такой сложной модели с любой заданной точностью. Однако стремление переносить на масштабный план объекты съемки с точностью, обеспечиваемой электронным тахеометром, не приводит к ожидаемым результатам. Следует отметить, что геодезические изыскания, выполненные на некоторый момент времени T_0, указывают только на соответствие положения стрелочных переводов, сигналов, предельных столбиков данному моменту времени T_0 (например, 10 сентября 2005 года 11^{45}).

Устройства путевого развития железнодорожной станции – это совокупность тесно взаимодействующих и в то же время пространственно слабозакрепленных объектов. Постоянные несбалансированные, разновекторные нагрузки от движущегося подвижного состава приводят к сдвигам верхнего строения пути относительно балластной призмы, балластной призмы относительно земляного полотна, земляного полотна относительно основания станционной площадки. Учитывая высокую точность проводимой съемки (10^{-3} – 10^{-5} м), можно утверждать, что спустя некоторое, весьма непродолжительное время координаты контрольных точек съемки, указанные на электронном масштабном плане станции, не будут соответствовать их реальному положению.

Цифровые технологии позволяют обеспечить обратную связь «электронная схема станции – путевое развитие станции». При наличии выделенных реперов, координаты которых будут корректироваться посредством глобальной навигационной связи или в другом режиме, положение остальных объектов путевого развития может быть рассчитано аналитически путем сопоставления значений старых и новых координат. Постоянная связь между геосъемкой реперов и цифровым масштабным планом станции осуществляется посредством специального узкопрофильного программного обеспечения, что позволит поддерживать масштабный план в актуальном виде с полным соответствием всех объектов натурным данным.

Реализация данной технологии имеет огромное значение для формирования надежных и безопасных систем. В условиях высокой динамичности транспортной нагрузки, неопределенной прогнозной ситуации постоянное наблюдение за дрейфом реперов позволит упреждать различные нештатные и аварийные ситуации. Если, например, в одной горловине фиксируется перемещение остряков стрелочных переводов в противоположных направлениях, то это свидетельствует об увеличении внутреннего напряжения в рельсовой колее с ожиданием негативных последствий. Мониторинг состояния объектов путевого развития поможет качественно планировать объем и последовательность ремонтно-профилактических работ в путевом хозяйстве, что, в конечном итоге, позволит повысить качество эксплуатационной работы в целом.

УДК 681.322-181.4:656.2

ПРОБЛЕМЫ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ НА ЖЕЛЕЗНОЙ ДОРОГЕ

П. Г. ДЕМИДОВ, П. В. ПАЛТО, В. И. ГАНАКОВ, С. И. ПАРАНИН
Белорусский государственный университет транспорта

Особенности защиты персональных компьютеров (ПК) обусловлены спецификой их использования. Как правило, ПК пользуется ограниченное число пользователей. ПК могут работать как в автономном режиме, так и в составе локальных сетей (сопряженными с другими ПК) и могут быть подключены к удаленному ПК или локальной сети с помощью модема по телефонной линии.

Стандартность архитектурных принципов построения, оборудования и программного обеспечения персональных компьютеров, высокая мобильность программного обеспечения и ряд других признаков определяют сравнительно легкий доступ профессионала к информации, находящейся в ПК. Если персональным компьютером пользуется группа пользователей, то может возникнуть необходимость в ограничении доступа к информации различных потребителей.

В настоящее время на железнодорожном транспорте всё больше используется микропроцессорная техника и компьютеры, объединяемые в компьютерные сети. В связи с последними событиями в мире существует опасность компьютерного терроризма.

В случае, если управление удаленными объектами (ЭЦ, станцией, трансформаторной подстанцией) будет производиться из единого центра управления, существует вероятность постороннего воздействия (компьютерного терроризма) на передаваемую информацию с использованием сетей соединения между этими объектами: искажение посланных команд, внесение помех, радиоатака, заражение компьютерными вирусами.

Хорошо оснащенным противником может быть предпринята атака еще одного вида, предполагающая удаленный перехват побочного электромагнитного излучения и наводок (сокращенно - ПЭМИН), испускаемого вашим компьютером. Эта дорогая и часто трудоемкая атака, вероятно, является более дешевой, чем криптоанализ.

Соответствующим образом оборудованный фургон может припарковаться рядом с центром управления и издалека перехватывать нажатия клавиш и сообщения, отображаемые на мониторе компьютера. Это скомпрометирует все ваши пароли, сообщения и т.п. Такая атака может быть предотвращена соответствующим экранированием всего компьютерного оборудования и сетевых кабелей с тем, чтобы они не испускали излучения. Технология такого экранирования известна под названием Tempest и используется рядом правительственных служб и организаций, выполняющих оборонные заказы.

Кроме того, можно использовать специальные генераторы "белого шума" для защиты от ПЭМИН, например: ГБШ-1, Салют, Пелена, Гром и др.

Ущерб от террористических действий в сетевой среде связан:

– с человеческими жертвами или материальными потерями, вызванными деструктивным использованием элементов сетевой инфраструктуры;

– возможными потерями (в том числе гибелью людей) от несанкционированного использования информации с высоким уровнем секретности или сетевой инфраструктуры управления в жизненно важных (критических) для государства сферах деятельности;

– затратами на восстановление управляемости сети, вызванными действиями по ее разрушению или повреждению;

– моральным ущербом как владельца сетевой инфраструктуры, так и собственного информационного ресурса;

– другими возможными потерями от несанкционированного использования информации с высоким уровнем секретности.

Крупнейшие кибератаки последних лет привели к опасным сбоям в работе телекоммуникационных сетей, зачастую угрожающим критическим объектам физической инфраструктуры государств, нанесли значительный материальный ущерб. О величине убытков от успешных атак на национально значимые сферы хозяйственного комплекса можно судить, например, по результатам инцидентов в 2003 году, связанных с перебоями в электроснабжении крупных регионов США и Канады или нарушениями в системе авиаперевозок в Англии. Потери измерялись сотнями миллионов долларов, а уровень социальной напряженности влиял на политическую обстановку в странах. Имеются убедительные свидетельства, что террористы использовали Интернет при планировании своих акций 11 сентября 2002 года.

В 1985 году в Японии леворадикальная группировка с помощью компьютерных систем предприняла атаку на единую сеть управления железной дорогой. К счастью, у компьютеров железной дороги оказалась надежная защита, взломать которую не удалось.

Для обеспечения безопасности движения поездов необходимо предусмотреть защиту от несанкционированного доступа. Несанкционированным доступом (НСД) к информации ПК будем называть незапланированное ознакомление, обработку, копирование, применение различных вирусов, в том числе разрушающих программные продукты, а также модификацию или уничтожение информации в нарушение установленных правил разграничения доступа. В защите информации ПК от НСД можно выделить три основных направления:

– первое ориентируется на недопущение нарушителя к вычислительной среде и основывается на специальных технических средствах опознавания пользователя;

– второе связано с защитой вычислительной среды и основывается на создании специального программного обеспечения по защите информации;

– третье связано с использованием специальных средств защиты информации ПК от несанкционированного доступа.

Для защиты персональных компьютеров используются различные программные методы, которые значительно расширяют возможности по обеспечению безопасности хранящейся информации. Среди стандартных защитных средств персонального компьютера наибольшее распространение получили:

- средства защиты вычислительных ресурсов, использующие парольную идентификацию и ограничивающие доступ несанкционированного пользователя;
- применение различных методов шифрования, не зависящих от контекста информации;
- средства защиты от копирования коммерческих программных продуктов;
- защита от компьютерных вирусов и создание архивов.

УДК 658.2.08:002+658.012.011.56

ПОВЫШЕНИЕ БЕЗОПАСНОСТИ СИСТЕМ ДОКУМЕНТООБОРОТА В БРЕСТСКОМ ПОГРАНИЧНОМ ПЕРЕГРУЗОЧНОМ РАЙОНЕ ПОСРЕДСТВОМ ВНЕДРЕНИЯ ЭЛЕКТРОННОЙ ПОДПИСИ

С. П. КАЛЮТЧИК
Белорусская железная дорога

Мировой опыт показывает высокую эффективность электронизации документооборота с применением электронной цифровой подписи (ЭЦП) в транспортных системах для решения самого широкого спектра задач, включая проблемы обеспечения безопасности. Правовая база для использования ЭЦП в Республике Беларусь создана еще в 2000 году после принятия закона «Об электронном документе». Ст. 12 указанного закона гласит, что ЭЦП предназначена для удостоверения информации, составляющей общую часть электронного документа, подтверждения подлинности и целостности электронного документа. Таким образом, основной смысловой нагрузкой ЭЦП является аутентификация документа и обеспечение требований информационной безопасности при его подготовке, передаче, исполнении и хранении. Основой для реализации указанного проекта служит использование ведомственной системы электронной цифровой подписи (ЭЦП). Разработка ядра системы применения электронной цифровой подписи будет закончена в ближайшее время Управлением Белорусской железной дороги.

Учитывая, что безопасность перевозок определяет уровень качества транспортного обслуживания, внедрение ЭЦП на железнодорожном транспорте будет способствовать привлечению дополнительных объемов транзитных перевозок, что является задачей общегосударственной важности. Выполняя эту задачу, Белорусская железная дорога присоединилась к Четырехстороннему проекту с участием немецких, польских и российских железных дорог. Проект разрабатывается с целью увеличения грузопотока по Второму международному транспортному коридору. Особое место в этом проекте отводится Брестскому пограничному перегрузочному району как пункту стыковки железнодорожной колеи различной ширины и как западным воротам Республики Беларусь, стран СНГ и Азии.

В Основных направлениях развития информационных технологий Белорусской железной дороги на 2005 год намечено создание в Брестском пограничном перегрузочном районе опытного полигона для внедрения систем электронного документооборота на основе ЭЦП. К сожалению, правовая база ОСЖД, в рамках которой организуются международные перевозки по Второму транспортному коридору, еще не позволяет отказаться от традиционных бумажных документов. Учитывая это ограничение, разрабатываемые в Бресте информационные технологии предполагают организацию электронного документооборота только внутри пограничного перегрузочного района.

Новая информационная технология предусматривает выдачу ЭЦП каждому работнику, который подписывает документы в ходе технологического процесса. Отправной точкой этой технологии является пункт передачи вагонов (ППВ) станции Брест–Восточный, где производится «электронизация» комплектов бумажных перевозочных и сопроводительных документов, с которыми прибывают грузовые отправки, следующие в направлении Запад–Восток. Для этого технологический персо-