ОРГАНИЗАЦИЯ СОТРУДНИЧЕСТВА ЖЕЛЕЗНЫХ ДОРОГ (ОСЖД)

III издание

Разработано: экспертами ОАО «РЖД» и Постоянной рабочей группы ОСЖД по кодированию и информатике (ПРГ КИ) в 2015 г.

Согласовано совещанием экспертов ПРГ КИ в 2015 г.

Утверждено итоговым совещанием ПРГ КИ 17-19 ноября 2015 г.

Дата вступления в силу: 19 ноября 2015 г.

Примечание: Теряет силу II издание от 01.07.2009 г.

Р 941-1

ПРИНЦИПЫ ОРГАНИЗАЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ВЗАИМОДЕЙСТВИИ ЦИФРОВЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ СВЯЗИ

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

ИБ	–	информационная безопасность
ИР	–	информационные ресурсы
ИТИ	–	информационно-телекоммуникационная инфраструктура
ОСЖД	–	Организация сотрудничества железных дорог
СОИБ	–	система обеспечения информационной безопасности
ЦТСС	–	цифровая телекоммуникационная сеть связи

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Для защиты информационных ресурсов и информационно-телекоммуникационной инфраструктуры (далее – ИР и ИТИ) железнодорожных предприятий при взаимодействии цифровых телекоммуникационных сетей связи (далее – ЦТСС) государств-членов ОСЖД в международном сообщении для каждого предприятия требуется построение системы обеспечения информационной безопасности (СОИБ) на основе совместного применения правовых, организационных и технических мер.

Целью настоящей Памятки является определение основных принципов и установление унифицированных требований к комплексу организационных и технических мероприятий при взаимодействии ЦТСС железнодорожных предприятий государств-членов ОСЖД в международном сообщении (далее – железнодорожных предприятий).

1.2. Основными принципами организации защиты информации при взаимодействии ЦТСС железнодорожных предприятий государств-членов ОСЖД являются:

- соответствие международным стандартам, законодательству, национальным стандартам и нормативным документам по защите информации государств-членов ОСЖД;
- организация защиты информации в ЦТСС в рамках системы управления информационной безопасностью железнодорожного предприятия;
- унифицированный подход к построению системы управления информационной безопасностью, обеспечивающий взаимное доверие железнодорожных предприятий к защите информации при взаимодействии ЦТСС;
- технологическая совместимость СОИБ ЦТСС железнодорожных предприятий в части механизмов и процедур защиты информации при взаимодействии ЦТСС;
- администрирование ЦТСС и СОИБ ЦТСС в границах железнодорожных администраций государств-членов ОСЖД;
- мониторинг и контроль защищенности ЦТСС, выявление и реагирование на инциденты информационной безопасности во взаимосогласованных границах на основе двухсторонних соглашений.

1.3. Определенные в п. 1.2 принципы организации защиты информации должны учитываться при разработке:

- политик информационной безопасности при взаимодействии ЦТСС железнодорожных предприятий;
- требований к организационным и техническим мерам защиты (профилей защиты) ИР и ИТИ железнодорожных предприятий;
- правовых и организационных мероприятий, регламентирующих вопросы

обеспечения информационной безопасности при взаимодействии ЦТСС железнодорожных предприятий государств–членов ОСЖД;

- организационных и технических мер защиты информации ЦТСС железнодорожных предприятий государств–членов ОСЖД при взаимодействии.

1.4. При разработке Памятки использованы документы:

- ИСО/МЭК 15408-1 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель» (ISO/IEC 15408-1 Information Technologies – Security Techniques – Evaluation Criteria for IT Security – Part 1: Introduction and General Model);
- ИСО/МЭК 15408-2 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности» (ISO/IEC 15408-2 Information Technologies – Security Techniques – Evaluation Criteria for IT Security – Part 2: Security Functional Components);
- ИСО/МЭК 15408-3 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности» (ISO/IEC 15408-3 Information Technologies – Security Techniques – Evaluation Criteria for IT Security – Part 3: Security Assurance Components);
- ИСО/МЭК 27001 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» (ISO/IEC 27001 Information Technology – Security Techniques – Information security management systems – Requirements);
- ИСО/МЭК 27002 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» (ISO/IEC 27002 Information technology — Security techniques — Code of practice for information security management);
- ИСО/МЭК 27005 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» (ISO/IEC 27005 Information technology. Security techniques. Information security risk management);
- ИСО/МЭК ТО 19791 «Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем» (ISO/IEC TR 19791 Information Technology – Security Techniques – Security assessment of operational systems);
- ИСО/МЭК 27033-1 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и

концепции» (ISO/IEC 27033-1 Information Technology – Security Techniques – Network Security – Part 1: Overview and concepts);

- ИСО/МЭК 27033-2 «Информационные технологии. Методы и средства обеспечения защиты. Защита сети. Часть 2. Руководящие указания по проектированию и внедрению защиты сети» (ISO/IEC 27033-2 Information Technology – Security Techniques – Network Security – Part 2: Guidelines for the design and implementation of network security).

2 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Анализ рисков – систематическое определение и анализ актуальных угроз безопасности информации, реализация которых может привести к нарушению безопасности информации, и возможного ущерба железнодорожным предприятиям ОСЖД и предоставление руководству железнодорожных предприятий ОСЖД информации, необходимой для принятия решений, связанных с оптимизацией капиталовложений в меры по обеспечению информационной безопасности.

Анализ уязвимостей – мероприятия по выявлению, идентификации и оценке уязвимостей ИР и ИТИ для определения возможности реализации угроз безопасности информации и способов предотвращения ущерба.

Аудит – периодический независимый и документированный процесс получения объективной оценки состояния ИР и элементов ИТИ с целью определения степени выполнения в организации установленных требований по обеспечению информационной безопасности.

Защита информации – технологические и административные процедуры, меры защиты информации, применяемые к ИР и ИТИ и направленные на исключение:

неправомерных доступа, копирования, предоставления или распространения информации (обеспечение конфиденциальности информации);

неправомерных уничтожения или модифицирования информации (обеспечение целостности информации);

неправомерного блокирования информации (обеспечение доступности информации).

Конфиденциальность: свойство безопасности информации, при котором доступ к ней осуществляют только субъекты доступа, имеющие на него право.

Целостность: свойство безопасности информации, при котором отсутствует любое ее изменение либо изменение осуществляется субъектами доступа, имеющими на него право.

Доступность: свойство безопасности информации, при котором субъекты доступа, имеющие права доступа, могут беспрепятственно их реализовать.

Информационная безопасность (ИБ)	–	состояние защищенности информации, при котором обеспечиваются такие ее характеристики, как конфиденциальность, целостность и доступность.
Информационные ресурсы (ИР)	–	совокупность данных, представляющих ценность для организации и выступающих в качестве материальных ресурсов.
Информационно-телекоммуникационная инфраструктура (ИТИ)	–	совокупность автоматизированных систем управления, информационных систем, сетей связи и передачи данных, обеспечивающих совместное функционирование и информационное взаимодействие железнодорожных предприятий в международном сообщении.
Инцидент информационной безопасности	–	непредвиденное или нежелательное событие (группа событий) безопасности, которое привело (могут привести) к нарушению функционирования информационной системы или возникновению угроз безопасности информации (нарушению конфиденциальности, целостности, доступности).
Контролируемая зона	–	пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, а также транспортных, технических или иных средств.
Конфиденциальная информация	–	информация ограниченного доступа, на распространение которой в соответствии с законодательством государства или в соответствии с коммерческим интересом железнодорожного предприятия накладываются ограничения.
Несанкционированный доступ	–	доступ к информации, нарушающий правила разграничения доступа к ИР и ИТИ.
Политика безопасности	–	совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация (в частности – железнодорожное предприятие) в своей деятельности.
Система обеспечения информационной безопасности ЦТСС	–	совокупность правовых, организационных и технических мероприятий, служб безопасности, и механизмов и мер защиты, органов управления и исполнителей, направленных на предотвращение или существенное затруднение нанесения ущерба пользователю и владельцу ЦТСС (соответствующему железнодорожному предприятию).

Служба безопасности	–	организационно-техническая структура системы обеспечения информационной безопасности, реализующая решение определенной задачи, направленной на противодействие той или иной угрозе информационной безопасности.
Система управления информационной безопасностью (СУИБ)	–	система управления, предназначенная для разработки, внедрения, применения, мониторинга, анализа, поддержания и совершенствования ИБ.
Событие информационной безопасности	–	идентифицированное возникновение состояния информационной системы (сегмента, компонента информационной системы), сервиса или сети, указывающее на возможное нарушение безопасности информации, или сбой средств защиты информации, или ранее неизвестную ситуацию, которая может быть значимой для безопасности информации.
Субъект доступа	–	лицо или процесс, действия которого регламентируются правилами разграничения доступа.
Удаленный доступ	–	процесс получения доступа (через внешнюю сеть) к объектам доступа информационной системы из другой информационной системы (сети) или со средства вычислительной техники, не являющегося постоянно (непосредственно) соединенным физически или логически с информационной системой, к которой он получает доступ.
Угроза	–	совокупность условий и факторов, определяющих потенциальную или реально существующую опасность возникновения инцидента информационной безопасности, который может привести к нанесению ущерба ИР.
Уязвимость ИР	–	недостаток (слабость) ИР, который (которая) создает потенциальные или реально существующие условия для реализации или проявления угроз безопасности информации.

3 ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ВЗАИМОДЕЙСТВИИ ЦТСС ЖЕЛЕЗНОДОРОЖНЫХ ПРЕДПРИЯТИЙ ГОСУДАРСТВ-ЧЛЕНОВ ОСЖД В МЕЖДУНАРОДНОМ СООБЩЕНИИ

3.1. Целью Политики информационной безопасности при взаимодействии ЦТСС железнодорожных предприятий (в дальнейшем Политика) должно являться определение комплекса мероприятий, направленных на обеспечение равнопрочной защиты ИР и ИТИ железнодорожных предприятий государств-членов ОСЖД. Равнопрочность защиты означает, что прочность в многозвенной цепи защиты ИР и ИТИ железнодорожных предприятий зависит от прочности слабейшей системы защиты той или иной взаимодействующей ЦТСС железнодорожного предприятия государства-члена ОСЖД, которая будет определять, при этом, итоговую прочность общей системы комплексной защиты информации.

3.2. Предметом Политики должны являться правовые, организационные и технические меры защиты от угроз безопасности ИР и ИТИ при взаимодействии ЦТСС железнодорожных предприятий государств-членов ОСЖД и меры противодействия механизмам реализации этих угроз нарушителями ИБ.

3.3. Требования Политики должны использоваться всеми взаимодействующими структурными подразделениями железнодорожных предприятий государств-членов ОСЖД, осуществляющими обслуживание и обеспечение функционирования ЦТСС, а также соответствующими службами безопасности.

3.4. Основой обеспечения безопасности ИР и ИТИ является функционирующая система управления информационной безопасностью (СУИБ), включающая должностных лиц из числа руководства железнодорожных предприятий государств-членов ОСЖД, специальные подразделения (службы) безопасности, наделенные соответствующими правами по координации мероприятий по защите информации, контролю эффективности реализуемых мер защиты информации и обеспечивающие практическую реализацию Политики безопасности на железнодорожных предприятиях.

3.5. Политика информационной безопасности при взаимодействии ЦТСС железнодорожных предприятий должна следовать следующим принципам:

- соответствие Политики законодательству государств-членов ОСЖД и документам ОСЖД;
- базирование защиты информации на результатах определения угроз безопасности информации в ЦТСС и анализа рисков реализации угроз безопасности информации;
- экономическая обоснованность и техническая реализуемость организационных и технических мер защиты информации при взаимодействии ЦТСС;
- отсутствие отрицательного влияния СОИБ ЦТСС на показатели качества предоставления услуг связи в международном сообщении;
- оценка эффективности мер защиты информации ЦТСС при взаимодействии;

- обеспечение осведомленности, обучения и тренировок персонала по вопросам обеспечения информационной безопасности;
- выявление, анализ и устранение уязвимостей в ЦТСС, программном обеспечении и программно-аппаратных средствах ЦТСС, включая средства защиты информации;
- обеспечение непрерывности функционирования ЦТСС и сохранение безопасного состояния ЦТСС в случае сбоев.

3.6. Политика информационной безопасности при взаимодействии ЦТСС железнодорожных предприятий определяет:

- перечень применимых нормативных правовых актов документов по защите информации государств-членов ОСЖД, национальных и международных стандартов;
- описание взаимодействия типовых организационных (ролевых) структур, обеспечивающих функционирование, взаимодействие и защиту информации в ЦТСС железнодорожных предприятий, служб безопасности и специальных организационных структур ОСЖД;
- перечень подлежащих защите ИР и ИТИ, обеспечивающих взаимодействие ЦТСС железнодорожных предприятий и подход к оценке значимости (определению возможного ущерба) ИР и ИТИ;
- перечень возможных уязвимостей и угроз ИР и ИТИ железнодорожных предприятий государств-членов ОСЖД, формируемый на основе международных и национальных баз уязвимостей и угроз и учитывающий специфичные уязвимости и угрозы безопасности ЦТСС железнодорожных предприятий;
- характеристики потенциальных нарушителей информационной безопасности при взаимодействии ЦТСС железнодорожных предприятий;
- предполагаемые способы реализации угроз безопасности информации по отношению ИР и ИТИ железнодорожных предприятий;
- базовые правовые и организационные меры защиты информации при взаимодействии ЦТСС железнодорожных предприятий;
- базовые механизмы защиты информации при взаимодействии ЦТСС железнодорожных предприятий.

3.7. В целях реализации унифицированного подхода к построению системы управления информационной безопасностью рекомендуется разрабатывать положения Политики информационной безопасности в соответствии с международным стандартом ИСО/МЭК 27001 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» (Information Technology – Security Techniques – Information security management systems – Requirements).

3.8. Успешная реализация Политики информационной безопасности при взаимодействии ЦТСС железнодорожных предприятий возможна только при

комплексном подходе к вопросу защиты информации, активном участии всех должностных лиц структурных подразделений железнодорожных предприятий, обеспечивающих функционирование ЦТСС и выполнение задач по целевому назначению во взаимодействии со специальными организационными структурами ОСЖД.

4 РАЗРАБОТКА ТРЕБОВАНИЙ К МЕРАМ ЗАЩИТЫ ИР И ИТИ ЖЕЛЕЗНОДОРОЖНЫХ ПРЕДПРИЯТИЙ ГОСУДАРСТВ-ЧЛЕНОВ ОСЖД ПРИ ВЗАИМОДЕЙСТВИИ ЦТСС В МЕЖДУНАРОДНОМ СООБЩЕНИИ

4.1. При разработке требований к мерам защиты ИР и ИТИ железнодорожных предприятий следует исходить из того, что для достижения главной цели – обеспечения установленных значений показателей качества предоставления услуг связи в международном сообщении – защита информации рассматривается как одно из приоритетных направлений деятельности для каждого железнодорожного предприятия, входящего в ОСЖД.

С этой целью для определенной в Политике информационной безопасности при взаимодействии ЦТСС железнодорожного предприятия характеристики нарушителя идентифицируются все возможные каналы несанкционированного доступа к ИР и ИТИ, и определяются необходимые меры защиты ЦТСС. При разработке требований к мерам защиты ИР и ИТИ следует исходить из того, что прочность общей системы комплексной защиты ИР и ИТИ железнодорожных предприятий государств-членов ОСЖД при взаимодействии их ЦТСС будет равна прочности наиболее слабого защитного контура.

4.2. В соответствии с требованиями к мерам защиты ИР и ИТИ железнодорожными предприятиями каждого государства-члена ОСЖД создается система обеспечения информационной безопасности (далее – СОИБ) ЦТСС, основанная на следующих принципах:

- обеспечение уровня безопасности, соответствующего требованиям к мерам защиты ИР и ИТИ;
- следование экономической целесообразности в выборе защитных мер (расходы на защиту не должны превосходить предполагаемый ущерб от нарушения информационной безопасности);
- всеобщий контроль, т.е. обеспечение безопасности в каждом функциональном сегменте ЦТСС во всех режимах работы;
- независимость системы защиты от субъектов защиты, т.е. лица, занимающиеся разработкой системы защиты, не должны быть в числе пользователей, работу которых предполагается контролировать;
- изоляция и разделение, т.е. объекты защиты, разделяются на группы таким образом, чтобы нарушение защиты в одной из групп не влияло на безопасность других групп;
- принцип недружественного окружения, т.е. система защиты должна проектироваться в расчете на неблагоприятное окружение;
- существование механизмов защиты рекомендуется, по возможности, скрывать от пользователей, работу которых предполагается контролировать;

- предоставление персоналу достаточной информации для осознанного поддержания режима безопасности.

4.3. При разработке требований к мерам защиты ИР и ИТИ следует исходить из того, что основными задачами, с точки зрения обеспечения информационной безопасности в ЦТСС, являются обеспечение доступности каналов для зарегистрированных пользователей и целостности обрабатываемой в них информации, а также недопущение несанкционированного использования ресурсов ЦТСС. Наиболее уязвимыми компонентами ЦТСС являются системы управления. Поэтому основной акцент в разрабатываемых требованиях к мерам защиты ИР и ИТИ должен делаться на решении задач физической защиты и защиты от несанкционированного доступа к системам управления ЦТСС.

4.4. СОИБ ЦТСС целесообразно строить с учетом угроз безопасности информации, обусловленных наличием потенциального нарушителя и уязвимостей элементов ЦТСС, на которые эти угрозы распространяются, при этом необходимо обеспечивать сохранение следующих основных характеристик защищенности информации:

- *конфиденциальность* достигается путем применения сертифицированных средств защиты информации от несанкционированного доступа, реализации правил разграничения доступа к информации, применения алгоритмов специального преобразования данных при передаче информации в сети передачи данных, а также организационных мер по предотвращению разглашения конфиденциальной информации и неправомерных действий со стороны лиц, имеющих право доступа к конфиденциальной информации;
- *целостность* достигается путем разработки и внедрения технологий резервирования и восстановления информационных ресурсов, применения технологий электронной (цифровой) подписи (в соответствии с законодательством государства-участника), физической охраной технических средств и носителей информации, другими организационными мерами;
- *доступность* достигается путем резервирования технических средств, дублирования каналов в ЦТСС, анализа уязвимостей и обнаружения вторжений, а также организационными мерами.

4.5. Требованиями к мерам защиты ИР и ИТИ железнодорожных предприятий при взаимодействии ЦТСС государств-членов ОСЖД определяется режим работы оборудования, при котором исключаются каналы, обеспечивающие физический и удаленный доступ к системе управления сетью и технологической связи со стороны сети другого государства в обход заданных правил управления доступом.

4.6. Технологическую связь с эксплуатационными подразделениями ЦТСС государств-членов ОСЖД рекомендуется организовывать по отдельным каналам.

4.7. Требования к мерам защиты ИР и ИТИ могут быть представлены в виде Профиля защиты в структуре, определенной ИСО/МЭК ТО 19791 «Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем» (ISO/IEC TR 19791 Information Technology – Security Techniques – Security assessment of operational systems); также могут использоваться и иные формы представления требований к мерам защиты, принятые в государствах-участниках ОСЖД.

5 ПРАВОВЫЕ И ОРГАНИЗАЦИОННЫЕ МЕРОПРИЯТИЯ, РЕГЛАМЕНТИРУЮЩИЕ ВОПРОСЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ВЗАИМОДЕЙСТВИИ ЦТСС ЖЕЛЕЗНОДОРОЖНЫХ ПРЕДПРИЯТИЙ ГОСУДАРСТВ-ЧЛЕНОВ ОСЖД

5.1. Правовые и организационные мероприятия, регламентирующие вопросы обеспечения информационной безопасности при взаимодействии ЦТСС железнодорожных предприятий государств-членов ОСЖД, должны соответствовать нормативно-правовой базе каждого государства, не противоречить международным нормативным документам по информационной безопасности и межправительственным соглашениям.

5.2. Основными правовыми и организационными мероприятиями по обеспечению безопасности при взаимодействии ЦТСС железнодорожных предприятий государств-членов ОСЖД являются:

- определение порядка взаимодействия служб безопасности;
- установление (по взаимному согласованию) порядка обмена информацией, определение ее объемов и конкретного содержания при взаимодействии между собой структурных подразделений железнодорожных предприятий, обеспечивающих функционирование ЦТСС и выполнение задач по целевому назначению и при взаимодействии структурных подразделений железнодорожных предприятий со специальными службами государств-членов ОСЖД;
- определение (при необходимости) третьей доверенной стороны для организации защищенного взаимодействия (документооборота) железнодорожных предприятий государств-членов ОСЖД;
- определение согласованного с пограничными службами государств-членов ОСЖД порядка допуска персонала линейно-эксплуатационных и аварийно-восстановительных бригад к работам в пограничной зоне и на участках границы, по которым проложены кабели связи;
- определение особенностей вызова и прибытия подразделений специальных служб государств-членов ОСЖД при возникновении чрезвычайных ситуаций природного и техногенного характера (аварий, опасных природных явлений, катастроф, стихийных или иных бедствий);
- организация совместного реагирования на нарушения (инциденты) информационной безопасности с возможностью привлечения внешних экспертов, центров компетенций по защите информации и используемым информационным технологиям;
- регламентация взаимодействия железнодорожных предприятий с разработчиками ЦТСС и подсистем ЦТСС, разработчиками и производителями используемого программного обеспечения, программно-технических средств и средств защиты информации в составе ЦТСС и СОИБ ЦТСС.

5.3. Для обеспечения защиты информации, содержащейся в ЦТСС, проводятся следующие мероприятия:

- оценка значимости ИР и элементов ИТИ;
- определение актуальных угроз безопасности информации, реализация которых может привести к нарушению безопасности информации, с учетом результатов анализа рисков реализации угроз безопасности информации;
- определение требований к системе защиты информации ИР, в том числе требований к защите информации при информационном взаимодействии с иными ИР и информационно-телекоммуникационными сетями;
- проектирование и внедрение СОИБ (элементов СОИБ);
- оценка соответствия СОИБ (элементов СОИБ) требованиям к защите информации;
- управление (администрирование) СОИБ (элементами СОИБ) (управление учетными записями, средствами защиты, установка обновлений ПО, анализ событий безопасности, информирование пользователей об угрозах ИБ);
- выявление инцидентов, реагирование на них, планирование и принятие мер по предотвращению повторного возникновения инцидентов;
- управление конфигурацией ЦТСС и СОИБ (элементов СОИБ) (контроль внесения изменений, анализ потенциального воздействия планируемых изменений на безопасность информации);
- контроль (мониторинг) за обеспечением уровня защищенности информации (контроль действий пользователей, аудит событий ИБ, анализ изменений угроз безопасности информации, периодический анализ уязвимостей с использованием международных и национальных баз данных уязвимостей и инструментальных средств (сканеров) безопасности, планирование модернизации СОИБ).

6 ОРГАНИЗАЦИОННЫЕ И ТЕХНИЧЕСКИЕ МЕРЫ ЗАЩИТЫ ЦТСС ЖЕЛЕЗНОДОРОЖНЫХ ПРЕДПРИЯТИЙ ГОСУДАРСТВ-ЧЛЕНОВ ОСЖД

6.1. Организационные и технические меры защиты ЦТСС должны охватывать все виды деятельности, связанные с созданием, эксплуатацией и развитием ИТИ. Они должны соответствовать нормативно-правовой базе каждого государства, не противоречить международным нормативным документам по информационной безопасности и межправительственным соглашениям.

6.2. Для реализации политики информационной безопасности, профилей защиты (требований к мерам защиты) в ЦТСС должны быть выполнены мероприятия по организации защиты информации и созданы СОИБ ЦТСС, в рамках которой должны быть реализованы организационные и технические меры по защите информации.

СОИБ ЦТСС предназначена для обеспечения требуемого уровня защищённости ЦТСС и должна обеспечивать комплексную защиту технических средств ЦТСС, ее систем управления, обеспечивающих управление оборудованием и параметрами информационного обмена в телекоммуникационной сети и пользователей железнодорожных предприятий от нарушений доступности, целостности и конфиденциальности.

СОИБ ЦТСС, должна быть многоуровневой и осуществляться как на программном, так и физическом уровнях.

6.3. СОИБ ЦТСС должна отвечать следующим основным требованиям:

- обеспечение защиты ЦТСС от актуальных угроз безопасности информации;
- обеспечение защиты информации на всех технологических этапах обработки информации и во всех режимах функционирования ЦТСС, в том числе при проведении ремонтных и регламентных работ;
- регулярное проведение контроля эффективности средств защиты;
- обеспечение защиты собственных объектов информатизации.

6.4. Система обеспечения информационной безопасности ЦТСС должна представлять собой территориально распределенную по структурным элементам ЦТСС систему, состоящую из взаимосвязанных, централизованно управляемых сегментов, обеспечивающих защиту от несанкционированного доступа к обрабатываемой в ЦТСС защищаемой информации и защиту технических средств ЦТСС.

6.5. Организационно СОИБ ЦТСС может подразделяться на следующие системы:

- систему управления СОИБ ЦТСС, обеспечивающую управление всей СОИБ ЦТСС;
- системы и средства защиты информации на участках (в сегментах) ЦТСС в зоне ответственности центров управления ЦТСС.

6.6. Организационно-технические меры защиты информации в сегментах ЦТСС в зоне ответственности центров управления ЦТСС, в зависимости от угроз безопасности информации и предъявленных требований безопасности, могут включать:

1) комплексную защиту периметра ЦТСС с использованием средств межсетевого экранирования, обнаружения и предотвращения вторжений, защиты от распределенных атак типа «отказ в обслуживании» (DDoS), сетевой антивирусной защиты, мониторинга сетевой активности;

2) сегментацию ИТИ и ЦТСС, сокрытие внутренней структуры телекоммуникационной сети, ограничение подключений к сетям общего пользования (Интернет), обеспечение защиты удаленного доступа к ИР и элементам ИТИ;

3) резервирование технических средств, дублирование каналов в ЦТСС. осуществление регламентного резервного копирования информации;

4) своевременное восстановление ЦТСС и СОИБ после отказов технических средств, аварий и других природных и техногенных воздействий, проведение тренировок по восстановлению безопасного состояния после сбоев и отказов;

5) обеспечение защиты оборудования и каналов связи от несанкционированного подключения;

6) многоуровневую идентификацию и аутентификацию субъектов доступа и управление доступом к защищаемой информации (ИР), элементам ИТИ, ЦТСС и другим объектам доступа;

7) сбор, запись, хранение и защиту информации о событиях безопасности в ЦТСС, а также возможность просмотра и анализа информации о событиях безопасности информации и реагирование на них, в том числе регистрацию действий пользователей и других событий, способных повлиять на функционирование ЦТСС и СОИБ;

8) учет машинных носителей информации, используемых в ЦТСС для хранения и обработки информации;

9) обеспечение безопасного функционирования телекоммуникационного оборудования при использовании внеполосного доступа для локального и удаленного администрирования и технической поддержки, в том числе со стороны разработчиков ЦТСС и производителей телекоммуникационного оборудования;

10) защиту передаваемой информации и каналов передачи данных между сегментами администрирования и телекоммуникационным оборудованием с использованием организационных и технических мер защиты или средств криптографической защиты в соответствии с законодательством государства-участника;

11) обнаружение компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации, предотвращение внедрения вредоносных компьютерных программ (компьютерных вирусов) и программных закладок путем применения средств антивирусной защиты;

12) обновление программного обеспечения, баз данных и используемых средств защиты информации;

13) обеспечение защиты собственных программно-технических средств СОИБ;

14) комплексы мер по защите беспроводного доступа, мобильных технических средств, каналов связи, защищаемой аудио и видеоинформации, IP-телефонии;

15) контроль целостности передаваемых данных, периодическую проверку целостности используемого программного обеспечения средств защиты информации;

16) физическую защиту средств хранения и обработки информации, организацию контролируемых зон на объектах эксплуатации ЦТСС, в том числе, ограничение доступа в зоны и помещения, где размещаются ИР и элементы ИТИ, средства обработки информации и вспомогательное оборудование.

6.7. Рекомендуется проведение оценки соответствия (сертификации) требованиям по безопасности информации в национальных системах сертификации программных и программно-технических средства, реализующих механизмы защиты информации, и средств защиты информации.

Сертификация средств защиты информации по требованиям, основанным на международном стандарте ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» (ISO/IEC 15408 Information Technologies – Security Techniques – Evaluation Criteria for IT Security) обеспечит взаимное доверие к безопасности информации взаимодействующих ЦТСС государств-участников ОСЖД.

6.8. Оценка соответствия реализованных мер защиты информации при взаимодействии ЦТСС предъявленным требованиям проводится в соответствии с национальным законодательством государства-участника ОСЖД (в форме аттестации, оценки эффективности, валидации или иной форме).