ЛЕКЦИЯ

«ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ТРАНСПОРТЕ»

ВОПРОСЫ ЛЕКЦИИ

1. Цели, задачи, объекты и угрозы информационной безопасности
2. Принципы построения и функционирования системы управления информационной безопасностью
3. Организационная структура и нормативная база обеспечения и управления информационной безопасностью
4. Корпоративные политики информатизации и информационной безопасности
5. Методики оценки значимости информационных ресурсов и безопасности информации и система оценки защищенности автоматизированных информационных и телекоммуникационных систем

ЛИТЕРАТУРА:

1. Баранова Е. К. Информационная безопасность и защита информации[Электронный ресурс]: учебное пособие / Е. К. Баранова, А. В. Бабаш, 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2017. - 322 с. (Высшее образование).

2. Информационная безопасность и защита информации на железнодорожном транспорте : учебник в 2ч./ С.Е. Ададуров , Под ред. А.А. Корниенко. М.: УМЦ ЖДТ, 2014. 440 с.

1. Цели, задачи, объекты и угрозы информационной безопасности

Информация, информационно коммуникационные технологии, информационная и телекоммуникационная инфраструктура определяют дальнейшее развитие экономики и технологий, социально-политической, культурной и духовной сферы, науки, образования и других сфер

человеческой деятельности. Информационная безопасность в условиях глобальной информатизации общества рассматривается сегодня как одна из важных компонент национальной безопасности, определяющая другие ее составляющие: экономическую, оборонную, социальную, экологическую и т.п.

Угрозы информационной безопасности, как указано в Стратегии национальной безопасности Российской Федерации до 2020 года, предотвращаются за счет совершенствования безопасности функционирования информационных и телекоммуникационных систем, критически важных объектов инфраструктуры и объектов повышенной опасности в Российской Федерации, повышения уровня защищенности корпоративных и индивидуальных информационных систем, создания единой системы информационно телекоммуникационной поддержки нужд системы обеспечения национальной безопасности. Информационная сфера и информационная безопасность также начинают играть одну из ключевых ролей в обеспечении важных, прежде всего экономических, интересов транспортного комплекса России, в управлении отраслью и железнодорожным транспортом, в решении проблем безопасности движения, пассажирских и грузовых перевозок. Это обусловлено целым рядом факторов:

- общей тенденцией построения Россией информационного общества;
- динамично нарастающей информатизацией и «интеллектуализацией» железнодорожного транспорта;
- созданием значительных информационных ресурсов и развитой информационной телекоммуникационной инфраструктуры в стране и отрасли;
- широким внедрением информационно управляющих и автоматизированных средств, информационных систем и телекоммуникационных сетей на железных дорогах России;

- соизмеримостью в недалеком будущем транспортных и информационных услуг и, как следствие, с увеличением (количественным и качественным) потенциальных угроз информационной, экономической, технологической, социальной и другим сферам железнодорожного транспорта, с возможным появлением злоумышленных действий, преступлений и терроризма в информационной среде, вовлечением ее в сферу информационного противоборства.

1.1 Цели, задачи, объекты и угрозы информационной безопасности

Цели и задачи информационной безопасности.

Под информационной безопасностью корпорации — холдинга ОАО «РЖД» — будем понимать состояние защищенности информационных активов — информации и информационной инфраструктуры, других информационных активов (ресурсов), при котором обеспечивается приемлемый риск нанесения ущерба в условиях проявления внешних и внутренних, случайных и преднамеренных угроз.

Основными целями обеспечения информационной безопасности и защиты информации в отрасли, компании ОАО «РЖД», корпоративных системах и сетях железнодорожного транспорта являются:

– поддержание высокого уровня безопасности движения, грузовых и пассажирских перевозок железнодорожного транспорта в условиях динамичной корпоративной информатизации;

– минимизация или обеспечение приемлемого уровня информационных рисков, экономического и других видов ущерба при нарушении безопасности информации;

– обеспечение руководства и сотрудников компании полной, достоверной и своевременной информацией, необходимой для принятия решений, и предоставление информационных услуг, в том числе по защите информации (обеспечение ее конфиденциальности, целостности и доступности), клиентам — пользователям информационных систем: грузоотправителям, грузополучателям, пассажирам и другим.

Другие важные цели обеспечения информационной безопасности ОАО «РЖД» — защита информационных ресурсов от несанкционированного доступа, обеспечение их целостности и доступности, защита информационных и телекоммуникационных систем от преступлений и актов терроризма, совершаемых с использованием уязвимостей информационных технологий, формирование систем электронного взаимодействия ОАО «РЖД» с органами власти, предприятиями, организациями и частными лицами, и создание на этой основе благоприятных условий для экономической стабильности и развития ОАО «РЖД».

Разработка и осуществление мероприятий для достижения целей обеспечения информационной безопасности должны проводиться в соответствии с принципами: законности, системности, комплексности, непрерывности, своевременности, преемственности и непрерывности совершенствования, разумной достаточности, персональной ответственности, минимизации полномочий, гибкости системы защиты, открытости алгоритмов и механизмов защиты, простоты применения средств защиты, научной обоснованности и технической реализуемости, а также обязательности контроля.

Основными задачами обеспечения информационной безопасности ОАО «РЖД» являются:

– создание механизмов своевременного выявления, прогнозирования, локализации и блокирования угроз безопасности, оперативного реагирования на проявления негативных тенденций в использовании информационных ресурсов и систем;

– совершенствование системы управления информационной безопасностью;

– создание необходимой непротиворечивой нормативной правовой базы обеспечения информационной безопасности;

– создание технической и технологической базы информационной безопасности;

– обеспечение правовой защиты субъектов информационных отношений;

– сохранение и эффективное использование информационных ресурсов;

– координация деятельности филиалов ОАО «РЖД», дочерних и зависимых организаций и предприятий в обеспечении информационной безопасности;

– унификация требований к обеспечению информационной безопасности;

– создание типовых технологий (комплексов) защиты информационных ресурсов и объектов информатизации, обеспечивающих установленные требования безопасности;

– создание комплексной системы контроля эффективности применяемых мер и средств защиты;

– эффективное пресечение посягательств на конфиденциальность, целостность и доступность информационных ресурсов.

Объекты информационной безопасности

Объектами обеспечения информационной безопасности корпорации являются информационные активы и, прежде всего, информация конфиденциального характера и информационная инфра структура. К защищаемой информации на железнодорожном транспорте в более широком смысле относится информация ограниченного доступа — сведения, содержащие государственную тайну, и информация конфиденциального характера — коммерческая тайна, персональные данные работников ОАО «РЖД» и других физических лиц, служебная тайна, а также информация, охраняемая авторским и патентным правом и являющаяся интеллектуальной собственностью. Наряду с информацией ограниченного доступа и интеллектуальной собственностью должна защищаться и открытая информация в части целостности и доступности — оперативная управленческая информация, данные, другая информация, циркулирующая в

корпоративных информационных систем и сетях (КИСС) железнодорожного транспорта. Информационная инфраструктура корпорации (рис. 4.2) образована несколькими слоями корпоративных информационноуправляющих, автоматизированных, информационных систем и информационнотелекоммуникационных сетей железнодорожного транспорта. Она включает:

1) средства, системы и объекты информатизации (центры обработки данных, информационновычислительные центры и комплексы, локальные вычислительные сети, информационноаналитические системы ситуационных центров и центров управления перевозками, другие информационные системы, локальные вычисли тельные сети, автоматизированные рабочие места (АРМ) и средства вычислительной техники), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), информационные и автоматизированные системы управления (АСУ) на железнодорожном транспорте:

АСУ финансовыми, материальными и трудовыми ресурсами (ЕК АСУФР/АСУТР);

информационные системы ЦУАСУ перевозочным процессом, вагонным и контейнерным парками, тяговым подвижным составом (АСОУП2, ГИД «Урал ВНИИЖТ», ДИСПАРК, ДИСКОН, ДИСТПС);

АСУ пассажирскими перевозками (АСУ «Экспресс3»);

автоматизированный комплекс системы фирменного транспортного обслуживания (АКС ФТО), АС «ЭТРАН» и многие другие;

2) первичные сети на основе единой магистральной цифровой сети связи, образованные волоконно-оптическими, спутниковыми, радиорелейными и кабельными системами, узлами, линиями пере дачи и каналами информационного обмена, и вторичные сети (корпоративная сеть передачи данных (СПД), сети обще технологической, оперативнотехнологической связи), осуществляющие прием, обработку,

хранение и передачу информации ограниченного доступа, их информативные физические поля.

Основными объектами защиты информационной инфраструктуры являются:

1) объекты информационной инфраструктуры, включающие программно-технические комплексы и систему управления единой магистральной цифровой сетью связи (ЕМЦСС);

2) системы управления автоматических телефонных станций обще технологической и оперативно-технологической сетей;

3) программно-технические комплексы и система управления СПД;

4) объекты автоматизированных систем управления и информационных систем, включающие:

– отдельные АРМ и локальные вычислительные сети (ЛВС); Иерархия слоев защищаемой информационной инфраструктуры ОАО «РЖД»

– серверные сегменты информационных систем и автоматизированных систем управления; программно-технические комплексы поддержания специализированных баз данных;

– системы документооборота.

Наиболее критичными с точки зрения максимальных значений рисков являются:

– серверные сегменты информационных технологий; – АРМ информационных систем;

– ЛВС систем перевозочным процессом (ЛВС АСУ дорожных центров управления перевозками, центров управления местной работой и станциями) и сбытом грузовых перевозок;

– ЛВС АСУ финансовохозяйственной деятельностью — единой корпоративной системы управления финансами и ресурсами (ЕК АСУ ФР), АСУ трудовыми ресурсами (ЕК АСУ ТР);

– ЛВС АСУ энергетическим комплексом;

– ЛВС АСУ сбытом и организацией пассажирских перевозок; – точки подключения информационных систем железных дорог иностранных государств и сетей общего пользования;

– АРМ системы ЭТРАН при подключении внешних пользователей; – система управления и программно-технические комплексы СПД;

– система управления и программно-технические комплексы ЕМЦСС; – системы управления автоматических телефонных станций обще-технологической и оперативно-технологической сетей.

К важным объектам защиты также относятся:

1) технические, программные и программно-технические средства (включая конфигурационные данные, нормативнометодическую и другую документацию), используемые для накопления, хранения, обработки, передачи и защиты информации;

2) служебная информация средств защиты информации (идентификаторы, пароли, таблицы разграничения доступа, криптографические ключи, информация журналов аудита безопасности и др.);

3) технические средства и системы, обрабатывающие открытую информацию, но размещенные в помещениях, в которых обрабатывается (циркулирует) информация ограниченного доступа, а так же сами помещения, предназначенные для обработки такой информации; помещения, предназначенные для ведения закрытых пере говоров, а также переговоров, в ходе которых оглашаются сведения ограниченного доступа.

Наиболее критичными элементами инфраструктуры ОАО «РЖД», связанными с использованием информационных ресурсов (активов) и подлежащими защите, являются:

– рабочие места пользователей;

– серверы ОАО «РЖД» (серверы баз данных, серверы приложений, файловые серверы, почтовые серверы и др.);

– сегменты вычислительных сетей ОАО «РЖД»;

– средства обеспечения коллективной работы пользователей (базы данных, архивы электронных версий документов, система электронного документооборота, система обмена сообщениями и др.);

– узлы доступа в сети общего пользования (прежде всего, Интернет);

– каналы связи

Угрозы информационной безопасности

Виды угроз информационной безопасности ОАО «РЖД»:

1) внешние угрозы, исходящие от субъектов, не входящих в состав пользователей и обслуживающего персонала системы, разработчиков системы и не имеющих непосредственного контакта с информационными системами и ресурсами, а также от природных явлений (стихийных бедствий), катастроф;

2) внутренние угрозы, исходящие от пользователей и обслуживающего персонала системы, разработчиков системы, других субъектов, вовлеченных в информационные процессы ОАО «РЖД» и имеющих непосредственный контакт с информационными системами и ресурсами, как допущенных, так и не допущенных к информации ограниченного доступа, а также при отказах аппаратных и технических средств и сбоях программного обеспечения.

Основными источниками угроз информационной безопасности выступают отдельные злоумышленники и их сообщества, а также плохие работники ОАО «РЖД»: преступные группировки (отдельные лица), организующие проведение противозаконных акций; организации (отдельные лица), пытающиеся извлечь прибыль не законным путем за счет несанкционированного доступа к информационным ресурсам ОАО «РЖД»; работники ОАО «РЖД», преследующие корыстные цели; недобросовестные, безответственные или неквалифицированные работники ОАО «РЖД», имеющие доступ к информационным ресурсам и технологиям.

В качестве основных типов угроз безопасности информации рассматриваются:

– компрометация конфиденциальности информации;

– нарушение целостности информации, включая изменение или фальсификацию (искажение и модификацию), а также полное или частичное уничтожение информации;

– нарушение доступности информации, включая блокирование санкционированного доступа к информации авторизованных пользователей.

Главными целями атак на информационные системы ОАО «РЖД» являются получение несанкционированного доступа к информационным ресурсам и ресурсам связи и их дальнейшее скрытное незаконное использование, дезорганизация работы важнейших управляющих, информационных и телекоммуникационных систем.

Способы реализации угроз:

– несанкционированный доступ в локальные вычислительные сети, в СПД и к техническим средствам, обрабатывающим и хранящим информацию ограниченного доступа (с использованием программно-технических комплексов) с целью получения информации и дальнейшего незаконного ее использования;

– доступ в ЛВС и СПД и съем информации с каналов передачи информации с целью дальнейшего незаконного ее использования; – применение специальных средств и механизмов реализации атак (кроме программвирусов) на программно-технические комплексы и базы данных телекоммуникационных сетей, ЛВС и СПД и их систем управления с целью дезорганизации работы информационных систем;

– заражение компьютерными вирусами и внедрение других разрушающих программ с целью дезорганизации работы информационных систем; – случайное разрушение информации или порча программного обеспечения при отсутствии механизмов разграничения и ограничения доступа к информационной инфраструктуре;

– съем информации по техническим каналам утечки.

Проблема предотвращения, парирования и нейтрализации этих угроз в КИСС и обеспечения информационной безопасности корпорации решается

комплексом нормативноправовых, организационных и программно-технических (технологических) мер, методов и средств, образующих систему обеспечения информационной безопасности.

2. Принципы построения и функционирования системы управления информационной безопасностью

Система обеспечения информационной безопасности (СОИБ) ОАО «РЖД» представляет собой сложную организационнотехническую систему, предназначенную для обеспечения защиты информации и информационной инфраструктуры от воздействий, которые могут нанести неприемлемый ущерб ОАО «РЖД» за счет утраты конфиденциальности, целостности и доступности информации.

Основными целями создания и функционирования СОИБ являются:

– обеспечение защиты информации, не относящейся к категории государственной тайны;

– внедрение и эксплуатация технических подсистем, комплексов и средств обеспечения информационной безопасности;

– обеспечение доступности соответствующих категорий информации для пользователей ОАО «РЖД», других организаций и частных лиц;

– недопущение непроизводственного и непроизводительного использования ресурсов информационной инфраструктуры;

Система управления информационной безопасностью — составляющая СОИБ и часть общей системы управления, основанной на подходе, учитывающем бизнес риски, предназначенная для разработки, внедрения, применения, мониторинга, анализа, поддержания и совершенствования информационной безопасности. СУИБ становится важным компонентом системы обеспечения информационной безопасности корпорации наряду с другими компонентами — организационным, правовым и техническим обеспечением, выступающими как объекты управления. В свою очередь, в системе управления информационной безопасностью можно выделить, как

показано на рис. 1, организационную (организационно-правовую) составляющую, включающую организационную структуру, нормативнометодическую базу, и, прежде всего, корпоративный стандарт и политику информационной безопасности (ИБ), а также техническую составляющую. Существующая система управления информационной безопасностью решает задачи категорирования информации и КИСС или автоматизированных информационных и телекоммуникационных систем (АИТС) компании, формирования требований к уровню безопасности информации в АИТС, мониторинга и аудита информационной безопасности, планирования и реализации мероприятий по достижению требуемого уровня безопасности.

Рисунок 1 Составляющие системы управления информационной безопасностью ОАО "РЖД"

На основе категории системы, требуемого уровня ее защиты и соответствующего этому уровню пакета требований доверия к безопасности, с учетом известных угроз и текущей политики безопасности формируются функциональные требования безопасности. Функциональные требования безопасности определяют профиль защиты, описывающий требования по безопасности информации для конкретной информационной системы. Последующий мониторинг безопасности информации позволяет фиксировать

текущее состояние безопасности информации в соответствующем задании по безопасности. Мониторинг безопасности информации осуществляется с использованием специализированных программных комплексов. Данные о текущем состоянии информационной безопасности и рекомендации по достижению требуемого состояния позволяют производить планирование и контроль реализации мероприятий по достижению требуемого уровня безопасности. В настоящее время осуществляется дальнейшее развитие систем обеспечения и управления информационной безопасностью компании на основе сочетания рискориентированного и верификационного подходов, суть которых рассмотрена в предыдущей главе. Это обусловлено накоплением значительных и разноплановых защищаемых информационных активов и ресурсов и созданием мощной информационной инфраструктуры, включающей большое количество информационных систем и телекоммуникационных сетей, в том числе корпоративного уровня. Методологической и критериальной основой дальнейшего совершенствования СУИБ является реализация принципа «базирования на рисках», т.е. оценка и обеспечение приемлемого риска при компрометации конфиденциальности, нарушении целостности и доступности информации. Работу СОИБ (и СУИБ) курируют вицепрезидент ОАО «РЖД», а также начальник Департамента безопасности ОАО «РЖД».

Среди основных направлений формирования нормативной базы следует выделить разработку комплекса политик информационной безопасности различного уровня, профилей защиты автоматизированных систем (АС) ОАО «РЖД» и отдельных объектов информатизации, документов, обеспечивающих соблюдение режима защиты информации, составляющей коммерческую тайну, разработку регламентов взаимодействия различных информационных систем, в том числе принадлежащих внешним пользователям и разработку организационнометодических документов, регламентирующих использование информационных ресурсов. В качестве примеров нормативных актов, действующих в ОАО «РЖД», можно привести

«Перечень сведений, составляющих коммерческую тайну ОАО «РЖД», «Инструкцию о порядке обращения с информацией, составляющей коммерческую тайну ОАО «РЖД», распоряжение «Об организации работ по предотвращению записи, хранения и распространения информации и программных продуктов непроизводственного характера» с «Примерным перечнем категорий информации и программных продуктов…» и «Примерным порядком организации создания корпоративных WEBсайтов, FTP серверов, конференций…», «Порядок подключения пользователей к информационным ресурсам ОАО «РЖД», «О внедрении электрон ной цифровой подписи в ОАО «РЖД» и ряд других. Техническая составляющая СОИБ образуется организационно и/ или функционально связанными комплексами и средствами защиты. Структура технической составляющей СОИБ во многом определяется архитектурой корпоративной информационнотелекоммуникационной сети ОАО «РЖД», которая объединяет информационные ресурсы и технические средства обработки и передачи информации центрального аппарата, железных дорог и других филиалов ОАО «РЖД», дочерних и зависимых обществ ОАО «РЖД». Важнейшими техническими компонентами информационнотелекоммуникационной сети ОАО «РЖД» являются СПД и ЕМЦСС. В настоящее время введены в действие комплекс защиты системы управления ЕМЦСС и комплекс защиты СПД магистрального и дорожного уровней, обеспечивающие регистрацию, учет и целостность программного обеспечения и обрабатываемой информации, разграничение доступа к ресурсам, аудит событий безопасности и обнаружение вторжений.

2.1 Принципы построения и функционирования системы управления информационной безопасностью

Задачи и принципы управления информационной безопасностью ОАО «РЖД»

Деятельность по управлению информационной безопасностью ОАО «РЖД» направлена на обеспечение безопасности (конфиденциальности,

целостности и доступности) информации и объектов информационной инфраструктуры, а также на сохранение единства информационного пространства ОАО «РЖД». Она реализуется в рамках развиваемой системы управления информационной безопасностью. СУИБ предназначена для разработки, внедрения, применения, мониторинга, анализа, поддержания и совершенствования информационной безопасности ОАО «РЖД». Она включает организационную структуру, нормативнометодическую базу информационной безопасности (корпоративный стандарт, политика информационной безопасности, положения, руководства, методики, регламенты, инструкции, процедуры), процессы, информационные, технические и другие ресурсы. Важным шагом по совершенствованию СУИБ стала разработка и утверждение корпоративного стандарта «Управление информационной безопасностью. Общие положения» СТО РЖД 1.18.0022009. Данный стандарт базируется на положениях стандартов ГОСТ Р ИСО/МЭК 154082008, ГОСТ Р ИСО/МЭК 177992005, ГОСТ Р ИСО/МЭК 270012006, ГОСТ Р ИСО/МЭК ТО 133352006, принципах Политики корпоративной информатизации ОАО «РЖД» и определяет основные принципы и общие требования к управлению информационной безопасностью и организационную структуру СУИБ ОАО «РЖД». В процессе управления информационной безопасностью ОАО «РЖД» в рамках СУИБ решаются следующие задачи:

1) выполнение требований законодательства и нормативных документов уполномоченных в области обеспечения ИБ государственных органов;

2) обеспечение информационной безопасности ОАО «РЖД» при обработке и использовании информационных активов ОАО «РЖД»;

3) определение информационных активов ОАО «РЖД», подлежащих защите;

4) определение категорий автоматизированных информационных и телекоммуникационных систем и информационных активов ОАО «РЖД» с целью определения приоритетов и требуемых уровней защиты информации;

5) анализ уязвимостей, построение моделей нарушителей и угроз безопасности информационных активов ОАО «РЖД»;

6) анализ и оценка рисков нарушения информационной безопасности АИТС и информационных активов ОАО «РЖД»;

7) разработка моделей защиты АИТС и информационных активов ОАО «РЖД»;

8) формирование требований безопасности информационных активов ОАО «РЖД», предъявляемых к АИТС ОАО «РЖД»;

9) определение направлений обеспечения информационной безопасности АИТС ОАО «РЖД»;

В процессе управления информационной безопасностью устанавливаются следующие принципы управления информационной безопасностью ОАО «РЖД».

1. Законность — соответствие правовым нормам.

2. Достаточность и нормирование защиты — реализация технически и экономически обоснованных уровней ИБ и мер защиты.

3. Базирование на рисках — выбор уровня ИБ, требований и мер ИБ основывается на результатах анализа и оценки рисков реализации угроз безопасности информационным активам ОАО «РЖД».

4. Надежность — сохранение безопасного состояния в случае сбоев АИТС.

5. Соразмерность затрат на защиту — затраты на обеспечение ИБ не должны превышать величину возможного ущерба, связанного с нарушением ИБ.

6. Простота — меры и механизмы обеспечения ИБ должны быть насколько это возможно, простыми.

7. Контроль доступа (управление доступом) — доступ к информации должен осуществляться только с использованием средств, реализующих политику разграничения доступа.

8. Открытость — безопасность АИТС ОАО «РЖД» не должна зависеть от мер по ограничению доступа к информации относительно реализации компонентов соответствующих систем обеспечения ИБ.

9. Разделение привилегий (прав) — функции безопасности АИТС, используемых в ОАО «РЖД», должны быть разделены между подсистемами их реализующими;

роли администраторов, операторов и пользователей системы должны быть разделены между персоналом ОАО «РЖД».

10. Приемлемость — пользователи АИТС должны осознавать необходимость в обеспечении ИБ, а также участвовать в регулярных тренировках и проходить обучение по вопросам организации ИБ. Реализованные механизмы ИБ не должны быть излишне обременительными для пользователей.

11. Многоуровневая защита — механизмы, обеспечивающие ИБ, должны применяться на нескольких уровнях защиты таким образом, что компрометация одного механизма безопасности не являлась бы достаточным условием компрометации конкретной АИТС, какойлибо ее части или других АИТС ОАО «РЖД».

12. Регистрация нарушений безопасности — нарушения ИБ АИТС ОАО «РЖД» должны регистрироваться в соответствующих электронных журналах. На основе анализа этой информации должен обеспечиваться возврат АИТС в безопасное состояние, производиться определение уязвимостей АИТС и способов нападения, использованных нарушителем, а также выявляться и привлекаться к ответственности нарушители.

13. Непрерывность защиты — обеспечение ИБ производится на всех стадиях и этапах жизненного цикла АИТС.

14. Периодическая оценка — требования и меры по обеспечению ИБ периодически контролируются, пересматриваются и пере оцениваются на основе следующих принципов: объективности, бес пристрастности, воспроизводимости, корректности, достаточности.

Жизненный цикл и требования к СУИБ ОАО «РЖД»

Основное требование состоит в том, что с учетом видов деятельности ОАО «РЖД» и на основе управления рисками должна быть разработана, внедрена, применяться на постоянной основе, подвергаться мониторингу и периодическому анализу, поддерживаться в работоспособном состоянии и совершенствоваться СУИБ . Функционирование СУИБ ОАО «РЖД» должно обеспечивать выполнение в ОАО «РЖД» требований законодательства Российской Федерации в сфере защиты информации и выявление нарушений безопасности критически важных АИТС и информационных активов ОАО «РЖД». Жизненный цикл СУИБ носит циклический характер и предусматривает реализацию следующих основных групп процессов:

1) разработка (модернизация) элементов СУИБ;

2) внедрение и применение элементов СУИБ;

3) мониторинг и анализ реализованных элементов СУИБ;

4) поддержание и, при необходимости, принятие решения о совершенствовании элементов СУИБ. В процессе разработки СУИБ ОАО «РЖД» должны быть:

а) определена область применения и границы СУИБ с учетом характеристик деятельности структуры, активов и технологий ОАО «РЖД»;

б) разработана Политика информационной безопасности;

в) установлен подход ОАО «РЖД» к анализу и оценке рисков нарушения ИБ, включающий: методы инвентаризации и оценки значимости (категорирования) информационных активов и АИТС;

методы исследования и представления угроз нарушения ИБ и характеристик вероятных нарушителей;

методы анализа и оценки рисков; критерии принятия рисков и допустимых уровней рисков;

г) проанализированы и оценены риски нарушения ИБ:

оценено влияние нарушений ИБ на деятельность ОАО «РЖД»;

оценены вероятность реализации угроз ИБ и связанный с этим ущерб (влияние нарушений ИБ на деятельность ОАО «РЖД»);

проанализированы реализованные в текущее время меры обеспечения ИБ;

определены уровни рисков реализации угроз ИБ;

определены недопустимые риски, требующие обработки (уменьшения, устранения);

д) определены и оценены варианты обработки (уменьшения, устранения) рисков, включающие:

применение мер обеспечения ИБ;

принятие рисков, при условии их соответствия установленным критериям принятия рисков;

перенос соответствующих рисков на третьи стороны (например, страховщиков, поставщиков и др.);

е) для обработки (уменьшения, устранения) рисков выбраны меры обеспечения ИБ;

ж) получена санкция руководства ОАО «РЖД» на предполагаемые остаточные риски;

з) получена санкция руководства ОАО «РЖД» на внедрение и применение СУИБ и ее элементов. В процессе внедрения и применения СУИБ ОАО «РЖД» или ее со ставных частей необходимо:

а) разработать план обработки рисков, который определяет действия, ресурсы (включая финансирование), обязанности и приоритеты управления рисками ИБ;

б) реализовать план обработки рисков;

в) реализовать выбранные меры обеспечения ИБ;

г) определить способ измерения (оценки) эффективности (результативности) выбранных мер обеспечения ИБ;

д) внедрить программы подготовки и осведомления персонала ОАО «РЖД» по вопросам ИБ;

е) управлять работой (функционированием) СУИБ; ж) управлять ресурсами для СУИБ;

з) реализовать процедуры и другие меры, позволяющие оперативно регистрировать события, относящиеся к ИБ, и реагировать на инциденты, относящиеся к ИБ. В процессе мониторинга и анализа СУИБ необходимо:

а) осуществлять мониторинг и анализ процедур и других мер обеспечения и управления ИБ в целях: своевременного определения нарушений и несоответствия требованиям ИБ; контроля эффективности реализованных мер и средств обеспечения ИБ; своевременного определения неудавшихся и успешных попыток нарушений и инцидентов, относящихся к ИБ; предоставления возможности руководству ОАО «РЖД» определять, выполняются ли таким образом, как ожидалось, действия, порученные должностным лицам или реализуемые информационными технологиями; оказания помощи в регистрации событий, относящихся к ИБ, и, таким образом, предотвращения инцидентов, относящихся к ИБ; определения, были ли эффективны действия, предпринятые для устранения на рушений ИБ;

б) проводить анализ эффективности СУИБ (включая соответствие политике ИБ и целям СУИБ), а также анализ мер обеспечения ИБ, принимая во внимание результаты аудита (мониторинга, контроля и оценки) ИБ, инциденты, относящиеся к ИБ, предложения и рекомендации всех заинтересованных сторон (руководства, пользователей, регулирующих органов, экспертов по ИБ, специализированных организаций по ИБ);

в) оценивать эффективность мер обеспечения и управления ИБ для подтверждения того, что требования ИБ были выполнены;

г) периодически анализировать и пересматривать организацию оценки рисков, а также остаточные риски и установленные допустимые

(приемлемые) уровни рисков, принимая во внимание про исходящие изменения в структуре ОАО «РЖД», бизнесцелях и бизнеспроцессах, используемых информационных технологиях, составе угроз ИБ, составе реализованных мер обеспечения и управления ИБ, в правовой и регулирующей системе, контрактных обязательствах и в социальной сфере;

д) проводить внутренний аудит (контрольные проверки) СУИБ (и ее составных частей) через запланированные промежутки времени, а также (при необходимости) — внепланово;

е) проводить на регулярной основе анализ направлений совершенствования СУИБ;

ж) обновлять (корректировать) планы обеспечения ИБ с учетом результатов мониторинга и деятельности по внутреннему аудиту; з) регистрировать действия и события, которые могут оказывать влияние на эффективность и характеристики СУИБ (или ее составных частей).

Реализация мониторинга ИБ СУИБ ОАО «РЖД» должна осуществляться по следующим направлениям:

1) оперативный мониторинг (мониторинг событий, относящихся к ИБ в АИТС ОАО «РЖД»);

2) мониторинг состояния (оценка соответствия текущего состояния ИБ АИТС ОАО «РЖД» уровню ИБ, определенному требованиями ИБ);

3) контрольные проверки (контроль достигнутого уровня ИБ АИТС ОАО «РЖД»).

В процессе сопровождения (поддержания и совершенствования) СУИБ ОАО «РЖД» необходимо:

а) планировать и осуществлять доработку СУИБ ОАО «РЖД» или ее составных частей;

б) предпринимать соответствующие корректирующие действия, учитывая при этом опыт в области ИБ ОАО «РЖД» и других организаций;

в) сообщать о предпринятых действиях и доработках СУИБ всем заинтересованным сторонам;

г) контролировать достижение целей совершенствования СУИБ.4.3.3. Мероприятия по управлению информационной безопасностью, подлежащие реализации в ОАО «РЖД» К мероприятиям управления ИБ, подлежащим реализации в ОАО «РЖД», относятся следующие: – активная поддержка процессов ИБ со стороны руководства ОАО «РЖД»;

– координация деятельности, связанной с ИБ;

– четкое распределение и разделение обязанностей, связанных с ИБ;

– инвентаризация всех значимых информационных активов;

– оценка значимости и категорирование информационных активов и АИТС;

– эффективная организация информационных активов и АИТС как объектов ИБ;

– анализ уязвимостей, формирование перечней угроз и характеристик вероятных нарушителей;

– анализ и оценка рисков нарушения ИБ;

– эффективное проектирование мер, средств и систем обеспечения ИБ;

– документирование должностных обязанностей персонала, связанных с ИБ;

– проведение регулярного обучения персонала в области ИБ;

– определение мер дисциплинарного характера к нарушителям ИБ;

– проведение предупредительных мероприятий при увольнении сотрудников ОАО «РЖД»;

– физическая защита средств хранения и обработки информации;

– резервирование электропитания для критичных ресурсов;

– защита (контроль) кабелей электропитания и телекоммуникационных кабелей; – надлежащее регламентное обслуживание оборудования;

– контроль за перемещением оборудования;

– надлежащее документирование эксплуатационных процедур;

– разделение средств разработки, средств тестирования и эксплуатируемых средств обработки информации;

– мониторинг производительности ресурсов АИТС и поддержание необходимых эксплуатационных характеристик АИТС в случаях их масштабирования;

– контроль за включением в АИТС новых средств обработки информации, а также за модификацией (заменой) используемых;

– применение надлежащих методов идентификации и аутентификации;

– разграничение доступа пользователей к ресурсам АИТС и документирование процедур предоставления доступа пользователей к ресурсам АИТС;

– защита от компьютерных вирусов и вредоносного программного обеспечения;

– осуществление регламентного резервного копирования ин формации;

– реализация мер управления ИБ в вычислительных сетях;

– защита передаваемой информации; – реализация надлежащих процедур управления съемными носителями информации.

3. Организационная структура и нормативная база обеспечения и управления информационной безопасностью

Организационная структура управления информационной безопасностью ОАО «РЖД» представлена на рис. 2 и включает:

1) Президента ОАО «РЖД»;

2) вицепрезидента ОАО «РЖД», курирующего вопросы обеспечения ИБ ОАО «РЖД»;

3) Комитет по информационной безопасности ОАО «РЖД»;

4) Департамент безопасности ОАО «РЖД»;

5) Департамент информатизации и корпоративных процессов управления ОАО «РЖД»;

6) департаменты и управления ОАО «РЖД» — функциональных заказчиков автоматизированных систем управления;

7) подразделения защиты информации Региональных центров безопасности — структурных подразделений ОАО «РЖД»;

8) подразделения информационной безопасности ГВЦ и ИВЦ — структурных подразделений ГВЦ;

9) подразделения и работников, организующих работу по защите информации филиалов ОАО «РЖД».

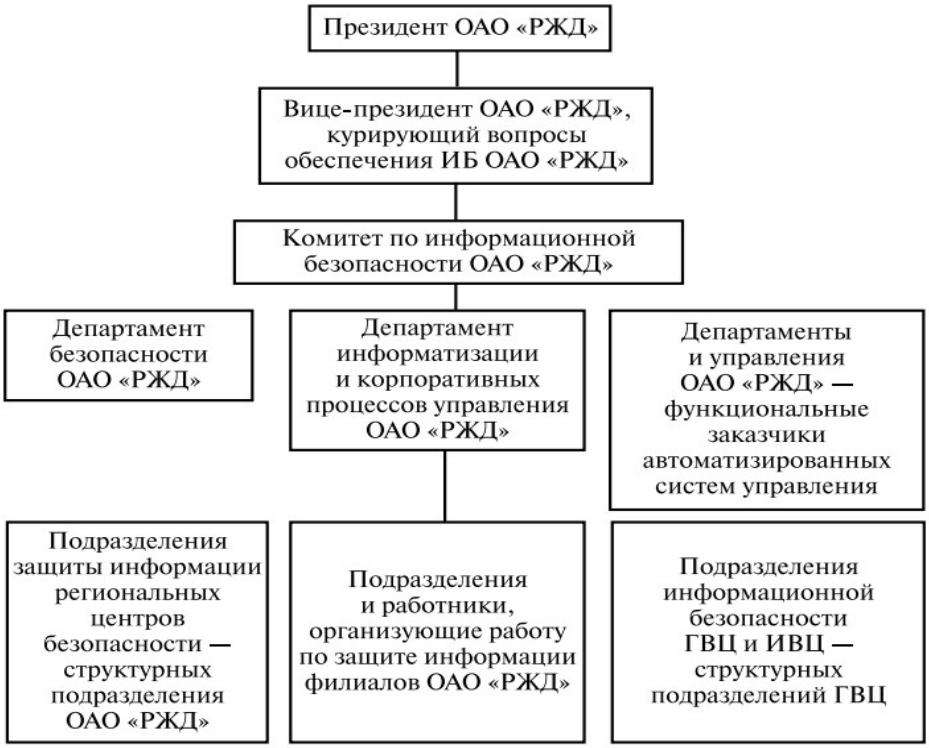

Рисунок 2 Организационная структура управления информационной безопасностью ОАО "РЖД"

Комитет по информационной безопасности (коллегиальный со вещательный орган ОАО «РЖД» по вопросам управления информационной безопасностью) решает следующие задачи: – поддержка корпоративной стандартизации в области ИБ;

– обеспечение реформирования СУИБ ОАО «РЖД»;

– контроль за выполнением настоящего стандарта и Политики ИБ ОАО «РЖД»;

– координация деятельности подразделений ОАО «РЖД» в области корпоративной информатизации в части учета требований ИБ.

Руководит работой Комитета по информационной безопасности вицепрезидент ОАО «РЖД», курирующий вопросы обеспечения ИБ ОАО «РЖД».

Организационная структура и взаимосвязи подразделений защиты информации дорожного уровня приведена на рис. 3.

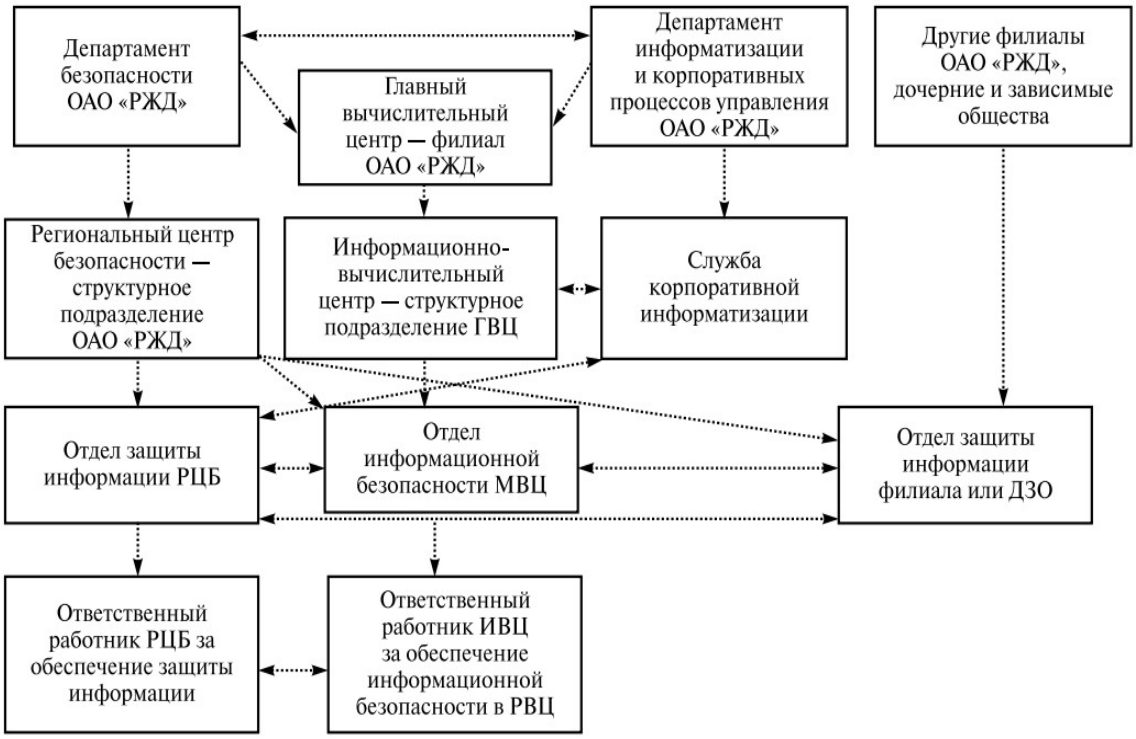

Рисунок 3 Структура и взаимодействие структурных подразделений защиты информации региона ведения железной дороги

На Департамент безопасности ОАО «РЖД» возлагается организация следующих работ:

– разработка нормативнометодической базы ИБ АИТС ОАО «РЖД», включая требования к конкретным АИТС и типам АИТС ОАО «РЖД»;

– внедрение нормативнометодической базы ИБ в практику деятельности структурных подразделений и предприятий ОАО «РЖД»;

– организация разработки и внедрения систем обеспечения ИБ АИТС ОАО «РЖД»;

– организация обучения персонала по вопросам ИБ;

– мониторинг ИБ АИТС ОАО «РЖД»;

– планирование и формирование заявок на выделение финансирования в части решения задач по обеспечению ИБ ОАО «РЖД»;

– подготовка предложений по совершенствованию СУИБ и от дельных систем обеспечения ИБ АИТС ОАО «РЖД»;

– участие в формировании организационной структуры СУИБ ОАО «РЖД»;

– согласование предлагаемых решений по обеспечению ИБ АИТС.

4. Корпоративные политики информатизации и информационной безопасности

Распоряжением Президента ОАО «РЖД» от 11 сентября 2006 г. № 1872р утверждена Политика корпоративной информатизации ОАО «РЖД» и среднесрочная программа мероприятий по ее реализации [2]. Напомним, что в данном документе корпоративная информатизация определена как комплекс мер, направленных на совершенствование информационных технологий и информационно-вычислительных систем ОАО «РЖД».

Цель: создание оптимальных условий для достижения стратегических целей, сохранения информационной целостности и безопасности компании и ее подразделений, эффективной поддержки реформирования ОАО «РЖД».

Политика корпоративной информатизации ОАО «РЖД» определяет следующие принципы организации корпоративной информатизации:

- системный и комплексный подход;
- обеспечение единого информационного пространства;
- обеспечение информационной целостности и безопасности, в том числе непрерывности ИТсервисов;
- применение передовых и перспективных решений и технологий;
- адекватное решаемым задачам организационноправовое обеспечение;

- использование лучших мировых практик в области ИТ;
- применение проектных принципов;
- стандартизация и унификация применяемых технологий, программного и аппаратного обеспечения.

Основные задачи обеспечения информационной безопасности АИТС дорожного уровня:

–определение информационных активов, подлежащих защите в АИТС;

– категорирование информационных активов и классификация АИТС в соответствии с приоритетами и требуемым уровнем защиты информации;

– анализ уязвимостей, прогнозирование и выявление внутренних и внешних угроз информационной безопасности, оценка защищенности АИТС;

– определение необходимых параметров, характеризующих величину рисков информационной безопасности;

– защита от несанкционированного вмешательства в процесс функционирования АИТС дорожного уровня;

– разграничение полномочий и ответственности СПДУ, РЦБ, ИВЦ, НКИ других подразделений, обеспечивающих процесс функционирования и защиту АИТС;

– защита данных, обрабатываемых и хранимых в АИТС, пере даваемых по каналам связи, от несанкционированного доступа, позволяющего произвести ознакомление, модификацию, фальсификацию или уничтожение данных;

– контроль целостности операционной среды исполнения прикладных программ (решения прикладных задач) и программных средств, восстановление их целостности в случае нарушения;

Основными способами реализации угроз ИБ являются:

– несанкционированный доступ (в том числе с использованием программно-технических средств) в АИТС дорожного уровня, а также к ее техническим средствам и информационным активам;

– перехват информации в сторонних и собственных сетях передачи данных СПДУ; – применение специальных средств, программно-технических алгоритмов и процедур проведения атак по отношению к АИТС дорожного уровня;

– несанкционированное использование зарегистрированным пользователем АИТС программных продуктов доступа и администрирования, не входящих в состав ПО, инсталлированного на его рабочем месте установленным порядком;

– внедрение (в том числе непреднамеренное) в АИТС дорожного уровня компьютерных вирусов и другого вредоносного программного обеспечения (троянские программы, программы«шпионы» и пр.);

– разрушение или порча информационных активов СПДУ при отсутствии (или ненадлежащей настройке) соответствующих механизмов защиты и управления доступом к АИТС дорожного уровня и обрабатываемой в них информации;

– перехват информации по техническим каналам;

– несанкционированное включение средств электронно-вычислительной техники, подключенных к АИТС, в локальные или корпоративные сети других организаций, а также во внешние информационные системы и сети, включая сеть Интернет;

– использование общедоступных незащищенных ресурсов и сервисов для передачи защищаемой информации.

Источники угроз ИБ делятся на три основных класса:

1) источники, связанные с действиями людей — внешние и внутренние нарушители;

2) источники, связанные с ненадежностью аппаратных средств, моральным старением и наличием ошибок в программном обеспечении;

3) источники, связанные с природными явлениями (стихийными бедствиями) и неблагоприятными техногенными факторами.

В качестве внешних нарушителей ИБ могут рассматриваться:

– лица, не входящие в состав пользователей и обслуживающего персонала, автоматизированных и информационных систем дорожного уровня, и являющиеся, например, разработчиками этих систем, пользователями систем, сопряженных с АИТС дорожного уровня, работниками организаций, предоставляющих СПДУ услуги на условиях аутсорсинга, пользователи сетей общего пользования (например, сеть Интернет), которым предоставлен доступ к АИТС дорожного уровня.

– преступные группировки (или отдельные лица), организующие проведение противозаконных акций в отношении информационных активов АИТС дорожного уровня;

– организации (или отдельные лица), пытающиеся извлечь прибыль (выгоду) незаконным путем за счет несанкционированного доступа к информационным активам СПДУ или преследующие иные цели.

В качестве потенциальных внутренних нарушителей ИБ могут рассматриваться пользователи и обслуживающий персонал АИТС дорожного уровня, другие субъекты (лица), вовлеченные в информационные процессы АИТС. Для минимизации угроз от потенциальных внутренних нарушителей ИБ должны проводиться соответствующие мероприятия при заключении трудовых договоров (контрактов), допуске работников к сведениям конфиденциального характера, при переводе работника на другую должность, при выходе работника в долгосрочный отпуск и прекращении трудового договора. Детально рассматриваются методы реализации

5. Методики оценки значимости информационных ресурсов и безопасности информации и система оценки защищенности автоматизированных информационных и телекоммуникационных систем

В ОАО «РЖД» разработан и утвержден ряд методик: методика оценки значимости информационных ресурсов, методики анализа и оценки текущего состояния безопасности информации в системах ОАО «РЖД» и другие. Здесь

рассмотрим содержание одной из них — Методики оценки значимости информационных ресурсов ОАО «РЖД» (Методика).

Цель данной Методики — обеспечить возможность оценки значимости характеристик (факторов) безопасности (конфиденциальности, целостности, доступности и любых других) каждого вида (подвида) информации для достижения целей функционирования ОАО «РЖД» [10].

В состав исходных данных должна быть включена, как минимум, следующая информация:

1) перечень основных целей функционирования ОАО «РЖД»;

2) перечень основных видов деятельности ОАО «РЖД»;

3) перечень основных видов информации ОАО «РЖД».

Для проведения оценки значимости информации в соответствии с выбранными критериями — факторами безопасности — требуется определение полного списка информационных активов (ресурсов), представляющих ценность для компании.

В состав экспертной группы должны входить управленческий персонал разных уровней;

специалисты по основным видам деятельности ОАО «РЖД»;

представители структурных подразделений ОАО «РЖД» — пользователей основных видов информации;

специалисты по информационным технологиям; специалисты по защите информации.

Применение Методики позволит ранжировать виды информации ОАО «РЖД» по степени значимости каждого связанного с ними фактора безопасности на достижение целей функционирования ОАО «РЖД» и получить оценку значимости (высокая/средняя/ низкая) всех факторов безопасности для данного вида (подвида) ин формации.

Основными этапами метода являются:

1) определение проблемы, которую необходимо решить (в данном случае — оценка видов информации, исходя из значимости их факторов безопасности для достижения целей функционирования организации);

2) построение иерархии — декомпозиция проблемы на простые составляющие: от проблемы через промежуточные составляющие к самому нижнему уровню — перечню простых альтернатив (в данном случае — факторам безопасности видов информации);

3) последовательная (для каждого уровня иерархии) оценка важности элементов (альтернатив) с помощью метода парных сравнений;

4) последовательная (для каждого уровня иерархии) оценка локальных приоритетов сравниваемых элементов (альтернатив);

5) проверка согласованности локальных приоритетов (расчет значений коэффициентов согласованности и их сравнение с пороговым значением);

6) иерархический синтез решения проблемы (в данном случае — получение оценки каждого вида информации в значимости отдельных факторов безопасности для достижения глобальной цели функционирования организации). Приведем описание шагов оценивания в соответствии с Методикой для первых двух этапов.

1. Определение глобальной цели функционирования организации. Глобальная цель функционирования организации должна отражать общую направленность ее деятельности (и ожидаемые при этом результаты). При формулировании глобальной цели нет необходимости в ее излишней детализации. Это может быть просто высоко уровневое декларативное заявление, например, «Обеспечение потребности государства, юридических и физических лиц в железно дорожных перевозках, работах и услугах, оказываемых железнодорожным транспортом, а также извлечение прибыли».

2. Определение подцелей функционирования организации. При выполнении данного шага оценивания необходимо сформулировать подцели функционирования организации, влияющие на глобальную цель. Подцели функционирования организации должны (по возможности) представлять

собой полное множество подцелей, от достижения которых зависит достижение глобальной цели функционирования организации. Они могут быть представлены видами деятельности организации.

3. Определение видов информации, используемой в организации. При выполнении данного шага оценивания необходимо выделить виды (если необходимо, выделить подвиды) информации, используемые при функционировании организации. Перечень видов информации должен, как минимум, охватывать всю информацию, составляющую коммерческую тайну организации и персональные данные, но не ограничиваться ею. Он должен охватывать программное, лингвистическое, информационное обеспечение, справочную, технологическую и другую вспомогательную информацию.

4. Определение факторов безопасности видов информации. При выполнении данного шага оценивания необходимо определить факторы безопасности видов информации как основы для оценки видов информации. В качестве факторов безопасности, используемых для оценки видов информации, можно определить любые ее характеристики безопасности (конфиденциальность, целостность, доступность, достоверность, подлинность или любые другие).

5. Построение иерархии, предназначенной для оценки значимости факторов безопасности рассматриваемых видов информации:

1) На первый (верхний) уровень иерархии поместить глобальную цель функционирования организации, которая должна соответствовать глобальной цели, определенной на шаге 1. При построении дерева иерархии необходимо использовать обозначение глобальной цели, принятое на этом шаге.

2) На второй уровень иерархии (уровень критериев сравнения) поместить подцели функционирования организации (виды деятельности). Подцели должны соответствовать подцелям, определенным на шаге 2. При построении дерева иерархии необходимо использовать обозначение подцелей, принятое на этом шаге. Соединить направленной связью каждую

подцель (вид деятельности) с глобальной целью функционирования организации.

3) Аналогично (если необходимо) можно определить любые другие промежуточные уровни иерархии. Пример иерархии для последующей оценки значимости факторов безопасности рассматриваемых видов информации

4) На следующий уровень иерархии (уровень критериев сравнения) поместить виды (при необходимости подвиды) информации, которые должны соответствовать видам информации, определенным на шаге 3. При построении дерева иерархии необходимо использовать обозначение видов информации, принятое на шаге 3. Соединить направленной связью виды информации с подцелями (видами деятельности), при достижении которых они используются, а подвиды информации — с соответствующими видами информации.

5) На нижний уровень иерархии (уровень альтернатив) поместить факторы безопасности видов (подвидов) информации. Факторы безопасности видов (подвидов) информации должны соответствовать факторам безопасности, определенным на шаге 4. При построении дерева иерархии необходимо использовать обозначение факторов безопасности, принятое на шаге 4.

5.1 Система оценки защищенности автоматизированных информационных и телекоммуникационных систем

ОАО «РЖД» Оценка защищенности АИТС дорожного уровня осуществляется с использованием Системы оценки защищенности автоматизированных информационных и телекоммуникационных систем ОАО «РЖД» (СОЗ), а также других систем, направленных на решение задач по оценке защищенности АИТС . Методологическим обеспечением СОЗ является использование технических регламентов Российской Федерации, стандартов информационной безопасности, руководящих документов ФСТЭК России, ФСБ России и иных нормативных документов; концепций,

политик и регламентов обеспечения информационной безопасности ОАО «РЖД»; методик оценки защищенности информационных активов, категорирования автоматизированных систем (АС), анализа рисков безопасности, формирования требований безопасности, проектирования АС в защищенном исполнении, оценки и контроля состояния информационной безопасности АС. СОЗ обеспечивает реализацию следующих функций:

– автоматизированный сбор и централизованную обработку информации о состоянии, параметрах и характеристиках информационной безопасности АИТС дорожного уровня различного состава и назначения;

– автоматизированное тестирование и анализ защищенности АИТС дорожного уровня в соответствии с заданными планами, параметрами, шаблонами и регламентами тестирования;

– проведение в автоматизированном режиме различных оценок выполнения требований ИБ, предъявляемых к АИТС дорожного уровня;

– автоматизации учета выявленных нарушений информационной безопасности АИТС дорожного уровня и принятых мер по их устранению;

– автоматизации аналитической деятельности подразделений, обеспечивающих информационную безопасность АИТС дорожного уровня по оценке состояния уровня ИБ АИТС дорожного уровня, и выработки обоснованных предложений и сбалансированных планов совершенствования ИБ АИТС.