Сопряжение автоматизированных информационных систем, применяемых для безопасности объектов метрополитена

Корнеев Николай Владимирович,
заведующий кафедрой информационной безопасности и программной инженерии РГСУ, д.т.н., профессор, член-корр. РАЕН, почётный учёный Европы

Башлыкова Анна Александровна,
аспирантка

При всем многообразии функциональных видов автоматизированных систем (АС) одним из требований к ним является обеспечение безопасности информации, т.е. речь идет об автоматизированных системамх в защищенном исполнении.

В свете развития в нашей стране процессов государственного регулирования различных сфер деятельности внимание различных государственных органов в первую очередь обращено на различные объекты со средоточением большого количества людей. Примерами таких объектов могут выступать метрополитены, которые должны обеспечивать безопасную перевозку пассажиров, соответствовать требованиям санитарно-гигиенических норм и безопасных условий труда для обслуживающего персонала, охраны окружающей среды и противопожарным требованиям, согласно Строительным нормам и правилам РФ. Метрополитены (СНиП 32-02-2003).

Метрополитен как объект управления — крупная, сложная, работающая при наличии помех нелинейная система, в которой одновременно задействовано большое количество подвижного состава, различного рода транспортных систем, которые, в свою очередь, должны работать слаженно и четко. О сложности метрополитена как объекта управления свидетельствуют следующие признаки:

- многообразие структурных подразделений, высокая степень централизации, взаимосвязанность и необходимость синхронизации действий различных служб;
- необходимость решения не только отдельных инженерно-экономических задач, но и вопросов долгосрочного планирования и прогнозирования, наличие больших внешних связей системы;
- постоянный рост объема работы и информации, затрудняющий и делающий невозможным для человека полный анализ информации и принятие оптимального решения без ЭВМ.

В современных условиях проблема обеспечения безопасности такого объекта, как метрополитен, выходит в разряд приоритетных, что обусловлено рядом причин, в т.ч.:

рост преступности в стране;

- активизация террористической и диверсионной деятельности националистических и подрывных организаций;
- неуменьшающееся количество несчастных случаев на платформах и прилегающих пространствах, аварий подвижного состава;
- насущная необходимость реструктуризации АС и электросети в соответствии с новейшими информационными технологиями, способствующими появлению оборудования информационно-вычислительного и телекоммуникационного назначения, требующего особой защиты.

Предмет защиты — конкретные объекты метрополитена, подлежащие защите с помощью той или иной системы. К ним относятся:

- люди — персонал объекта, пассажиры;
- материальные и хозяйственные объекты (предметы отделки станций, платформ, оборудование);
- информация, обрабатываемая и хранящаяся в АС;
- система управления эксплуатацией (СУЭ), в состав которой входят системы: обеспечения кондиционирования и вентиляции воздуха; управления эскалаторным оборудованием; контроля основных энергетических показателей; обеспечения экологического мониторинга;
- информация, поступающая от технической системы охраны — системы контроля доступом через турникеты, пожарной сигнализации (СПС); аварийного оповещения и управления эвакуацией персонала и пассажиров (СОУЭ); охранной сигнализации («тревожные кнопки»); видеоконтроля (СВК);
- информация обеспечивающей системы метрополитена: электрочасофикации и синхронизации; проводной радиотрансляции; управления звуком, обеспечивающая местное громкоговорящее вещание и оповещение.

Физическое пространство, где сосредоточены те или иные ценности и объекты метрополитена, во многом определяет возможные действия нарушителя безопасности и ответные мероприятия по предотвращению угроз безопасности объектов метрополитена.

Автоматизированная система управления (АСУ) метрополитеном является комплексом методов и технических средств, которые наиболее четко и полно исполняют функции управления процессом перевозок на основе использования теории управления социально-экологическими системами, экономико-математических методов, а также электронно-вычислительных машин в сочетании с разнообразной техникой регистрации, диагностики и передачи первичной информации в вычислительный центр.

При создании АС перед специалистами по защите информации встает ряд проблем, не решаемых в рамках задач системной интеграции, с использованием существующих на рынке технических средств. Важнейший этап на пути решения проблемы — это ее осознание.

Данная статья посвящена попытке сформулировать часть наиболее распространенных проблем, способных появиться при построении защищенных АС метрополитена и их сопряжении. При этом заметим, что экспертами в этой области довольно часто рассматриваются чисто технические вопросы, а комплекс организационных факторов, также оказывающих влияние на процесс создания АС в защищенном исполнении, остается, как правило, за границами их внимания.

Так, например, принципы построения и оптимизации технической системы охраны (ТСО) объектов метрополитена представляют собой:

- универсальность, предполагающую, что все решения должны быть отработаны и унифицированы;
- комплексность, предполагающую, что используемые приемы работы и применяемые ТС взаимоувязаны между собой, дополняют друг друга по функциональным и техническим показателям;
- разумную достаточность, означающую, что мероприятия по обеспечению безопасности метрополитена должны быть адекватны возможным угрозам со стороны вероятного нарушителя по материально-техническим и кадровым ресурсам;
- оперативность, предполагающую приоритет методов и средств защиты, обеспечивающих быстрое обнаружение и последующую нейтрализацию возможных угроз;
- адаптивность, предусматривающую что методы и средства защиты могут быть достаточно гибко приспособлены к изменениям организационных и технических условий функционирования метрополитена;
- непрерывность, систематичность, означающие, что выбранные решения обеспечат достаточно эффективную круглосуточную защиту объектов АС метрополитена;
- целеустремленность — сосредоточение усилий, направляемых на защиту наиболее ценных ресурсов или наиболее уязвимых участков АС метрополитена;
- многорубежность, предполагающую использование дополнительных пространственных рубежей безопасности или методов защиты для наиболее ответственных, с точки зрения безопасности, помещений и зон (например, базовые помещения систем инженерного обеспечения (СИО): вентиляционная камера, электрощитовая комната, помещения резервного электропитания и диспетчерской службы);
- равнопрочность создаваемых границ безопасности;
- последовательность в использовании соответствующих методов и средств при обнаружении, отражении и ликвидации угроз безопасности (так называемая эшелонированность безопасности);
- совместимость с существующими системами;
- простоту, экологическую чистоту и незаметность («дружественность»), предполагающих, что развертываемая система не создаст дополнительных препятствий для нормального функционирования метрополитена, не потребует очень высокой квалификации и длительной подготовки обслуживающего персонала, не причинит вреда защищаемым материальным ценностям объекта;
- неуязвимость — способность противостоять предпринимаемым попыткам выведения системы из строя;
- документированность, предполагающую регистрацию интересующих событий, связанных с защищаемым объектом, что необходимо для последующего анализа тревожных и нештатных ситуаций и достигнутого уровня защищенности в метрополитене;
- правомерность, означающую, что все применяемые меры организационного и технического характера легальны и юридически обоснованы.

Специфика построения и оптимизации ТСО и АС в метрополитене в том, что необходимо учитывать, что современным системам безопасности присущи все характерные признаки сложных человеко-машинных систем, как то:

- наличие большого числа взаимосвязанных элементов;
- неопределенность из-за неполной информации о потенциальном нарушителе и его действиях;
- субъективизм, связанный с необходимостью принятия человеком важных оперативных решений;
- многообразие условий функционирования (различные условия эксплуатации, наличие естественных и промышленных помех, замкнутость помещения, постоянная вибрация).

Перечисленные сложности могут способствовать возникновению несанкционированной модификации информации о безопасности в АС, что в свою очередь может привести к несанкционированным действиям (неверной маршрутизации или утрате передаваемых данных) или искажению смысла передаваемых сообщений.

Целостность аппаратуры, установленной в метрополитене, нарушается при ее повреждении, похищении или незаконном изменении алгоритмов работы. Угрозы доступности данных возникают в том случае, когда объект (оператор или процесс) не получает доступа к законно выделенным ему службам или ресурсам.

Если в качестве примера обратиться к той части АС, которая занимается обработкой видео-изображений, поступающих с камер, установленных в помещениях метрополитена, то способы воздействия угроз на передаваемые изображения можно подразделить на информационные, программно-математические, физические, радиоэлектронные.

К информационным способам относятся:

- нарушение адресности и своевременности информационного обмена,
- несанкционированный доступ к информационным ресурсам;

- манипулирование информацией (дезинформация, сокрытие или искажение информации);
- незаконное копирование данных в информационных системах;
- нарушение технологии обработки информации.

Программно-математические способы включают:
- внедрение компьютерных вирусов;
- уничтожение или модификацию данных в автоматизированных информационных системах.

Физические способы включают:
- уничтожение или разрушение средств обработки информации и связи;
- уничтожение, разрушение или хищение машинных или других оригинальных носителей информации;
- поставку «зараженных» компонентов автоматизированных информационных систем.

Радиоэлектронными способами являются:
- перехват информации в технических каналах ее возможной утечки;
- радиоэлектронное подавление линий связи и систем управления.

Необходимо отметить, что АСУ по существу представляет собой человеко-машинную систему. Центральной фигурой управления остается человек. Именно он всегда будет определять содержание и характер деятельности АСУ метрополитена — как на стадии ее создания, так и на стадиях ее совершенствования и определения перечня решаемых задач. Человек будет пользоваться результатом обработки информации, которую по его указанию выполнит и выдаст машина для принятия наиболее квалифицированного решения.

АСУ метрополитена состоит из частей и подсистем, обеспечивающих комплексное решение экономических, организационных, технических и математических задач управления перевозками пассажиров. К ним относятся:
- Экономико-организационная модель АСУ метрополитена, которая определяет экономические и организационные основы управления, порядок внутренних и внешних связей в системе, формы воздействия управляющей системы на процесс хозяйственной деятельности метрополитена.
- Информационное обеспечение АСУ метрополитена, которое снабжает службы необходимой входной и выходной технико-экономической информацией, нормативными карточками и ленточками, усовершенствованной нормативно-справочной документацией, данными информационного словаря, классификаторов, шифров кодов, используемых в процессе управления. Информационное обеспечение весьма важная, если не основная, часть АСУ.
- Методическое обеспечение АСУ метро включает инструкции и положения как о системе в целом, так и об отдельных подсистемах управления.
- Математическое обеспечение АСУ метро состоит из комплекса алгоритмов, блок-схем и программ работы ЭВМ.
- Техническое обеспечение АСУ метро включает комплекс вычислительных машин, устройства сбора и передачи информации, средства диспетчеризации, дистанционного управления и контроля за перевозочным процессом, хозяйственной деятельностью линейных предприятий и служб.

АСУ метро должна:
- обеспечивать повышение эффективности работы метрополитена, снижение себестоимости, повышение производительности труда в производственных предприятиях и в управлении, улучшение использования технических средств и производственных фондов;
- оперативно давать руководителям всех рангов и инженерно-техническому персоналу информацию, необходимую для принятия решений по управлению производственно-хозяйственной деятельностью метрополитена;
- обеспечивать комплексную автоматизацию работ по планированию, технической подготовке, регулированию, учету и анализу деятельности всех подразделений метрополитена по реализации плана перевозок пассажиров, снабжению и другим видам деятельности;
- централизованно производить переработку информации, используя эффективные экономико-математические и технические средства, позволяющие принимать оптимальные решения в планировании и организации перевозочного процесса;
- обеспечивать оперативную связь объектов управления с управляющей системой на базе автоматизации сбора, регистрации передачи, накопления и обработки информации;
- использовать в АСУ метрополитена унифицированные документы и технические средства.

Обеспечение безопасности автоматизированных информационных систем зависит от безопасности используемого в них программного обеспечения. Особую опасность представляет уничтожение информации в автоматизированных базах данных и базах знаний. Уничтожается информация на носителях, значительное место в преступлениях против автоматизированных информационных систем занимают взрывы, разрушения, вывод из строя соединительных кабелей, систем кондиционирования.

Уязвимости АС могут быть внесены как на технологическом, так и на эксплуатационном этапах жизненного цикла АС. На технологическом этапе нарушителями могут быть инженерно-технические работники, участвующие в процессе проектирования, разработки, установки и настройки программно-аппаратного обеспечения АС.

Внесение эксплуатационных уязвимостей может иметь место при неправильной настройке и использовании программно-аппаратного обеспечения АС. В отличие от технологических, устранение эксплуатационных уязвимостей требует меньших усилий, поскольку для этого достаточно изменить конфигурацию АС. Характерными примерами уязвимостей этого типа являются:
- наличие слабых, не стойких к угадыванию паролей доступа к ресурсам АС. При активизации этой уязвимости нарушитель может получить несанкционированный доступ к АС путём взлома пароля при помощи метода полного перебора или подбора по словарю;
- наличие в системе незаблокированных встроенных учётных записей пользователей, при помощи которых потенциальный нарушитель может собрать дополнительную информацию, необходимую для проведения атаки. Примерами таких учётных записей являются запись «Guest» в операционных системах или запись «Anonymous» в FTP-серверах;
- неправильным образом установленные права доступа пользователей к информационным ресурсам АС. В случае если в результате ошибки администратора пользователи, работающие с системой, имеют больше прав доступа, чем это необходимо для выполнения их

функциональных обязанностей, то это может привести к несанкционированному использованию дополнительных полномочий для проведения атак;

- наличие в АС неиспользуемых, но потенциально опасных сетевых служб и программных компонентов. Так, например, большая часть сетевых серверных служб, таких как Web-серверы и серверы СУБД, поставляются вместе с примерами программ, которые демонстрируют функциональные возможности этих продуктов. В некоторых случаях эти программы имеют высокий уровень привилегий в системе или содержат уязвимости, использование которых злоумышленником может привести к нарушению информационной безопасности системы. Обычно и технические системы безопасности, и сопряженные автоматизированные системы строятся по централизованному принципу с размещением на определенном месте основной аппаратуры управления и контроля, что позволяет принимать оперативные и наиболее рациональные решения при возникновении нештатных ситуаций. Вместе с тем чрезмерная централизация снижает надежность и живучесть систем. Наглядный пример тому — имевшие место аварии на ТЭЦ или пожар на Останкинской башне, оставившие потребителей без соответствующих услуг.

Для улучшения этих характеристик в АС метрополитена возможно частичное резервирование оборудования центрального поста (сервера) на пространственно удаленном резервном рабочем месте. Данные от АСУ могут быть использованы также на рабочих местах администратора АС, оператора бюро пропусков или сотрудника отдела кадров, диспетчера систем инженерного обеспечения, оператора систем оповещения, выделенного сотрудника службы безопасности метрополитена.

Не все системы и виды связи, определенные СНиП и СП «Метрополитены», обоснованы с точки зрения перспектив. Вместе с тем следует отметить нарастающую необходимость создания централизованной системы информирования пассажиров, включающую систему голосовой связи «пассажир — диспетчер информационного центра» и управляемые из того же центра информационные панели для пассажиров в вестибюлях и на платформах, а также необходимость системы SOS.

Уже сейчас, после первых успешных внедрений в метрополитенах Казани, Москвы, Петербурга, понятно, что современные цифровые системы радиосвязи полностью удовлетворяют насущные и перспективные потребности метрополитенов. Очевидно и то, что поездная и технологическая радиосвязь будут реализовываться на одной аппаратной основе. Выбор стандарта обусловливается эффективностью использования частотного ресурса и обеспечения радиопокрытия всех служебных помещений, вестибюлей станций и тоннелей (что определяется несущей частотой и мощностью радиостанций, а также качеством радиоизлучающего кабеля).

Реализация комплексной системы радиосвязи и полуторагодовой опыт ее эксплуатации в метрополитене г. Казани выявил одну очень острую системную проблему организационного характера, присущую (хотя и в меньшей степени) и системам проводной связи. Ее суть состоит в том, что возможности современных систем связи используются едва ли наполовину, поскольку в метрополитенах пока не организована адекватная им диспетчерская служба.

На всех линиях должны быть следующие виды связи: поездная диспетчерская, поездная радиосвязь, тоннельная, электродиспетчерская, электромеханическая диспетчерская, эскалаторная диспетчерская, радиосвязь диспетчеров с восстановительными формированиями, стрелочная, связь совещаний метрополитена, полицейская, служебная между диспетчерскими пунктами и объектами СЦБ, автоматики, телемеханики, местная в пределах объектов, административно-хозяйственная (автоматическая телефонная), информационная.

Подводя итог, следует заметить и перспективы, например такие, как оплата с помощью банковской карты проезда в метро. При должном подходе участников система может существенно снизить нагрузку на кассовые узлы столичного метрополитена в начале месяца, когда пассажиры обновляют транспортные карты или покупают проездные билеты. Кроме того, преимуществом такого решения является безопасность использования: в случае утери обычного билета владелец не может его восстановить, а кредитную карту можно заблокировать по телефону и восстановить в течение нескольких дней.

В АСУ метрополитена необходимо будет учитывать три действующих лица: транспортный оператор (в данном случае Московский метрополитен), коммерческий банк и расчетный центр (компания, выпускающая карты), который регистрирует информацию о выпущенных картах, получает сведения о прохождении держателей банковских карт через входные турникеты, проводит процедуру сверки рассчитанных сумм по картам с данными транспортного оператора, передает проверенные данные для списаний по картам банку, а также контролирует своевременную загрузку паспортов карт участниками проекта.

Информация между этими участниками системы должна передаваться по скоростным каналам связи; у метрополитена и расчетного центра должны существовать центры обработки данных (ЦОД) для хранения и обработки данных.