**ОРГАНИЗАЦИЯ СОТРУДНИЧЕСТВА ЖЕЛЕЗНЫХ ДОРОГ (ОСЖД)**

II издание

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

Согласовано итоговым совещанием ПРГ КИ с 17-19 ноября 2015 г., Комитет ОСЖД

Утверждено XXXI заседанием Конференция Генеральных директоров (ответственных представителей) железных дорог ОСЖД 25-29 апреля 2016 г., Кыргызская Республика, г. Чолпон-Ата

Дата вступления в силу: 29 апреля 2016 г.

Примечание: Теряет силу I издание от 29.04.2005 г.

**О+Р 941**

# БЕЗОПАСНОСТЬ ОБЩИХ ИНФОРМАЦИОННЫХ РЕСУРСОВ И ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ

## СОДЕРЖАНИЕ

# ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

| | | |
|---|---|---|
| БД | – | база данных |
| ИР | – | информационные ресурсы |
| ИТИ | – | информационно-телекоммуникационная инфраструктура |
| ЛВС | – | локальная вычислительная сеть |
| МЭ | – | межсетевой экран |
| НСД | – | несанкционированный доступ |
| ОС | – | операционная система |
| ОСЖД | – | Организация сотрудничества железных дорог |
| СУБД | – | система управления базами данных |
| Смарт - карта | – | пластиковая карта со встроенным микропроцессором, обеспечивающая активное взаимодействие с терминалом |
| ППО | – | прикладное программное обеспечение |
| VLAN | – | виртуальная локальная вычислительная сеть |

# 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 рекомендуется реализовать системы обеспечения информационной безопасности (СОИБ) железнодорожных предприятий, основанные на применении правовых, организационных и технических мер.

1.2. Целью настоящей памятки является определение общих принципов, концепции защиты информации и установление унифицированных требований к комплексу организационных и технических мероприятий по защите общих ИР и ИТИ железнодорожных предприятий государств-членов ОСЖД в международном сообщении (далее – железнодорожных предприятий) в ходе всего процесса функционирования информационно-телекоммуникационных систем и сетей, связанного с подготовкой, обработкой, хранением и передачей информации.

1.3. Основными принципами организации защиты информации при взаимодействии ЦТСС железнодорожных предприятий 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.

1.4. 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 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 27033-3 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления» (ISO/IEC 27033-3 Information Technology – Security Techniques – Network Security – Part 3: Reference networking scenarios – Threats, design techniques and control issues);
- ИСО/МЭК 27033-4 «Информационные технологии. Методы и средства обеспечения безопасности. Сетевая безопасность. Часть 4. Коммуникации для обеспечения безопасности между сетями с применением шлюзов безопасности» (ISO/IEC 27033-4 Information Technology – Security Techniques – Network Security – Part 4: Securing communications between networks using security gateways);
- ИСО/МЭК 27033-5 «Информационные технологии. Методы и средства обеспечения безопасности. Безопасность информационной сети. Часть 5. Коммуникации для обеспечения безопасности между сетями с применением виртуальных частных систем» (ISO/IEC 27033-5 Information Technology – Security Techniques – Network Security – Part 5: Securing communications across networks using Virtual Private Networks (VPNs).

## 2 ОСНОВНЫЕ 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 ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИР И ИТИ

Риск информационной безопасности ИР и ИТИ – это ситуация, когда угроза, реализуясь через использование уязвимости, приводит к нанесению вреда (ущерба) информационным ресурсам организации. Ресурсы, значимые для деятельности организации и имеющие уязвимости, подвергаются риску, если по отношению к ним существует какая-либо угроза.

Для оценки рисков необходимо:

- определить ценность (значимость) информационных ресурсов;
- определить угрозы и уязвимости;
- проанализировать риски реализации угроз;
- оценить эффективность контрмер (мер защиты информации).

## 3.1 Определение ценности информационных ресурсов

1. Классификация ресурсов.

Информационные ресурсы, являясь объектом отношений физических, юридических лиц и государства-члена ОСЖД, подлежат учету и защите, как всякое материальное имущество (и нематериальные активы) железнодорожного предприятия, наряду с другими ресурсами. При этом железнодорожному предприятию предоставляется право самостоятельно в зоне своей ответственности, устанавливать режим защиты информационных ресурсов и доступа к ним.

В широком смысле ресурс – это все, что представляет ценность, с точки зрения организации, и может являться объектом защиты.

Защите подлежат ресурсы следующих информационных систем:

- информационные системы управления перевозочным процессом;
- информационные системы, содержащие информационные активы (ресурсы) конфиденциального характера.

Основными объектами защиты являются:

- служебная информация средств защиты информации (например, идентификаторы, пароли, таблицы разграничения доступа, информация журналов аудита безопасности);
- программно-технические средства (включая конфигурационные данные), используемые для обработки и анализа информации, в том числе каналы информационного обмена и средства защиты информации;
- оборудование (физические ресурсы);
- информация (базы данных, файлы, все виды документации);
- программное обеспечение (системное, прикладное, утилиты и другие вспомогательные программы);

- сервис и поддерживающая инфраструктура (например, обслуживание средств вычислительной техники, энергоснабжение, обеспечение климатических параметров).

2. Разработка и согласование критериев и методики определения ценности ресурсов.

3. Сбор, обработка данных, формирование, согласование и утверждение ранжированной шкалы информационных ресурсов железнодорожных предприятий с учетом их ценности.

### 3.2 Определение угроз и уязвимостей

1. Обобщение и классификация угроз.

Угроза ИБ – совокупность условий и факторов, которые могут стать причиной нарушения целостности, доступности, конфиденциальности ИР.

Угрозы классифицируются в зависимости от возможности нанесения ущерба ИР и ИТИ при нарушении целей ИБ. Ущерб может быть причинен каким-либо субъектом, а также может быть следствием событий, не зависящих от субъекта.

Выделяются следующие виды ущерба ИР и ИТИ:

- материальный и моральный ущерб от дезорганизации деятельности железнодорожного предприятия;
- материальный, моральный ущерб от любых неправомерных действий;
- материальный ущерб от невозможности выполнения взятых обязательств перед третьей стороной;
- материальный, моральный ущерб от нарушения международных обязательств;
- материальный ущерб от разглашения защищаемой информации;
- моральный, физический, материальный ущерб личности, от разглашения персональных данных лиц;
- моральный, материальный ущерб от нарушения конституционных прав и свобод личности;
- материальный ущерб от необходимости восстановления нарушенных прав и объектов защиты.

2. Оценка параметров и ранжирование угроз.

Ранжирование угроз позволяет определить наиболее опасные (актуальные) угрозы, которые в дальнейшем используются при анализе и определении актуальных источников угроз и методов их реализации.

3. Оценка уязвимости ресурсов.

Под уязвимостью понимается недостаток (слабость) элемента ИТИ, который (которая) создает потенциальные или реально существующие условия для реализации или проявления угроз безопасности информации.

Уязвимости выделяются в зависимости от того, по отношению к каким ИР и элементам ИТИ возможна реализация атак, и подразделяются, в основном, на

уязвимости среды передачи данных и телекоммуникационного оборудования (ТКО), ОС, СУБД, ППО, средств ЗИ.

При наличии уязвимостей нарушитель может получить доступ к различной защищаемой информации, например:

- при наличии уязвимостей среды передачи данных и ТКО – к передаваемой по сети информации, адресам сетевых устройств, протоколам передачи данных, параметрам настройки ТКО, политике и правилам управления потоками информации, настройкам портов и интерфейсов ТКО;
- при наличии уязвимостей ОС – к объектам файловой системы ОС (томам, каталогам, файлам и другим объектам файловой системы), записям журналов регистрации событий, реестру, паролям;
- при наличии уязвимостей СУБД – к объектам БД (исполняемым объектам БД; хранимой в БД информации), механизмам управления элементами БД;
- при наличии уязвимостей ППО – к объектам доступа, создаваемым прикладным программным обеспечением;
- при наличии уязвимостей средств ЗИ – к защищаемым с использованием средств ЗИ объектам доступа, параметрам настройки, правилам разграничения доступа, аутентификационной информации, ключевой информации, служебным БД средств ЗИ.

Проявление уязвимостей определяется возможностью выполнения нарушителем действий, направленных на:

- обход средств защиты информации;
- отключение средств защиты информации;
- преодоление средств защиты информации.

Основными возможными причинами проявления уязвимостей являются следующие:

- ошибки в программном обеспечении, в том числе в программном обеспечении средств защиты информации;
- нарушения порядка, правил и требований к установке и настройке программного обеспечения, в том числе программного обеспечения средств защиты информации;
- нарушение порядка, правил и требований к эксплуатации и сопровождению программного обеспечения, в том числе программного обеспечения средств защиты информации (в том числе нарушение или невыполнение процедур установки обновлений программного обеспечения).

Для известных уязвимостей поиск и анализ уязвимостей проводится с использованием международных и национальных банков данных угроз безопасности информации.

### 3.3 Анализ рисков

1. Классификация и согласование уровней рисков.

Классификация рисков – процесс выделения множества угроз ИБ, по определенному признаку (например, относящихся к определенной подсистеме или типу ресурса).

2. Оценка уровней рисков.

Оценка уровня риска определяется на основании оценок вероятности реализации угрозы и оценке возможного ущерба.

Ущерб от реализации угрозы складывается из ущерба от ее непосредственного воздействия на ИР (нарушений доступности, конфиденциальности, целостности) и ущерба от последствий таких нарушений.

Анализируя эти характеристики угрозы (вероятность реализации и ущерб от угрозы), владельцы ИР могут оценить величину риска по каждой из возможных угроз и характеристике безопасности, выработать меры по его уменьшению, и затем по остаточным рискам убедиться, что риски снижены до приемлемого уровня.

### 3.4 Оценка эффективности контрмер

Оценка эффективности контрмер должна включать:

1. Классификацию контрмер и средств защиты.

С целью сокращения уязвимостей и возможности реализации угроз безопасности информации применяются меры защиты информации (контрмеры).

Контрмеры разрабатываются как комплекс средств и механизмов защиты. Это могут быть организационные, экономические, технические, программные, социальные, правовые и иные механизмы, обеспечивающие локализацию и предотвращение угроз или снижение потенциального ущерба.

Основными видами контрмер являются:

- меры по выявлению и устранению уязвимостей;
- меры по идентификации и аутентификации пользователей и ресурсов;
- меры по управлению доступом субъектов доступа к объектам доступа;
- меры по регистрации событий безопасности;
- меры по ограничению программной среды;
- меры по контролю использования машинных носителей информации;
- меры по реализации антивирусной защиты;
- меры по обнаружению (предотвращению) вторжений;
- меры по обеспечению целостности и доступности ИР;
- меры по физической защите технических средств ИР и ИТИ;

2. Оценку эффективности используемых типовых средств защиты.

Оценить эффективность используемых средств защиты можно на основе:

- информации об инцидентах реализации угроз, на исключение которых направлены конкретные средства защиты информации;

- анализа степени влияния применяемых средств защиты информации на реализуемую информационную технологию.

3. Оценку стоимости контрмер.

Стоимость контрмер целесообразно соотнести с возможным ущербом от реализации угроз безопасности и со стоимостью реализации альтернативных контрмер.

4. Оценку эффективности контрмер.

Целесообразно оценить эффективность распределения (сочетания) организационных и технических мер. При необходимости – скорректировать соотношение.

5. Определение допустимого риска.

Очевидно, что экономически целесообразным является допущение определенного уровня риска, когда ущерб для железнодорожного предприятия не будет представляться существенным.

# 4 ОСНОВНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ДЛЯ ИР И ИТИ

Обеспечение безопасности информации для ИР и ИТИ должно осуществляться с учетом угроз безопасности информации, определяемых по результатам:

- оценки возможностей нарушителей по реализации угроз;
- анализа возможных уязвимостей;
- анализа возможных способов реализации угроз безопасности информации;
- анализа последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

Возможные угрозы безопасности информации, обрабатываемой в ИР и ИТИ железнодорожных предприятий подразделяются на внешние и внутренние.

Внешние угрозы обусловлены действиями субъектов, не входящих в состав пользователей, обслуживающего персонала и разработчиков ИР и ИТИ железнодорожных предприятий, а также явлениями природного или техногенного характера.

Внутренние угрозы исходят от пользователей, обслуживающего персонала и разработчиков компонент ИР и ИТИ железнодорожных предприятий, а также других лиц, имеющих локальный или удаленный доступ к ИР и элементам ИТИ.

## 4.1 Основные источники внешних угроз

Источниками внешних угроз безопасности ИР и ИТИ могут являться:

- деятельность политических и экономических структур, направленная против экономических интересов железнодорожных предприятий;
- террористическая деятельность;
- преступные действия международных групп (организаций) и отдельных лиц, направленные против деятельности организаций (предприятий), участвующих в информационном обмене в рамках автоматизированных систем, образующих ИР и ИТИ железнодорожных предприятий;
- стихийные бедствия, катастрофы и другие явления природного или техногенного характера.

## 4.2 Основные источники внутренних угроз

Источниками внутренних угроз безопасности ИР и ИТИ могут являться:

- несанкционированный доступ к защищаемой информации, хранимой и обрабатываемой в ИР и ИТИ;
- случайное или преднамеренное вмешательство в нормальный процесс функционирования ИР и ИТИ, отказ технического оборудования, влияние человеческого фактора, хищение технических средств, форс-мажорные обстоятельства;

- обесценивание данных вмешательством посторонних лиц (хищение информации, ее модификация или разрушение);
- использование санкционированного доступа к информации в целях, не связанных с теми, для которых этот доступ предоставлялся;
- несанкционированная модификация конфигурационных файлов, настроек средств защиты информации;
- злоупотребление конфиденциальной информацией (нарушение заключенных соглашений в области владения, пользования, распоряжения информацией);
- вредоносные компьютерные программы;
- нарушение целостности, конфиденциальности и достоверности или потеря передаваемых сообщений (информации);
- снижение или ограничение услуг сети передачи данных.

### 4.3 Возможные последствия реализации угроз безопасности ИР и ИТИ

Последствия от возможной реализации угроз безопасности ИР и ИТИ могут нанести значительный ущерб интересам железнодорожных предприятий, в том числе:

- остановку информационно-вычислительных процессов и блокирование информационного взаимодействия;
- разглашение информации ограниченного доступа;
- раскрытие стратегических планов деятельности железнодорожных предприятий;
- утечку информации о текущей хозяйственной деятельности предприятия;
- формирование негативного общественного мнения;
- потерю актуальной информации;
- навязывание неверных или невыгодных решений;
- утрату доверия и авторитета у других членов ОСЖД.

# 5 РАЗРАБОТКА ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Целью Политики информационной безопасности (в дальнейшем – Политики) является определение комплекса мероприятий, направленных на обеспечение защиты ИР и ИТИ железнодорожных предприятий.

Предметом Политики должны являться правовые, организационные и технические меры защиты от угроз безопасности ИР и ИТИ железнодорожных предприятий и меры противодействия механизмам реализации этих угроз нарушителями ИБ.

Требования Политики должны использоваться всеми взаимодействующими структурными подразделениями железнодорожных предприятий, осуществляющими обслуживание и обеспечение функционирования ИР и ИТИ, а также службами безопасности.

Основой обеспечения безопасности ИР и ИТИ является функционирующая система управления информационной безопасностью (СУИБ), включающая должностных лиц из числа руководства железнодорожных предприятий и службу безопасности, наделенную соответствующими правами по координации мероприятий по защите информации, контролю эффективности реализуемых мер защиты информации и обеспечивающие практическую реализацию Политики безопасности на железнодорожном предприятии.

Политика информационной безопасности железнодорожного предприятия определяет:

- перечень применимых нормативных правовых актов документов по защите информации, национальных и международных стандартов;
- описание взаимодействия структурных подразделений, осуществляющих обслуживание и обеспечение функционирования ИР и ИТИ и служб безопасности железнодорожных предприятий;
- перечень подлежащих защите общих ИР и ИТИ железнодорожных предприятий и подход к оценке значимости (определению возможного ущерба) общих ИР и ИТИ;
- перечень возможных уязвимостей и угроз общих ИР и элементов ИТИ железнодорожных предприятий, формируемый на основе международных и национальных баз уязвимостей и угроз и учитывающий специфичные этих ИР и элементов ИТИ уязвимости и угрозы безопасности;
- характеристики потенциальных нарушителей информационной безопасности общих ИР и элементов ИТИ железнодорожных предприятий;
- предполагаемые способы реализации угроз безопасности информации по отношению общим ИР и ИТИ железнодорожных предприятий;
- основные правовые и организационные мероприятия по информационной безопасности;

- основные направления и технологии обеспечения информационной безопасности общих ИР и ИТИ железнодорожных предприятий.

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).

Обеспечение выполнения положений Политики информационной безопасности, включая разработку превентивных и восстановительных мер, направленных на уменьшение (нейтрализацию) угроз безопасности информации и снижение вероятности их возникновения является одной из основных задач руководства железнодорожных предприятий.

Знание конкретных источников и характера угроз безопасности позволит уполномоченным органам железнодорожных предприятий, осуществляющим планирование и организацию выполнения мероприятий по защите информации, осуществлять планомерную и целенаправленную работу по уменьшению вероятности возникновения этих угроз и снижению возможного ущерба при их реализации.

Превентивные меры защиты информации должны быть направлены на значительное снижение вероятности реализации конкретных угроз безопасности информации путем усиления защиты ИР и элементов ИТИ, на которые направлены эти угрозы.

Превентивные меры включают комплекс мероприятий по разработке СОИБ, непрерывному контролю и анализу состояния информационной безопасности на объектах железнодорожных предприятий и постоянным совершенствованием СОИБ в процессе эксплуатации.

Организационные и технические мероприятия по обеспечению информационной безопасности общих ИР и ИТИ организуются и выполняются службами, эксплуатирующими ИР и ИТИ, и включают:

- создание совместных структурных подразделений, ответственных за безопасность ИР и ИТИ;
- планирование мероприятий по обеспечению безопасности ИР и ИТИ;
- анализ угроз безопасности ИР и ИТИ и общий контроль состояния внутренней информационной безопасности;
- разработку регламентной и нормативно-технической документации по обеспечению безопасности информации, обрабатываемой в автоматизированных системах, образующих ИР и ИТИ железнодорожных предприятий;

- регистрацию, систематизацию и анализ событий, влияющих на безопасность ИР и ИТИ;
- мониторинг состояния программно-технических средств обеспечения функционирования ИР и ИТИ, а также средств защиты информации;
- обеспечение резервирования технических средств обеспечения функционирования ИР и ИТИ, а также средств защиты информации;
- определение и разграничение полномочий пользователей ИР и ИТИ по доступу к информации;
- проведение комплекса мероприятий по защите от вредоносных компьютерных программ ИР и ИТИ;
- резервное копирование информации.

Выполнение восстановительных мер при возникновении нештатных ситуаций (нарушений безопасности) осуществляется обслуживающим персоналом и администраторами сетей связи и передачи данных. Планирование восстановительных мер определяется системой документов, устанавливающих требования к обязательным мероприятиям, проводимым заблаговременно и после возникновения нарушений, угрожающих штатному функционированию ИР и ИТИ.

# 6 РАЗРАБОТКА ПРАВОВЫХ И ОРГАНИЗАЦИОННЫХ МЕРОПРИЯТИЙ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Правовые и организационные мероприятия должны охватывать все виды деятельности, связанные с созданием, эксплуатацией и развитием ИТИ. Они должны соответствовать нормативно-правовой базе каждого государства-члена ОСЖД, не противоречить международным нормативным документам по информационной безопасности и межправительственным соглашениям.

Основными правовыми и организационными мероприятиями по обеспечению безопасности информационных и телекоммуникационных систем и сетей железнодорожных предприятий являются:

- определение общих принципов работы со средствами вычислительной техники;
- определение общих принципов работы со средствами связи и передачи данных;
- установление регламента (правового режима, порядка) доступа эксплуатационного персонала и посторонних лиц на объекты, к техническим средствам систем;
- установление размеров контролируемой зоны, установление регламента доступа в зону эксплуатационного персонала и посторонних лиц, допуска посторонних транспортных средств;
- разработка разрешительной системы доступа пользователей и эксплуатационного персонала систем и иных объектов этих систем и предприятий железнодорожного транспорта к информационным ресурсам;
- управление доступом к машинным носителям информации;
- документирование должностных обязанностей персонала, связанных с ИБ;
- разработка согласованной представителями железнодорожных предприятий эксплуатационной и организационно-распорядительной документации:
  - инструкций и руководств по эксплуатации технических средств систем ИТИ и технических средств защиты;
  - общего для железнодорожных предприятий перечня конфиденциальной информации;
  - правил доступа к чувствительной информации;
  - инструкций по выполнению установленных требований безопасности для пользователей эксплуатирующих подразделений, администраторов систем, а также для сотрудников служб безопасности;
  - инструкций по организации учета и хранения съемных машинных носителей информации;
  - инструкций по совместному выявлению и реагированию на нарушения (инциденты) информационной безопасности;

- установление правил персональной ответственности сотрудников эксплуатирующих подразделений;
- проведение регулярного обучения персонала в области ИБ;
- установление (по взаимному согласованию) порядка обмена информацией, определение ее объемов и конкретного содержания при взаимодействии железнодорожных предприятий.

# 7 РАЗРАБОТКА ОСНОВНЫХ НАПРАВЛЕНИЙ И ТЕХНОЛОГИЙ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИР И ИТИ

Для создания СОИБ технических, программных и информационных ресурсов информационных и телекоммуникационных систем и сетей железнодорожных предприятий необходимо задействовать, и интегрировать функции основных видов современных средств и технологий защиты, которые смогут исключить, устранить или значительно смягчить последствия угроз безопасности.

В ИР и ИТИ железнодорожных предприятий можно выделить три основных уровня обеспечения информационной безопасности:

- уровень защиты от несанкционированного доступа аппаратной и программной платформы каждого средства вычислительной техники;
- уровень защиты интрасети (корпоративной сети железнодорожного предприятия) как объединения множества средств вычислительной техники, возможно разделенных на различные сегменты, в зависимости от требований обеспечения безопасности информации в каждом из сегментов;
- уровень защиты межсетевого взаимодействия.

Комплекс решений по защите ИР и ИТИ железнодорожных предприятий должен предполагать решение следующих задач:

- защиту ресурсов компьютеров, систем управления базами данных, сетевых операционных систем и иного общесистемного программного обеспечения;
- защиту каналов связи посредством установки межсетевых экранов и использования средств криптографической защиты информации (в соответствии с законодательством государства-члена ОСЖД);
- установку средств аудита, мониторинга и контроля защищенности интрасетей с целью обнаружения уязвимостей средств их защиты;
- защиту электронного обмена данными;
- защиту от физического проникновения на объекты эксплуатации ИР и ИТИ.

Решение вышеперечисленных задач определяет круг возможных направлений защиты и примерный состав программно-технических средств защиты информации для конкретных подсистем ИР и ИТИ, который включает:

- средства доверенной загрузки средств вычислительной техники;
- средства идентификации и аутентификации субъектов доступа;
- средства управления доступом к информационным и сетевым ресурсам;
- средства регистрации событий безопасности информации;
- средства антивирусной защиты;
- средства контроля использования съемных машинных носителей информации
- средства контроля защищенности;

- системы и средства мониторинга информационной безопасности;
- средства межсетевого экранирования;
- средства обнаружения вторжений;
- средства защиты клиент-серверных технологий;
- средства построения корпоративных защищенных сетей передачи данных;
- средства криптографической защиты информации (применяемые в соответствии с законодательством государства-члена ОСЖД).

Защита программно-технических средств ИТИ от внешних программно-технических воздействий предусматривает организацию защиты от внешних воздействий, способных нарушить целостность или доступность защищаемых аппаратно-программных ресурсов ИТИ.

Защита от внешних программных воздействий обеспечивает:

- антивирусную защиту информации и программного обеспечения ИТИ;
- контроль защищенности;
- мониторинг информационной безопасности;
- обнаружение и отражение сетевых атак (вторжений) в реальном масштабе времени;
- экранирование сетевых адресов и фильтрацию сетевых пакетов.

В качестве определяющих выделены три основные цели защиты ИР и ИТИ:

- обеспечение конфиденциальности обрабатываемой информации;
- обеспечение целостности ИР и ИТИ;
- обеспечение доступности информации и сервисов.

Конфиденциальность обрабатываемой информации предполагает, что вся чувствительная информация в системе ранжирована по определенным критериям, устанавливаются правила доступа к ней различных категорий пользователей, и созданы механизмы, обеспечивающие предотвращение несанкционированного доступа к этой информации.

Целостность ИР и ИТИ предполагает наличие механизмов и средств контроля, обеспечивающих предотвращение несанкционированной модификации ИР и ИТИ. Целостность ИР и ИТИ включает понятия целостности технических средств, программного обеспечения, информационного обеспечения, организационного обеспечения.

Доступность предполагает наличие механизмов, обеспечивающих предотвращение отказов при доступе пользователей к информации и разрешенным функциям обработки информации.

Защита ИР и ИТИ железнодорожных предприятий и автоматизированных систем, их образующих, предусматривает следующие основные направления:

- обеспечение идентификации и аутентификации пользователей ИР;

- управление доступом к ИР и элементам ИТИ;
- обеспечение защиты от несанкционированного доступа к ИР и элементам ИТИ;
- обеспечение защиты информации в каналах связи ИТИ железнодорожных предприятий;
- обеспечение системы регистрации и учета действий пользователей ИР и ИТИ железнодорожных предприятий;
- управление инцидентами ИБ;
- обнаружение и предотвращение вторжений;
- обеспечение защиты клиент-серверных технологий;
- обеспечение антивирусной защиты ИР и ИТИ железнодорожных предприятий;
- обеспечение централизованного управления безопасностью и централизованного администрирования средств защиты информации ИР и ИТИ железнодорожных предприятий;
- разработку защищенных узлов подключения к глобальным сетям (сеть Интернет);
- обеспечение контроля использования съемных машинных носителей информации;
- обеспечение контроля беспроводных соединений;
- обеспечение защиты мобильных технических средств.

### 7.1 Идентификация и аутентификация пользователей и ресурсов

При доступе в ИР и ИТИ рекомендуется осуществлять идентификацию и аутентификацию пользователей.

Идентификация предполагает установление характеристик, способных однозначно идентифицировать (определить) объект в системе.

Аутентификация пользователей может осуществляться с использованием паролей, аппаратных средств, биометрических характеристик, иных средств или (в случае многофакторной (двухфакторной) аутентификации) – определенной комбинации указанных средств.

При использовании механизмов идентификации и аутентификации пользователей в ИР и ИТИ рекомендуется обеспечить:

- предоставление пользователю ИР и ИТИ аутентификационной информации (например, пароля) способом, исключающим возможность его компрометации;
- уникальные пароли для первоначального входа в систему с принудительной сменой после первого входа;

- регулярную смену паролей доступа к ИР и ИТИ;
- интерактивные процедуры для смены пароля пользователем в процессе работы, обеспечивающие достаточное качество (сложность) паролей.

В качестве носителей идентификационных характеристик могут использоваться:

- смарт-карты, электронные замки и другие носители информации для надежной идентификации и аутентификации пользователей ИР и ИТИ;
- человек, как носитель индивидуальных биометрических признаков, человеческая память, запоминающая набор символов, которым является пароль или PIN-код.

Для осуществления надежной аутентификации пользователей ИР и ИТИ могут использоваться электронные, биометрические, криптографические и другие разнообразные способы и методы (в соответствии с законодательством государства-члена ОСЖД).

Выбор конкретных способов и средств идентификации и аутентификации для использования в системе информационной безопасности ИР и ИТИ железнодорожных предприятий может быть осуществлен на этапе проектирования в комплексе с выбором других необходимых средств защиты.

### 7.2 Средства защиты информации ИР и ИТИ от несанкционированного доступа

По способу технической реализации средства защиты информации от несанкционированного доступа делятся на два больших класса: программно-технические комплексы защиты и программные средства защиты, причем программно-технические комплексы защиты имеют значительное предпочтение.

Данные комплексы реализуют:

- подсистему идентификации и аутентификации;
- подсистему контроля целостности;
- подсистему контроля использования съемных машинных носителей информации;
- подсистему разграничения доступа.

Функции подсистемы идентификации и аутентификации в большинстве систем выполняются аппаратной компонентой комплекса. Для аутентификации пользователей, как правило, используются две величины: считываемый из электронного идентификатора код и вводимый с клавиатуры пароль.

Функции контроля целостности программного обеспечения выполняются программным кодом из постоянного запоминающего устройства комплекса или программой, считанной из файла, защита которого обеспечивается подсистемой разграничения доступа. Механизм контроля целостности ИР и ИТИ предназначен для своевременного обнаружения модификации ИР и ИТИ и позволяет обеспечить правильность функционирования системы защиты информации и целостность

обрабатываемой информации. В части обеспечения контроля целостности информации и средств защиты информации целесообразно:

- применять встроенные механизмы контроля целостности используемых в ИР и ИТИ операционных систем, прикладного ПО и средств защиты информации;
- обеспечить отсутствие в ИР и ИТИ средств разработки и тестирования (отладки), либо выделение их в отдельный сегмент;
- вести не менее двух копий программных средств (например, дистрибутивов, лицензионных ключей, параметров настройки) для обеспечения возможности восстановления работоспособности этих средств в случае нарушения их работы;
- применять средства разграничения доступа, запрещающие модификацию или удаление защищаемых ресурсов;
- применять средства сравнения защищаемых ресурсов с их эталонными копиями (и восстановления в случае нарушения целостности);
- применять средства контроля целостности, например, для подсчета и сравнения контрольных сумм (в соответствии с законодательством государства-члена ОСЖД);
- применять средства электронной (цифровой) подписи (в соответствии с законодательством государства-члена ОСЖТ).

Функции подсистемы запрета загрузки со съемных носителей информации реализуются средствами контроля использования съемных носителей информации и средствами доверенной загрузки.

Управление доступом к ИР и ИТИ должно осуществляться в целях контроля доступа к информации, предотвращения неавторизованного доступа и обеспечения авторизованного доступа к ИР и ИТИ, операционным системам и информации в прикладных системах. Разграничение доступа осуществляется путем фильтрации системных запросов на выполнение файловых операций или операций в базах данных и сравнения полномочий (привилегий) текущего пользователя с атрибутами защиты объекта, по отношению к которому запрашивается операция.

При этом рекомендуется применять следующие организационные меры защиты:

- доступ в контролируемые зоны должен предоставляться только авторизованному персоналу железнодорожного предприятия;
- размещение оборудования в местах доступа посторонних лиц должно быть выполнено таким образом, чтобы исключить возможность неавторизованного доступа, хищения или повреждения. При невозможности такого размещения рекомендуется принять меры к тому, чтобы оборудование не оставалось без контроля со стороны уполномоченного персонала;

- запрет на вынос оборудования и носителей информации с территории железнодорожного предприятия без соответствующего разрешения;
- меры защиты для предотвращения неавторизованного доступа к оборудованию, повреждения или утери оборудования и носителей информации при организации работы оборудования вне контролируемых зон, а также при транспортировке носителей информации за пределами территории железнодорожного предприятия.

### 7.3 Средства криптографической защиты информации

В целях подтверждения авторства электронных документов, проверки целостности программного и информационного обеспечения, идентификации пользователей ИР и ИТИ, шифрования/расшифрования блоков оперативной памяти, файлов, электронных документов, сетевых пакетов или сетевого трафика используются средства криптографической защиты информации, ресурсы сервера открытых ключей, если таковые предусмотрены (в соответствии с законодательством государства-члена ОСЖД).

### 7.4 Межсетевые экраны

Одними из основных элементов защиты ИР и ИТИ от НСД при межсетевом взаимодействии являются межсетевые экраны, основанные на принципах фильтрации сетевых адресов и пакетов.

Межсетевой экран (МЭ) предназначен для защиты внутренней сети организации от несанкционированного сетевого доступа и решает следующие задачи:

- фильтрацию сетевых пакетов в соответствии с задаваемыми администраторами правилами;
- осуществление передачи IP-пакетов по принципу «запрещено всё, что не разрешено» что защищает от нападений, основанных на новых, незнакомых или неясных IP-сервисах, а также ошибок конфигурации;
- трансляцию сетевых адресов отправителя и получателя в туннеле, скрывающую внутренние адреса субъекта и объекта передачи;
- возможность сокрытия прикладных функций защищаемой сети и используемых сетевых протоколов, топологии сети и факта функционирования МЭ как средства защиты с фильтрующими возможностями;
- специфическую обработку IP-опций, способствующую предохранению от раскрытия извне топологии корпоративной сети железнодорожного предприятия (интранет);
- защиту каналов управления и мониторинга пограничных маршрутизаторов;
- учет и регистрацию действий администраторов и различных параметров работы абонентов;

- функционирование комплекса с использованием защищенной операционной среды для исключения несанкционированной модификации и осуществления разрушающих программных воздействий;
- автоматический контроль целостности исполняемых модулей;
- возможность удаленного управления работой МЭ, мониторинг состояния, изменение правил фильтрации и др.

Приоритетом использования являются МЭ нового поколения (NGFW), основными отличительными особенностями которых являются:

- использование пользователей и приложений как критериев фильтрации;
- интеграция технологии фильтрации трафика с технологиями защиты от компьютерных атак.

### 7.5 Средства мониторинга и контроля защищенности

Обязательными элементами защиты современных корпоративных сетей должны быть средства мониторинга и контроля защищенности ИТИ.

Средства мониторинга и контроля защищенности предназначены для обеспечения выявления возможных уязвимостей и контроля защиты информации в ИТИ на уровнях системного и прикладного программного обеспечения, а также защиты от атак на корпоративные сети со стороны открытых сетей передачи данных.

Принцип мониторинга и контроля защищенности заключается в следующем. На защищаемые элементы интрасети (компьютеры, серверы и т.д.) устанавливаются программные драйверы – агенты, которые контролируют соблюдение политики безопасности и значения настроек защиты соответствующих ресурсов. При отклонениях от нормы эти агенты фиксируют изменения и передают их на серверы безопасности и консоль администратора безопасности. Если программное обеспечение или программно-технические средства, имеют соответствующие встроенные механизмы мониторинга и контроля защищенности (например, сетевые коммутаторы, средства защиты информации), то события безопасности передаются на серверы безопасности штатными средствами.

Мониторинг и контроль защищенности заключается в возможности проведения периодического анализа защищенности узлов и сегментов корпоративной сети на предмет наличия в них уязвимостей и заблаговременного их устранения.

Средства мониторинга и контроля защищенности включают:

- средства контроля (анализа) защищенности, включая:
  - сканеры безопасности, содержащие обновляемые актуальные базы известных уязвимостей и механизмы выявления таких уязвимостей в системном и прикладном ПО, веб-серверах, сетевом оборудовании;
  - средства контроля правильности установки и настройки программного обеспечения, позволяющие выявлять небезопасные конфигурации ОС и

ППО, на основе анализа их состава, версий, значений параметров настройки и пр.;

- средства мониторинга сетевых и хостовых потоков информации, включая:
  - средства учета сетевого трафика, позволяющие формировать статистические данные по сетевому трафику;
  - средства анализа содержимого сетевого трафика (DLP-системы), направленные на предотвращение утечек конфиденциальной информации;
  - специализированные средства обнаружения компьютерных атак (системы обнаружения вторжений, СОВ);
- средства контроля соответствия элементов СОИБ принятым национальным стандартам в области защиты информации и политикам ИБ, включая:
  - специализированные средства контроля соответствия параметров и характеристик элементов ИТИ принятым национальным стандартам в области защиты информации и политикам ИБ;
  - специализированные средства контроля операционных систем, прикладного программного обеспечения, средств и механизмов защиты, в том числе встроенные в ОС и ППО (шаблоны доменных политик, средства от производителей конкретных ОС и ППО);
  - средства контроля целостности программного обеспечения, обеспечивающие регулярный контроль неизменности состава и настроек ОС и ППО;
- компоненты управления средствами мониторинга и контроля защищенности;
- компоненты формирования отчетов по состоянию информационной безопасности.

Структурно средства мониторинга и контроля защищенности состоят из следующих компонент:

- клиентской части – агентов, функционирующих на подконтрольных объектах (компьютерах и серверах) и осуществляющих контроль объектов посредством регистрации событий и исполнения управляющих административных команд;
- серверной части (выделенных серверов) для сбора информации от агентов или встроенных средств мониторинга и анализа полученной информации;
- консолей администраторов безопасности – выделенных компьютеров для мониторинга и управления средствами защиты и формирования отчетов по состоянию информационной безопасности.

### 7.6 Защита клиент-серверных технологий

Клиент-серверные технологии представляют основной класс технологий в распределенных вычислительных системах при работе пользователей с разделяемыми ресурсами.

Так как серверы с ресурсами и клиенты в них нуждающиеся, как правило, территориально разнесены, основными проблемами защиты в этих технологиях

являются проблемы идентификации и аутентификации пользователей и серверов, а также проблемы защиты доступа к серверам со стороны несанкционированного пользователя во время сеанса с санкционированным пользователем.

Проблемы идентификации и аутентификации в открытых и корпоративных сетях решаются при помощи использования цифровых сертификатов и средств криптографической защиты информации (в соответствии с законодательством государства-члена ОСЖД). Каждый сервер и каждый клиент имеют соответствующее программное обеспечение, цифровые сертификаты и криптографические ключи, обеспечивающие их однозначную идентификацию и надежную аутентификацию.

Защита сеансов и непрерывности потоков между клиентом и сервером обеспечивается с использованием специальных защитных протоколов обработки информации, а также криптографических механизмов защиты информации, основанных на использовании цифровых сертификатов (в соответствии с законодательством государства-члена ОСЖТ).

### 7.7 Средства антивирусной защиты

Корпоративные вычислительные сети железнодорожных предприятий включают в себя тысячи компьютеров, десятки серверов, активное и пассивное телекоммуникационное оборудование и имеют сложную структуру. С ростом количества элементов сети увеличивается вероятность возможности ее заражения вредоносными компьютерными программами, что может привести, в том числе, к дезорганизации функционирования сети.

Для того чтобы обезопасить корпоративные сети от заражения вредоносными компьютерными программами, необходимо выявлять и контролировать все возможные каналы их проникновения в сеть:

- проникновение вредоносных компьютерных программ на компьютеры с помощью зараженных переносимых источников, например, съемных машинных носителей информации;
- заражение вредоносными компьютерными программами с помощью инфицированного программного обеспечения, полученного из Интернет;
- заражение вредоносными компьютерными программами со стороны удаленных зараженных компьютеров или серверов, подключенных к корпоративной сети;
- инфицирование с помощью зараженных вложений электронной почты или ссылок на вредоносные сайты.

К основным принципам построения систем антивирусной защиты для корпоративных систем относятся: комплексный подход к созданию системы антивирусной защиты и централизованное управление антивирусной защитой.

Корпоративные системы антивирусной защиты железнодорожных предприятий должны обладать следующими функциональными возможностями:

- возможность обнаружения вредоносных компьютерных программ;

- возможность обнаружения деструктивного кода типа «троянский конь»;
- готовность быстрого реагирования на появление новых видов угроз (эвристический анализ);
- обслуживание и поддержка;
- список защищаемых точек возможного проникновения вредоносных компьютерных программ;
- администрирование, управляемость, поддержка;
- управление антивирусной защитой удаленных пользователей;
- централизованное уведомление;
- высокая производительность системы;
- удаленное администрирование;
- обновление (ПО и базы признаков компьютерных вирусов) и др.

### 7.8 Системы и средства управления инцидентами информационной безопасности

Для реализации управления инцидентами ИБ рекомендуется реализация следующих мер:

- обнаружение и идентификация инцидентов на основе результатов мониторинга событий безопасности информации;
- своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в ИТИ;
- анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;
- планирование и принятие мер по устранению инцидентов, в том числе по восстановлению элементов ИТИ и ИР в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;
- планирование и принятие мер по предотвращению повторного возникновения инцидентов.

Для выявления инцидентов информационной безопасности, а также контроля выполнения мероприятий по управлению инцидентами ИБ могут применяться специализированные средства автоматизации.

### 7.9 Защищенные узлы подключения к Интернет и иным открытым сетям

Обеспечение возможности безопасного подключения ИР и ИТИ железнодорожных предприятий к глобальной сети Интернет или другим открытым сетям целесообразно реализовать за счет применения технологии построения защищенных узлов доступа, включающей в себя:

- разбиение сети на специализированные сегменты (административный сегмент, демилитаризованную зону, пользовательские сегменты);
- обмен информацией между сегментами в зашифрованном виде;
- использование при создании клиентских сегментов технологии VLAN или других способов сегментирования;
- использование для серверов средств защиты от НСД;
- реализацию механизма оперативного пополнения баз данных признаков компьютерных атак (решающих правил), выявленных недостатков в известном программном обеспечении;
- реализацию возможности оперативного реагирования на атаки;
- реализацию возможности постепенного наращивания архитектуры за счет введения дополнительных проверок правильности работы сетевых фильтров, усиления средств авторизации и аутентификации пользователей и т.д.

В состав средств защищенного узла доступа также могут включаться:

- система обнаружения вторжений, обеспечивающая защиту ресурсов ЛВС (например, компьютеров, серверов ЛВС, Web-серверов, МЭ) от атак злоумышленников и авторизованных пользователей как через сети передачи данных, так и внутри ЛВС;
- система анализа защищенности сетевых сервисов и протоколов (сканеры безопасности);
- средства обеспечения исключения (запрета) передачи защищаемой информации из корпоративной сети железнодорожного предприятия в открытые сети.

### 7.10 Защита против физического проникновения в компоненты ИР и ИТИ

Для реализации защиты от физического проникновения в компоненты ИР и ИТИ рекомендуется выполнить следующие основные мероприятия:

- выбор инженерно-технических средств физической защиты объектов систем, отдельных технических средств этих систем, исключающих несанкционированный доступ к объектам, техническим средствам, их хищение и нарушение работоспособности;
- выбор технических средств защиты против физического проникновения в компоненты ИР и ИТИ.

# 8 РАЗРАБОТКА СТРУКТУРЫ СИСТЕМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИР И ИТИ

## 8.1 Основные задачи системы информационной безопасности ИР и железнодорожных предприятий

Система обеспечения информационной безопасности ИР и ИТИ железнодорожных предприятий позволяет осуществить:

- поддержку высокой доступности обрабатываемой информации для пользователей ИР и ИТИ в соответствии с предоставленными им правами и полномочиями;
- защиту обрабатываемой информации от несанкционированного удаления, изменения, ознакомления и копирования;
- защиту компьютеров, серверов и телекоммуникационного оборудования от несанкционированного доступа к их ресурсам;
- поддержку конфиденциальности, контроля целостности и подтверждения подлинности электронных документов при помощи средств шифрования и электронной (цифровой) подписи (в соответствии с законодательством государства-члена ОСЖД);
- комплексный подход к применению специализированных аппаратных, программных и аппаратно-программных средств и систем защиты;
- контроль целостности информационного обеспечения, общего и специального программного обеспечения для его защиты от несанкционированного изменения;
- защиту программного обеспечения и данных от вредоносных компьютерных программ (вирусов);
- регистрацию и протоколирование действий пользователей и приложений, ведение системного аудита, мониторинг действий пользователей на автоматизированных рабочих местах системы;
- администрирование и контроль использования ресурсов в системе;
- централизованное управление идентификационными параметрами, аутентификационной информацией и криптографическими ключами в соответствии с законодательством государства-члена ОСЖД, установленным регламентом и требованиями эксплуатационных документов;
- защиту информации при ее передаче по каналам связи корпоративных компьютерных сетей железнодорожного предприятия.

## 8.2 Структура и функции системы обеспечения информационной безопасности ИР и ИТИ железнодорожных предприятий

Структура системы обеспечения информационной безопасности и функции ее подсистем должны быть разработаны так, чтобы обеспечить масштабирование и наращивание ее функций при вводе в ИР и ИТИ новых функциональных подсистем.

Система обеспечения информационной безопасности ИР и ИТИ может включать следующие основные компоненты:

- подсистему защиты информации от несанкционированного доступа;
- криптографическую подсистему;
- подсистему контроля защищенности;
- подсистему антивирусной защиты.

Подсистема защиты информации от НСД может иметь многоуровневую распределенную структуру и предназначена для обеспечения идентификации и аутентификации субъектов доступа в ИТИ, управления доступом субъектов доступа к объектам доступа в ИТИ, регистрации событий безопасности и других функций, направленных на предотвращение НСД на всех функциональных уровнях ИТИ.

Криптографическая подсистема защиты информации должна обеспечивать выполнение функций шифрования/расшифрования, формирование и проверку электронной (цифровой) подписи документов, криптографическую идентификацию и аутентификацию пользователей ИР и ИТИ железнодорожных предприятий (в соответствии с законодательством государства-члена ОСЖД).

Подсистема контроля защищенности должна обеспечивать анализ защищенности сетевой операционной системы, СУБД, выделенных сегментов и рабочих станций ЛВС, обнаружение уязвимостей в используемых программных и технических средствах, обнаружение и блокирование атак из сети Интернет, оповещение администратора безопасности об обнаруженных атаках, формирование отчетов по состоянию безопасности.

Подсистема антивирусной защиты должна обеспечивать антивирусную защиту рабочих станций, файловых серверов, баз данных, электронной почты, шлюзов (узлов доступа) Интернет и иных ИР и ИТИ железнодорожных предприятий.

**Подсистема защиты информации от несанкционированного доступа к ИР и ИТИ** железнодорожных предприятий должна обеспечивать:

- защиту ИР и ИТИ от НСД со стороны внешних телекоммуникационных сетей;
- защиту ИР и ИТИ от НСД на уровне защищаемых сегментов ЛВС;
- защиту от НСД на уровне разграничения доступа механизмами сетевых операционных систем;
- защиту от НСД на уровне разграничения доступа механизмами систем управления базами данных;

- защиту компьютеров программно-техническими комплексами защиты от НСД;
- администрирование средств информационной защиты;
- регистрацию системных событий и попыток НСД к защищаемым ресурсам;
- оперативное оповещение администраторов безопасности о попытках НСД.

Поддержка технических решений по НСД, в рамках реализации установленных политик информационной безопасности в ИР и ИТИ железнодорожных предприятий, должна обеспечиваться комплексом взаимоувязанных мер нормативно-распорядительного, организационного и технического характера.

***Защита от НСД со стороны внешних телекоммуникационных сетей*** обеспечивается выбором соответствующей топологии сети, использованием средств разграничения доступа, контролем данных и фильтрацией трафика на канальном, сетевом, транспортном и прикладном уровнях протокола TCP/IP.

Основными мероприятиями при этом являются разбиение сети на отдельные сегменты (административный сегмент, демилитаризованную зону, и т.д.), использование маршрутизаторов, межсетевых экранов и коммутаторов, а также других мер и средств защиты.

Для исключения возможности использования неавторизованных каналов доступа в систему путем целесообразно отключить все неиспользуемые сетевым и телекоммуникационным оборудованием протоколы, сервисы, порты. Данную меру рекомендуется реализовать, в первую очередь, в пограничных устройствах доступа из сети Интернет к ИР и ИТИ железнодорожных предприятий.

***Защита от НСД на уровне защищаемых сегментов ЛВС*** обеспечивается в рамках сегментирования ИТИ железнодорожных предприятий, разграничения доступа к сетевым ресурсам за счет последовательного применения ряда маршрутизаторов, межсетевых экранов, коммутаторов и других мер защиты.

Одной из важнейших задач в этом плане является организация защищенного доступа к внутренним сегментам ИТИ через коммутаторы с поддержкой фильтрации сетевого уровня, фактически выполняющих функции внутренних маршрутизаторов, регламентирующих процесс обмена между сегментами ИТИ, межсетевые экраны, а также с использованием систем обнаружения вторжений и средств защиты от «отказа в обслуживании».

Кроме физического разбиения сети на сегменты возможно создание логических сегментов с помощью технологии виртуальных сетей. Принцип организации таких сетей заключается в добавлении поля в стандартный заголовок Ethernet-фрейма, которое содержит номер виртуальной сети, к которой относится данный фрейм. При этом непосредственное обращение машин из одной виртуальной сети к другой виртуальной сети возможно только согласно разрешенным маршрутам.

Доступ к сегменту сети (демилитаризованной зоне), в котором располагаются потенциально уязвимые сетевые службы, осуществляется с использованием межсетевых экранов или коммутаторов с функцией фильтрацией сетевых пакетов, межсетевых

экранов уровня веб-сервера (WAF).

***Защита от НСД на уровне разграничения доступа механизмами сетевой ОС*** достигается за счет использования в полном объеме встроенных механизмов безопасности сетевых операционных систем, прошедших процедуру оценки соответствия в соответствии с законодательством государства-члена ОСЖД. Использование этих механизмов осуществляется во взаимосвязи с другими механизмами защиты в рамках единой политики информационной безопасности ИР и ИТИ железнодорожных предприятий.

Политика безопасности на уровне ОС должна обеспечивать решение двух основных задач:

- «ужесточение» настроек ОС, приводящее к изменению ее конфигурации с целью повышения уровня безопасности системы в целом;
- удаление компонентов операционной системы, не нужных для функционирования системы в рамках выполняемых задач.

В результате этого уменьшается набор компонентов, которые необходимо поддерживать в актуальном состоянии, и уменьшается количество возможных точек атаки нарушителя.

Для реализации этих задач необходимо устанавливать ОС со всеми имеющимися к ней обновлениями, особенно обновлениями, относящимися к вопросам безопасности информации. Необходимо исключать возможность неадекватных полномочий доступа к системной информации критичного характера за счет использования процедуры ручной проверки прав доступа к системным файлам. Затем необходимо вручную исключать из операционных сетевых систем излишние компоненты.

Для контроля правильности настроек ОС и заблаговременного обнаружения уязвимостей рекомендуется использование средств контроля защищенности ОС.

***Защита от НСД на уровне разграничения доступа механизмами СУБД*** обеспечивается путем использования в полном объеме встроенных механизмов безопасности СУБД. Реализация политики безопасности на уровне СУБД аналогична подходу к безопасности ОС.

В этом случае рекомендуется устанавливать версию СУБД со всеми имеющимися обновлениями. После установки этих обновлений необходимо постоянно поддерживать СУБД в актуальном состоянии, периодически устанавливая на неё новые обновления, в частности те, которые имеют отношение к безопасности СУБД.

Кроме того, рекомендуется исключить возможную неадекватность атрибутов доступа к объектам системы, исключить компоненты, не требующиеся для обеспечения работы в рамках выполняемых задач, отключить или сменить пароли для встроенных учетных записей СУБД, периодически удалять неиспользуемые учетные записи пользователей СУБД, и проводить ряд других взаимоувязанных мер в рамках реализации единой политики информационной безопасности ИР и ИТИ железнодорожных предприятий.

Для контроля правильности настроек и возможностей заблаговременного обнаружения уязвимостей СУБД, рекомендуется использование средств контроля защищенности СУБД.

***Защита от НСД компьютеров ИР и ИТИ*** железнодорожных предприятий достигается использованием средств защиты, осуществляющих следующие действия, например:

- идентификацию и аутентификацию пользователей по электронному идентификатору и паролю;
- контроль целостности программного и информационного обеспечения;
- запрет загрузки операционной системы со съемных машинных носителей информации;
- разграничение доступа пользователей к ресурсам компьютера.

***Регистрация критичных системных событий*** в ИТИ должна обеспечиваться средствами защиты от НСД и средствами контроля защищенности в автоматизированном режиме, путем записи информации о времени, характере и другой информации об этих событиях в системные регистрационные журналы.

Оперативный анализ событий, происходящих в системе, должен осуществляться на основе анализа администраторами ИР и ИТИ журналов регистрации системных событий и журналов аудита.

Некоторые средства защиты, например средства обнаружения атак в реальном масштабе времени, обладают встроенными механизмами оперативного оповещения администраторов о критичных событиях путем выдачи этой информации на консоль управления, передачи ее по электронной почте или, например, путем SMS-оповещений.

**Подсистема криптографической защиты информации системы ИР и ИТИ** железнодорожных предприятий может иметь распределенную структуру и обеспечивать выполнение следующих функций:

- шифрование (расшифрование) данных на компьютерах пользователей ИР и ИТИ;
- формирование (проверку) электронной цифровой подписи и шифрование (рашифрование) данных, при их передаче между абонентами ИР и ИТИ, а также доступе к информационным ресурсам железнодорожных предприятий.

Построение подсистемы криптографической защиты выполняется в соответствии с законодательством государств-членов ОСЖД.

**Подсистема контроля защищенности ИР и ИТИ** железнодорожных предприятий может включать следующие основные элементы:

- систему обнаружения вторжений;
- систему анализа защищенности на уровне сети Интернет;
- систему анализа защищенности на уровне операционной системы;
- систему анализа защищенности на уровне СУБД.

***Система обнаружения вторжений может включать:***

- программно-технические средства, позволяющие эффективно и с высоким быстродействием обнаруживать и блокировать внешние атаки;
- программные средства, позволяющие выполнять обнаружение и блокирование атак в реальном масштабе времени во внутренних сегментах ИТИ, производимых злоумышленниками как снаружи, так и изнутри ИТИ, а также регистрировать все операции, проводимые при осуществлении атаки для последующего анализа.

При этом решаются следующие задачи:

- обнаружение атак, имеющих целью «обойти» существующие защитные механизмы. К таким атакам могут быть отнесены: сканирование портов и использование сканеров безопасности, атаки типа «подбор пароля» и «отказ в обслуживании», использование «троянских коней», несанкционированное подключение к сети и т.д.;
- анализ сетевого трафика, включающего изучение информационных потоков, используемых сетевых протоколов и т.д.;
- анализ данных, поступающих от маршрутизаторов, коммутаторов и МЭ;
- оповещение в реальном масштабе времени администратора безопасности через консоль управления, электронную почту или путем SMS-оповещений об обнаруженной атаке;
- регистрация атак в журнале для дальнейшего воспроизведения и анализа и т.д.

***Система анализа защищенности на уровне сети Интернет*** предназначена для решения одного из важных аспектов управления сетевой безопасностью – выявления уязвимостей. При помощи данной системы следует проводить регулярные всесторонние или выборочные тесты сетевых сервисов, операционных систем, прикладного программного обеспечения, маршрутизаторов, межсетевых экранов, Web-серверов и т.п. Таким образом, система может выполнять следующие действия:

- проведение инвентаризации ИР и ИТИ;
- обнаружение в ИР и ИТИ уязвимостей, позволяющих обойти существующие защитные механизмы (к таким уязвимостям могут быть отнесены: неправильная конфигурация сетевого оборудования, устаревшее программное обеспечение, неиспользуемые сетевые сервисы, «слабые» пароли и т.д.);
- анализ изменений уровня защищенности ИР и ИТИ и т.д.

***Система анализа защищенности на уровне операционной системы*** должна периодически выполнять анализ защищенности компьютера или сервера по двум направлениям:

- анализ настроек операционной системы, которые могут быть использованы злоумышленниками для осуществления атаки;
- сканируемая система должна проверяться на наличие «следов», уже оставленных злоумышленниками.

***Система анализа защищенности на уровне СУБД*** предназначена для проверки СУБД на наличие недостатков при конфигурировании, которые могут быть использованы злоумышленниками. Проверка в этом случае осуществляется в соответствии с шаблонами, учитывающими различные требования по безопасности баз данных.

***Подсистема антивирусной защиты*** требует использования комплекса средств, обеспечивающих в предлагаемой архитектуре ИР и ИТИ:

- антивирусную защиту средств вычислительной техники;
- антивирусную защиту шлюзов (узлов доступа) Интернет;
- администрирование всех антивирусных продуктов, установленных в сети;
- периодическое обновление программного обеспечения и баз данных признаков вредоносных компьютерных программ.
- анализ сообщений электронной почты;
- централизованное администрирование средств антивирусной защиты.

## 9 ВЕДЕНИЕ ДЕЛ ПО ПАМЯТКЕ

Ведение дел по Памятке осуществляется Постоянной рабочей группой ОСЖД «Кодирование и информатика».