителя;

4) априорные знания нарушителя о характеристиках ИС.

Детальные модели угроз и нарушителей разрабатываются для каждой ИС.

7. Подход к оценке рисков информационной безопасности для объектов информатизации

Цель анализа угроз ИБ заключается в снижении рисков ИБ, которые могут, в конечном итоге, привести к нарушению устойчивости и бесперебойности функционирования объектов транспортной инфраструктуры и транспортного комплекса в целом, ущемлению национальных интересов Российской Федерации в сфере безопасности на транспорте и интересов субъектов персональных данных.

Требования к обеспечению ИБ определяются с помощью систематической оценки рисков ИБ. Посредством оценки рисков ИБ происходит выявление угроз информации и уязвимостей основных элементов ИС объектов информатизации, оценка вероятности возникновения угроз и возможных последствий реализации таких сценариев «угроза-уязвимость».

Цель анализа рисков ИБ заключается в определении уровней рисков ИБ для информации, ИС, объектов информатизации и их элементов. Результаты анализа рисков ИБ используются для выбора средств и мер обеспечения ИБ и контроля уровня защищенности информационных ресурсов ИС объектов информатизации Росжелдора.

Таким образом, анализ и оценка рисков ИБ – это систематический анализ:

1) вероятного ущерба, наносимого деятельности Росжелдора и иным субъектам информационных отношений в результате нарушения ИБ с учётом возможных последствий от потери конфиденциальности, целостности или доступности информации и других ресурсов;

2) вероятного наступления нарушения с учётом существующих угроз и уязвимостей, а также внедрённых мероприятий по защите информации.

Выбор мероприятий по обеспечению ИБ основывается на соотношении стоимости их реализации к эффекту от снижения рисков ИБ и возможным убыткам в случае нарушения безопасности. Также принимаются во внимание факторы, которые не могут быть представлены в денежном выражении (например, последствия нарушений транспортной безопасности, ущерб национальным интересам Российской Федерации и пр.).

Анализ рисков ИБ проводится на регулярной основе и обеспечивает:

1) учёт изменений требований и приоритетов деятельности объектов информатизации Росжелдора;

2) учёт появления новых угроз ИБ и уязвимостей основных элементов ИС объектов информатизации Росжелдора;

3) выявление фактов снижения эффективности существующих мероприятий по защите информации.

При проведении анализа рисков ИБ учитывается:

1) значимость различных информационных и других ресурсов для Росжелдора и иных субъектов информационных отношений;

2) актуальность угроз ИБ для объектов информатизации;

3) уязвимости основных элементов ИС объектов информатизации;

4) возможности реализации угрозы ИБ с использованием уязвимостей.

Критерием оценки значимости различных информационных и других ресурсов для Росжелдора является ценность данных ресурсов, т.е. то, насколько важную роль играет информация или другой ресурс в деятельности Росжелдора, в процессах обеспечения транспортной безопасности, а также в целом для обеспечения национальной безопасности Российской Федерации. При этом стоимость самих ресурсов может составлять лишь малую часть общих затрат.

Возможность реализации угрозы оценивается вероятностью её реализации в течение заданного отрезка времени для некоторого информационного ресурса. При этом вероятность реализации угрозы определяется следующими основными показателями:

1) привлекательность ресурса (показатель используется при рассмотрении угрозы от умышленного воздействия со стороны нарушителя);

2) возможность использования ресурса для получения дохода (также используется при рассмотрении угрозы от умышленного воздействия со стороны нарушителя);

3) технические возможности реализации угрозы;

4) степень сложности использования уязвимости и реализации угрозы.

Показатели ценности ресурсов, значимости угроз и уязвимостей,

эффективность средств защиты могут быть определены как количественными методами (преимущественно для стоимостных характеристик), так и качественными (в частности, учитывающими штатные или чрезвычайно опасные нештатные воздействия внешней среды).

8. Основные положения технической политики в области обеспечения безопасности информации

Реализация технической политики в области обеспечения ИБ должна исходить из предпосылки, что невозможно обеспечить требуемый уровень защищенности информации не только с помощью одного отдельного средства (мероприятия), но и с помощью их простой совокупности. Необходимо их системное согласование между собой (комплексное применение), а отдельные разрабатываемые системы защиты информации в ИС объектов информатизации Росжелдора должны рассматриваться как часть единой системы ИБ при оптимальном соотношении технических (аппаратных, программных) средств и организационных мероприятий.

В рамках системы ИБ осуществляются:

1) реализация разрешительной системы допуска пользователей к информационным ресурсам ИС Росжелдора;

2) обеспечение физической безопасности объектов информатизации (территории, здания, помещении) с комплексным применением современных технических средств охраны, обнаружения, наблюдения, сбора и обработки информации;

3) ограничение доступа пользователей ИС и иных лиц в здания и помещения, где проводятся работы с информацией ограниченного доступа и размещены средства информатизации и коммуникации, на которых обрабатывается указанная информация, непосредственно к самим средствам информатизации и коммуникациям;

4) разграничение доступа пользователей ИС и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защита информации в подсистемах различного уровня и назначения, входящих в состав ИС;

5) учет информационных ресурсов ИС, регистрация и контроль действий пользователей, обслуживающего персонала и посторонних лиц;

6) предотвращение внедрения в ИС вредоносного программного обеспечения;

7) криптографическая защита информации, обрабатываемой и передаваемой средствами вычислительной техники и связи;

8) необходимое резервирование технических средств ИС и дублирование массивов и носителей информации;

9) обеспечение акустической защиты помещений объектов информатизации, в которых циркулирует информация ограниченного доступа, в том числе противодействие оптическим и лазерным средствам наблюдения;

10) установление на объектах информатизации Росжелдора организационно-правового режима безопасности информации (нормативно-правовое обеспечение);

11) выполнение организационно-технических мероприятий по защите информации ограниченного доступа, в том числе аттестация ИС объектов информатизации по требованиям безопасности информации;

12) организационные и программно-технические мероприятия по предупреждению несанкционированных действий (доступа) к информационным ресурсам ИС;

13) комплекс мероприятий по контролю функционирования средств и систем защиты информации ограниченного доступа после случайных или преднамеренных воздействий.

9. Обеспечение защиты от использования нарушителем технических каналов утечки информации

Организационно-технические мероприятия по защите информации ограниченного доступа от утечки по техническим каналам предусматривают:

1) комплекс мер и соответствующих технических средств, ослабляющих уровень информативных сигналов для речевой и сигнальной информации;

2) комплекс мер и соответствующих технических средств, создающих помехи при съеме информации.

Для большинства объектов информатизации Росжелдора в соответствии с условиями эксплуатации и размещения оборудования ИС признаются неактуальными угрозы утечки информации по каналам побочных электромагнитных излучений и наводок. Угрозы утечки акустической речевой информации и угрозы утечки видовой информации в большинстве случаев являются актуальными, в связи с чем необходимо использовать соответствующие инженерно-технические средства защиты информации и/или организационно-технические мероприятия.

Основные методы и способы защиты акустической (речевой) информации заключаются в реализации организационных и технических мер для обеспечения звукоизоляции ограждающих конструкций защищаемых помещений, их систем вентиляции и кондиционирования, не позволяющей вести прослушивание акустической (речевой) информации. Степень звукоизоляции определяется исходя из характеристик помещения, его расположения и особенностей обработки информации ограниченного доступа.

С целью защиты видовой информации размещение устройств вывода информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео и буквенно-цифровой информации, входящих в состав ИС в помещениях, в которых они установлены, осуществляется таким образом, чтобы была исключена возможность просмотра посторонними лицами текстовой и графической видовой информации ограниченного доступа.

Детальное описание мероприятий по защите информации от утечки по техническим каналам определяется принятыми в Росжелдоре документами по технической защите информации.

10. Основные меры и методы (способы) защиты от угроз, средства обеспечения требуемого уровня защищенности информационных ресурсов.

10.1. Организационные (административные) меры защиты

Организационные (административные) меры защиты – это меры, регламентирующие процессы использования информационных ресурсов объектов информатизации Росжелдора, деятельность персонала, а также порядок взаимодействия пользователей ИС со средствами обработки и носителями информации таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз ИБ или снизить размер ущерба в случае их реализации.

10.2. План мероприятий по технической защите информации

В Росжелдоре должен быть документирован порядок действий по обеспечению технической защиты информации (далее – ТЗИ) объектов информатизации Росжелдора.

Потребности Росжелдора устанавливаются в документах, описывающих процессы обеспечения безопасности информации ограниченного доступа, их содержание и управление ими.

Разрабатывается план мероприятий по ТЗИ, представляющий собой документ, определяющий последовательность, сроки и ожидаемые результаты выполнения мероприятий по обеспечению требуемого уровня защищенности информации.

В плане отражаются краткосрочные, среднесрочные и долгосрочные мероприятия, направленные на достижение и поддержание требуемого уровня защищенности. При помощи плана обеспечивается своевременное внедрение защитных мер в соответствии с приоритетами, определёнными на основе анализа рисков.

Организационные меры предусматривают создание и поддержание в актуальном состоянии на объектах информатизации Росжелдора нормативной базы по вопросам ИБ и разработку (введение в действие) нормативно-методических и организационно-распорядительных документов.

В случае, когда обслуживание АС осуществляется сторонними организациями на основании договоров с Росжелдором, указанные организации должны иметь, следующие документы:

1) договор на обслуживания АС, включающий положения об обеспечении исполнителем по договору конфиденциальности и безопасности информации ограниченного доступа при ее обработке;

2) регламент взаимодействия с Росжелдором.

10.3. Соответствие требованиям законодательства Российской Федерации

Все применяемые нормы законодательства Российской Федерации, обязательные предписания, регулирующие требования и договорные обязательства, следует четко определять и документировать для каждого объекта (типов объектов) информатизации Росжелдор и их ИС. Конкретные мероприятия по обеспечению безопасности информации и обязанности должностных лиц Росжелдор и пользователей ИС по выполнению этих требований необходимо соответствующим образом определять, документировать и доводить до сведения заинтересованных лиц.

10.4. Персонал (пользователи ИС)

Защитные меры в этой категории должны снижать риски ИБ в результате ошибок, преднамеренного или непреднамеренного нарушения правил ИБ, связанных с человеческим фактором.

Обязанности по соблюдению требований ИБ следует распределять на стадии подбора персонала, включать в служебные контракты, трудовые договоры (далее – трудовые договоры), договоры гражданско-правового характера, проводить их мониторинг в течение всего периода работы работника.

Ответственность и права работников в соответствии с действующим законодательством Российской Федерации должны быть разъяснены персоналу и включены в условия трудового договора (договора гражданско-правового характера).

Соглашения о конфиденциальности (соглашения о неразглашении) используются для уведомления работников о том, что информация является информацией ограниченного доступа. Работники должны подписывать такое соглашение как неотъемлемую часть условий трудового договора.

Временные работники и представители третьих сторон, не подпадающие под стандартный трудовой договор (содержащий соглашение о соблюдении конфиденциальности), должны подписывать отдельно соглашение о соблюдении конфиденциальности до того, как им будет предоставлен доступ к ресурсам Росжелдор.

Соглашение о соблюдении конфиденциальности следует пересматривать при изменении условий трудового договора, особенно в случае изменения обязанностей работника или истечении сроков трудовых договоров.

Необходимо регулярно проводить обучение персонала процедурам обеспечения ИБ и правильному использованию средств обработки информации.

Обучение персонала должно обеспечить знание требований ИБ, ответственности в соответствии с законодательством Российской Федерации, мероприятий по управлению ИБ, а также знание правильного использования средств обработки информации, прежде чем будет предоставлен доступ к ресурсам.

Для работников, отвечающих за обеспечение ИБ, необходимо планировать и проводить обучение на специализированных курсах по обеспечению ИБ.

Необходимо разработать формализованные процедуры, устанавливающие дисциплинарную ответственность работников, нарушивших политику и процедуры

обеспечения безопасности информации Росжелдор.

10.5. Обеспечение непрерывности функционирования ИС

На объектах информатизации Росжелдор необходимо обеспечить непрерывность функционирования ИС с целью минимизации негативных последствий, вызванных бедствиями и нарушением безопасности (которые могут быть результатом природных бедствий, несчастных случаев, отказов оборудования или преднамеренных действий) с помощью сочетания профилактических и восстановительных мероприятий по управлению ИБ.

Необходимо разработать и внедрить план обеспечения непрерывности функционирования ИС с целью восстановления нормального функционирования ИС в течение требуемого времени при его нарушении.

10.6. Эксплуатационные меры

Целью защитных мер данной категории является поддержание в рабочем состоянии процедур по обеспечению ИБ, правильного и надежного функционирования оборудования, программных и технических средств.

Все аспекты операций и конфигураций должны быть документированы.

Должно проводиться техническое обслуживание оборудования для обеспечения его надежности, доступности и целостности. Требования по обеспечению безопасности, которые должны соблюдать подрядчики при выполнении технического обслуживания, должны быть документально оформлены и записаны в соответствующих контрактах.

10.7. Структура, функции и полномочия подразделения обеспечения информационной безопасности

Организация работ по защите информации ограниченного доступа возлагается на руководство Росжелдора.

При привлечении для разработки системы ИБ или ее отдельных компонентов специализированных организаций в Росжелдоре из числа работников ответственных за ТЗИ определяются ответственные за взаимодействие с указанными организациями.

При разработке и внедрении системы ИБ с участием специализированных организаций ответственный за ТЗИ осуществляет методическое руководство и участвует в разработке конкретных требований по ИБ, аналитическом обосновании необходимости создания системы ИБ, согласовании выбора средств вычислительной техники и связи, технических и программных средств защиты, организации работ по выявлению возможных каналов утечки информации или воздействий на нее и предупреждению утечки и нарушения целостности защищаемой информации, а также в аттестации ИС.

Задачами по ТЗИ в области защиты информации являются:

1. Определение состава и объема информации ограниченного доступа,

а также круга лиц, которые в силу занимаемого служебного положения в Росжелдоре и/или выполняемых функций имеют к ней доступ.

2. Определение участков сосредоточения информации ограниченного доступа; технологического оборудования, выход из строя которого (в том числе уязвимого в аварийном отношении) может привести к значительным экономическим и иным потерям (анализ уязвимости).

3. Организация мероприятий и координация работ подразделений Росжелдора и подведомственных организаций и ведомств по защите информации.

4. Разработка проектов организационно-распорядительных и нормативно-методических документов по вопросам обеспечения защиты информации ограниченного доступа, определение порядка обращения с информацией, содержащей сведения конфиденциального характера.

5. Формирование требований к системе ИБ и ее элементам в процессе их создания и проектирования, участие в их испытаниях и приемке в эксплуатацию.

6. Планирование, организация и обеспечение функционирования системы ИБ Росжелдора, а также подсистем защиты информации в ИС Росжелдора.

7. Организация контроля функционирования системы ИБ и ее элементов, тестирования системы ИБ.

8. Разработка рекомендаций по технической защищенности помещений Росжелдора, в которых осуществляются работы с носителями информации ограниченного доступа.

9. Организация обучения работников Росжелдора в соответствии с их функциональными обязанностями по обеспечению ЗИ.

10. Организация обучения пользователей ИС правилам безопасной обработки информации.

11. Участие в расследовании происшедших нарушений ИБ, принятие мер реагирования на попытки НСД к информации и нарушениям правил функционирования системы ИБ и ее элементов.

12. Организация выполнения восстановительных процедур после инцидентов ИБ.

13. Изучение, анализ, оценка состояния и разработка предложений по совершенствованию системы ИБ Росжелдора.

14. Применение в деятельности Росжелдора новейших технологий, передового опыта в области защиты информации.

15. Организация совместной работы с представителями других организаций по вопросам обеспечения безопасности информации.

16. Постоянная проверка соответствия требований принятой в Росжелдоре технологии обработки информации ограниченного доступа требованиям законодательства Российской Федерации, контроль за соблюдением этого соответствия.

17. Взаимодействие с органами власти, службами безопасности и защиты информации других организаций, координация работы структурных подразделений

Росжелдора по вопросам обеспечения защиты информации.

Также в обязанности работников ответственных за ТЗИ входит участие в выработке решений по всем вопросам, связанным с процессом обработки информации с точки зрения обеспечения его защиты.

Подразделение по защите информации Росжелдора либо должностное лицо на которое возложены обязанности по ТЗИ:

обеспечивает подготовку проектов текущих и перспективных планов работ и осуществляет контроль за выполнением стоящих перед ним задач;

возглавляет разработку проектов внутренних нормативных, методических и инструктивных материалов по направлениям деятельности ТЗИ;

организует исполнение требований внутренней нормативной документации Росжелдора по обеспечению ТЗИ и координирует деятельность структурных подразделений Росжелдора в решении задач защиты информации ограниченного доступа;

оценивает эффективность действующих внутренних нормативных, методических и инструктивных материалов, касающихся деятельности Росжелдора;

участвует в организации проведения служебных расследований по факту произошедших инцидентов ИБ;

обеспечивает правильное применение в работе действующего законодательства Российской Федерации;

обеспечивает предоставление работникам Росжелдора консультаций по вопросам обеспечения ИБ;

разрабатывает предложения по составу программного обеспечения и технических средств обеспечения ИБ;

разрабатывает предложения по разграничению доступа к информационным ресурсам, программным и техническим средствам ИС;

разрабатывает технические правила и рекомендации по отражению и нейтрализации угроз безопасности информации, участвовать в реализации указанных рекомендаций;

определяет уровень/класс защищенности ИС и ее сегментов;

участвует в проведении аттестационных испытаний ИС;

участвует в проведении проверок выполнения требований по обеспечению безопасности объектов информатизации;

оценивает применяемые способы, методы и средства защиты информации;

формирует отчетные материалы о выявленных нарушениях, попытках или фактах несанкционированного доступа к информации, о невыполнении пользователями требований по защите информации.

10.8. Физические средства защиты

На объектах информатизации Росжелдора должен быть введен режим ограничения доступа в здания и помещения, в которых обрабатывается информация ограниченного доступа, размещены технические средства, обрабатывающие информацию ограниченного доступа, и хранятся материальные носители

информации ограниченного доступа, а также установлена система контроля и управления доступом.

Необходимость доступа работников объекта/пользователей ИС в помещения объектов информатизации Росжелдора, в которых обрабатывается информация ограниченного доступа, размещены технические средства и хранятся материальные носители информации, определяется в соответствии с их функциональными/должностными обязанностями.

Физическая охрана объектов информатизации (компонентов ИС) включает:

1. Организацию системы охранно-пропускного режима и системы контроля допуска на объект.
2. Введение дополнительных ограничений по доступу в помещения, предназначенные для хранения информации ограниченного доступа (кодовые и электронные замки, карточки допуска и т.д.).
3. Визуальный и технический контроль контролируемой зоны объекта защиты.
4. Применение систем охранной и пожарной сигнализации, систем пожаротушения и т.д.

10.9. Общие положения

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав объектов информатизации и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты информации.

С учетом всех требований и принципов обеспечения безопасности информации в ИС объектов информатизации Росжелдора должно быть обеспечено внедрение процедур:

1. Идентификации и аутентификации субъектов доступа и объектов доступа.
2. Управления доступом субъектов доступа к объектам доступа.
3. Ограничения программной среды.
4. Защиты машинных носителей информации.
5. Регистрации событий безопасности.
6. Антивирусной защиты.
7. Обнаружения вторжений.
8. Контроля (анализа) защищенности информации.
9. Обеспечения целостности информационной системы и информации.
10. Обеспечения доступности информации.
11. Защиты среды виртуализации.
12. Защиты технических средств.
13. Защиты информационных систем, их средств, систем связи и передачи данных.
14. Выявления инцидентов и реагирование на них.
15. Управления конфигурациями информационных системы и системы защиты информации.

10.10.Идентификация и аутентификация субъектов доступа и объектов доступа

Идентификация и аутентификация субъектов доступа и объектов доступа обеспечиваются за счет:

1) проверки подлинности при входе в ИС по идентификатору и паролю;
2) проверки подлинности устройств, в том числе стационарных, мобильных и портативных;
3) управления средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации.

Система идентификации и аутентификации представляет собой комплекс программно-технических средств, обеспечивающих идентификацию пользователей ИС и подтверждение подлинности пользователей при получении доступа к информационным ресурсам. Система идентификации и аутентификации включает в себя компоненты, встроенные в операционные системы, межсетевые экраны, СУБД и приложения, которые обеспечивают управление идентификационными данными пользователей, паролями и ключевой информацией, а также реализуют различные схемы подтверждения подлинности при входе пользователя в систему и получении доступа к системным ресурсам и приложениям.

Встроенные средства идентификации и аутентификации могут дополняться наложенными средствами, обеспечивающими синхронизацию учетных данных пользователей в различных хранилищах и предоставление единой точки доступа и администрирования для всех пользователей ИС.

10.11. Управление доступом субъектов доступа к объектам доступа

Средства управления доступом обеспечивают:

1) управление учетными записями пользователей;
2) назначение прав доступа пользователей к объектам доступа;
3) контроль доступа пользователей к защищаемым ресурсам в соответствии с их правами.

При определении прав доступа пользователей ИС к защищаемой информации применяется «принцип недоверия», который означает, что все полномочия по доступу являются персональными, указаны явно и проверены перед предоставлением доступа, а также «принцип минимума полномочий», означающий, что по запросу на доступ к объектам информатизации предоставляются полномочия, минимально необходимые и достаточные для реализации данного запроса.

Процедуры управления доступом исключают возможность «самосанкционирования».

Средства разграничения доступа исключают возможность доступа к объектам информатизации неавторизованных пользователей.

В ИС должны использоваться средства межсетевого экранирования и проводиться сегментирование сетей. Сегментирование и межсетевое экранирование предназначено для разграничения межсетевого доступа на уровне сетевых

протоколов и защиты ИС от сетевых атак со стороны сетей общего пользования.

В ИС должны применяться защитные меры, направленные на обеспечение защиты от несанкционированного доступа и нерегламентированных действий в рамках предоставленных полномочий, повреждения или нарушения целостности информации, необходимой для регистрации, идентификации, аутентификации и (или) авторизации пользователей ИС.

10.12. Ограничение программной среды

Ограничение программной среды обеспечивается за счет:

1) установки (инсталляции) только разрешенного к использованию программного обеспечения и (или) его компонентов;

2) установки (инсталляции) необходимых компонентов программного обеспечения, в том числе настройки параметров установки компонентов и контроля за установкой компонентов программного обеспечения;

3) запуска необходимых компонентов ПО, в том числе настройки параметров запуска компонентов и контроля за запуском компонентов ПО.

10.13. Защита машинных носителей информации

Защита машинных носителей информации обеспечивается за счет:

1. Учета машинных носителей информации.
2. Контроля доступа к машинным носителям информации.
3. Контроля использования машинных носителей информации.
4. Контроля своевременного и надежного уничтожения информации с носителей.

10.14. Регистрация событий безопасности

Регистрация событий ИБ поводится с целью обнаружения событий ИБ, связанных с нештатным функционированием программных и аппаратных средств, а также с работой пользователей ИС.

В ИС и их компонентах обеспечивается:

1) регистрация и учет событий ИБ в журналах средств защиты информации, системного и прикладного ПО;

2) хранение информации о событиях безопасности в течение установленного времени хранения;

3) мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них.

С момента предоставления пользователям прав доступа к ресурсам ИС должно вестись протоколирование, сбор и накопление информации о происходящих в системе событиях ИБ.

Результаты протоколирования используются для выявления нарушения состояния ИБ и проведения расследования инцидентов ИБ.

10.15. Антивирусная защита

К использованию в ИС допускаются только лицензионные средства защиты от вредоносного ПО.

Используемые в ИС средства защиты от вредоносного ПО должны обеспечивать защиту от всех вредоносных программ, включая rootkit и рекламное ПО.

Средства защиты от вредоносного ПО должны быть установлены на всех компонентах ИС.

10.16. Криптографическая защита информации

Средства криптографической защиты информации (СКЗИ) используются для защиты информации, передаваемой по каналам связи.

В целях обеспечения сохранности СКЗИ, инсталлирующих СКЗИ носителей, эксплуатационной и технической документации к СКЗИ, рабочих станций, на которых установлены и используются СКЗИ, должны размещаться в помещениях, исключающим возможность бесконтрольного проникновения посторонних лиц. Помещения выделяются с учетом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к СКЗИ.

Для инсталлирующих СКЗИ носителей, эксплуатационной и технической документации к СКЗИ и ключевых документов обеспечиваются безопасные условия хранения.

Помещения, в которых используются СКЗИ и хранятся инсталлирующие СКЗИ носители, эксплуатационная и техническая документация к СКЗИ, ключевые документы, должны быть оборудованы средствами физической защиты (хранилища (запираемые шкафы, сейфы и т.п.), надежные, запираемые двери выделенных помещений и т.д.).

На объектах информатизации Росжелдора должны быть определены требования по управлению криптографическими ключами, в том числе ключевыми документами. Управление криптографическими ключами включает следующие этапы:

1. Получение/генерация криптографических ключей.
2. Использование и хранение криптографических ключей.
3. Смена криптографических ключей.
4. Уничтожение криптографических ключей.
5. Действия при компрометации криптографических ключей.

10.17. Обнаружение вторжений

Обнаружение вторжений проводится для компонентов ИС, подключенных к сетям международного информационного обмена, путем использования в составе информационной системы программных или программно-аппаратных средств

обнаружения вторжений.

Средства обнаружения и предотвращения вторжений должны обеспечивать обнаружение, регистрацию и предотвращение сетевых атак на информационные ресурсы объектов информатизации.

10.18. Контроль (анализ) защищенности информации

Средства анализа защищенности должны обеспечивать:

1) возможность выявления уязвимостей, связанных с ошибками в конфигурации программного обеспечения, которые могут быть использованы нарушителем для реализации атак на систему;

2) проведение контроля установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации.

Контроль защищенности предназначен для выявления и ликвидации уязвимостей сетевых сервисов, приложений, функциональных подсистем, системного ПО и СУБД, а также мониторинга и аудита событий, активного сетевого оборудования, серверов, рабочих станций, входящих в состав ИС.

10.19. Обеспечение целостности информационной системы и информации

Контроль целостности программных и информационных ресурсов ИС предназначен для контроля и оперативного восстановления целостности критичных файлов ОС и приложений на серверах и рабочих станциях сети, включая конфигурационные файлы, файлы данных, программы и библиотеки функций.

В ИС должна обеспечиваться целостность программных средств объектов информатизации, обрабатываемой информации, а также неизменность программной среды, при этом:

неизменность программной среды обеспечивается путем исключения из программной среды средств разработки и отладки программ;

целостность программных средств проверяется при загрузке системы по наличию имен (идентификаторов) элементов средств защиты информации;

периодическое тестирование функций системы ИБ с помощью тест-программ, имитирующих попытки несанкционированного доступа.

10.20. Обеспечение доступности информации

Обеспечение доступности информации обеспечивается за счет:

1. Использования отказоустойчивых технических средств.
2. Резервирования технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы.
3. Периодического резервного копирования информации на резервные машинные носители информации.
4. Обеспечения возможности восстановления информации с резервных

машинных носителей информации (резервных копий) в течение установленного временного интервала.

10.21. Защита среды виртуализации

Защита среды виртуализации обеспечивается за счет:

1. Идентификации и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации.
2. Управления доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин.
3. Регистрации событий ИБ в виртуальной инфраструктуре.
4. Управления потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры.
5. Контроля целостности виртуальной инфраструктуры и ее конфигураций.
6. Резервного копирования данных, резервирования технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры.
7. Реализации антивирусной защитой в виртуальной инфраструктуре.

10.22. Защита информационных систем, их средств, систем связи и передачи данных

Защита ИС, их средств, систем связи и передачи данных обеспечивается за счет:

1. разделения в ИС функций по администрированию ИС, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций ИС;
2. обеспечения защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи;
3. обеспечения подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов;
4. исключения возможности отрицания пользователем факта отправки и получения информации другому пользователю;
5. защиты параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации;
6. защиты мобильных технических средств, применяемых в ИС.

10.23. Выявление инцидентов и реагирование на них

Обнаружение инцидентов ИБ осуществляется на постоянной основе за счет

выявления событий ИБ и/или подозрительной активности.

Меры по выявлению инцидентов ИБ (одного события ИБ или группы событий ИБ), которые могут привести к сбоям или нарушению функционирования ИС и (или) к реализации угроз безопасности информации ограниченного доступа должны обеспечивать:

1) обнаружение, идентификацию, анализ инцидентов ИБ в ИС;
2) принятие мер по устранению и предупреждению инцидентов ИБ;
3) расследование инцидентов ИБ.

С целью профилактики нарушений проводятся мероприятия, направленные на:

1) доведение до пользователей ИС всей важности и необходимости выполнения задач по обеспечению ИБ в рамках своей компетенции;
2) проведение проверок с целью выявления нарушений или предпосылок к нарушениям при работе с информационными ресурсами ИС;
3) доведение, при необходимости, до пользователей ИС результатов проведения проверок.

10.24. Управление конфигурацией информационной системы

Процесс управления конфигурациями ИС и системы защиты в ее составе предназначен для:

1) уменьшения количества инцидентов ИБ, связанных с внесением изменений в ИС и системы ИБ;
2) поддержания актуальности ПО и аппаратных средств ИС и системы ИБ;
3) повышения эффективности взаимодействия подразделений и подрядных организаций, вовлеченных в установку, модификацию и техническое обслуживание ПО, аппаратных средств ИС и системы ИБ.

Управление конфигурацией обеспечивается за счет:

контроля лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных;

управления изменениями конфигураций ИС и системы ИБ;

анализа потенциального воздействия планируемых изменений в конфигурациях ИС и системы ИБ.

10.25. Управление системой обеспечения безопасности информации

Управление системой обеспечения информационной безопасности ИС объектов информатизации Росжелдора должно представлять собой часть общей системы управления объекта, предназначенной для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и повышения уровня информационной безопасности. Элементы управления системой обеспечения безопасности информации приведены на

Рисунок № 1. к Концепции.

В рамках управления системой ИБ должно быть реализовано следующее:

Определение основных направлений обеспечения ИБ.

Выбор подхода к управлению рисками ИБ, анализ и оценка рисков ИБ, определение вариантов обработки рисков ИБ для наиболее критичных информационных ресурсов;

Выбор защитных мер и их обоснование для минимизации рисков ИБ.

Принятие руководством объектов информатизации Росжелдора остаточных рисков ИБ и решения о реализации и эксплуатации/совершенствовании систем обеспечения ИБ.

Осуществление постоянного контроля и мониторинга системы обеспечения ИБ для своевременного выявления нарушений и инцидентов ИБ, а также выявление необходимости в совершенствовании системы обеспечения ИБ.

Выделение необходимых и достаточных ресурсов (как финансовых, так и людских) для нормального функционирования и совершенствования системы обеспечения ИБ.

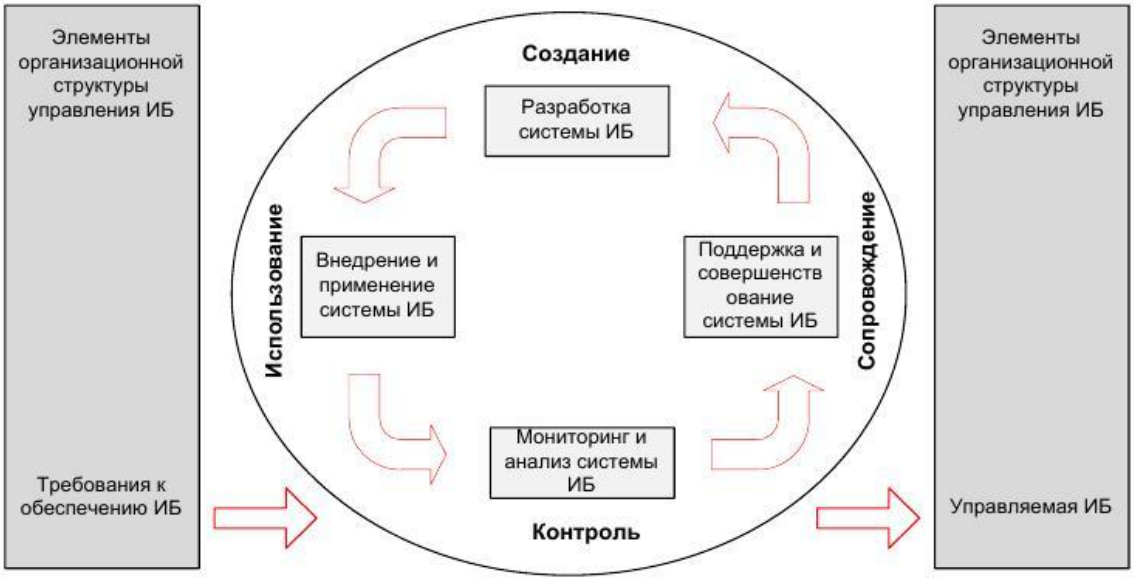

Рисунок № 1. Элементы управления системой обеспечения ИБ

10.26. Контроль эффективности системы обеспечения ИБ

Обязательной составляющей мероприятий по обеспечению ИБ является организация проверок и оценок состояния ИБ на объектах информатизации Росжелдора. Проверка и оценка состояния ИБ производится с помощью аудита и мониторинга эффективности ИБ.

Аудит ИБ может быть внутренним или внешним. Внутренний аудит ИБ проводится силами подразделения на которое возложены функции по ТЗИ Росжелдора, а также силами соответствующих подразделений объектов информатизации (эксплуатирующих организаций) на регулярной периодической основе или же при необходимости по распоряжению руководства Росжелдора. Внешний аудит проводится сторонней по отношению к Росжелдору организацией.

Цель аудита ИБ состоит в проверке и оценке соответствия ИБ требованиям нормативных документов Росжелдора, руководящим документам ФСТЭК России,

документам ФСБ России, международным стандартам и законодательству Российской Федерации.

Основными задачами мониторинга ИБ являются оперативное и постоянное наблюдение, сбор, анализ и обработка данных для обнаружения инцидентов ИБ и выявление ситуаций, создающих угрозы ИБ.

На объектах информатизации Росжелдора на периодической основе проводится оценка эффективности и результативности работы процессов и мер обеспечения ИБ. Оценка эффективности осуществляется на основе расчета показателей эффективности и результативности (метрик ИБ) процессов и сравнения получаемых значений с целевыми и пороговыми значениями. На основании полученных результатов принимается решение о необходимости совершенствования мер по обеспечению ИБ.