БЕЗОПАСНОСТЬ НА ТРАНСПОРТЕ

УДК 656.2.08.

С. П. КАЛЮТЧИК, помощник Начальника Белорусской железной дороги, г. Минск

ОСОБЕННОСТИ ОРГАНИЗАЦИИ РАБОТ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА БЕЛОРУССКОЙ ЖЕЛЕЗНОЙ ДОРОГЕ

Обеспечение информационной безопасности на железнодорожном транспорте является приоритетной задачей , требующей целенаправленных систематических усилий со стороны персонала, специализированных служб, руководителей Белорусской железной дороги, научно-исследовательских и проектных организаций. В статье рассматриваются принципы развертывания и функционирования системы обеспечения информационной безопасности предприятия с учетом общей специфики деятельности железнодорожного транспорта и Белорусской железной дороги конкретно.

Информационная эра привела к глобальным изменениям в методах выполнения своих обязанностей для большого числа профессий. В наше время с использованием достижений информатизации нетехнический служащий среднего уровня может выполнять работу, которую раньше делал высококвалифицированный специалист, имея при этом в своем распоряжении столько точной и оперативной информации, сколько никогда не имел.

Вместе с тем, использование компьютеров и автоматизированных технологий привело к появлению целого ряда организационных, технологических и иных проблем для множества организаций, предприятий и ведомств. Блага, предоставляемые компьютерами, объединенными в единую сеть, оборачиваются иной, порой весьма негативной стороной.

Наличие обобщенных баз данных наряду с удобством доступа к информации, ее хранению, обработке авторизованными пользователями формирует совершенно новые предпосылки нерегламентированного получения информации, причем уже отсортированной по различным признакам и в больших объемах.

Использование сетей передачи электронных данных создает источник самых различных их уязвимостей, что в конечном итоге может привести к модификации сведений либо полному/частичному уничтожению.

Применение элементов «искусственного интеллекта» в системах автоматизированного управления процессами потенциально определяет наличие мощнейших угроз их сбоя, способных вывести из строя любую отрасль, где применяются такие системы, причем с абсолютно непредсказуемыми последствиями.

Таким образом, следует констатировать, что поскольку, по общепринятому мнению, информация в современном мире стала одной из наибольших ценностей, безопасность этой информации является определяющим элементом в самом процессе информатизации.

Кроме того, не следует забывать, что базовые принципы обеспечения безопасности информации, такие, как собственник и владелец информационных ресурсов, информационных систем, объекты права собственности в сфере информатизации, информационные ресурсы, системы и т. д., имеют законодательную основу в большинстве государств и, в частности, в Республике Беларусь, где еще в 1995 году принят закон «Об информатизации».

На фоне этой достаточно непростой картины рассмотрим проблему организации обеспечения безопасности информационных технологий в условиях функционирования железнодорожного транспорта с его специфическими правилами, требованиями и нормами.

Многие вопросы, возникающие при исследовании в этой области, являются в значительной мере риторическими, так как очевидно, что развитие железнодорожного транспорта, одной из наиболее востребованных и интенсивных отраслей мировой экономики, в самой полной мере связано с развитием информационных процессов, а следовательно, информационной безопасности.

Информационные технологии применяются абсолютно во всех сферах деятельности железных дорог, в том числе Белорусской. На основе технологий информатизации уже в настоящее время на Белорусской железной дороге базируются такие ключевые направления, как организация управления движением поездов на полигоне дороги, обеспечение организации и осуществления пассажирских перевозок, решение задач СЦБ, централизованное управление и контроль устройств обеспечения безопасности движения, обработка инфор-

мации по коммерческим задачам, отработка блока финансово-экономических и бухгалтерских вопросов, диспетчерская централизация управления энергетикой и т.п.

Стоящая перед профильными специалистами Белорусской железной дороги проблема модернизации системы управления движением (создание дорожного Центра управления перевозками) требует решения задач информационного обеспечения работы этого подразделения, а следовательно, информационной безопасности, на качественно ином, более высоком уровне.

Очевидно, что нарушение нормального функционирования хотя бы одного из перечисленных направлений деятельности может привести к существенным, а возможно, и фатальным срывам в работе отрасли.

Вместе с тем следует признать, что на Белорусской железной дороге, по сравнению с большинством железнодорожных администраций, являющихся ее партнерами, существует масса проблем в решении актуальных задач обеспечения информационной безопасности на своих предприятиях. К указанным вопросам причастные специалисты начинают подходить только сейчас, при этом сталкиваясь с рядом нюансов и обстоятельств, обусловленных спецификой объекта защиты – структур железнодорожного транспорта.

Общепринятые понятия, принципы, задачи информационной безопасности, пути их решения к настоящему моменту отработаны и достаточно широко известны. Существуют апробированные методики разработки, внедрения и функционирования систем обеспечения информационной безопасности в самых разнообразных организациях.

В общем виде такая деятельность состоит из следующих этапов:

– обследование систем применения информационных технологий на предприятии (в концерне, организации, отрасли и т. п.);

– актуализация перечня угроз информационной безопасности применительно к конкретному объекту защиты;

– определение «узких» мест, или уязвимостей информационных систем;

– разработка типовых профилей защиты предприятия и (или) его структурных подразделений, представляющих из себя основные направления и методы профилактики, выявления, пресечения угроз информационной безопасности в области уязвимости информационных систем объекта защиты;

– разработка общих принципов построения системы обеспечения информационной безопасности на конкретном объекте или его структурном подразделении;

– расчет сил и средств подразделений информационной безопасности объекта. Разработка инструкций, правил, прав и обязанностей работников, связанных с обеспечением информационной безопасности на объекте;

– мониторинг (внешний или внутренний) системы обеспечения информационной безопасности на предмет выявления недостатков этой системы как потенциальных, так и вновь образовавшихся;

– анализ результатов текущей работы, мероприятий по мониторингу, выработка мер совершенствования действующей системы информационной безопасности объекта защиты.

Изложенная выше последовательность действий при создании системы обеспечения информационной безопасности сложилась на основе опыта крупнейших мировых корпораций как специализирующихся в разработке информатизационных продуктов, так и являющихся их потребителями. Как показала практика, общепринятые подходы в данном направлении оказались применимыми в организациях любой сферы деятельности, уровня сложности и иерархической структуры. Возникающие частные обстоятельства, как правило, с учетом конкретных особенностей объекта защиты укладываются в общую схему действий.

Наибольшие отклонения от выработанных механизмов создания системы информационной безопасности объективно проявляются только в некоторых отраслях хозяйственно-экономической деятельности, в том числе на железнодорожном транспорте. Связано это с рядом разноплановых факторов, таких, как особенности структурного построения железнодорожной администрации, специфика действующих технических и технологических нормативов, применение во внутренних перевозках технологических норм, выработанных на международном уровне для международного сообщения и т. п.

Для Белорусской железной дороги данная ситуация оказалась тем более характерна, что Белорусская магистраль в наименьшей степени подверглась организационным и структурным преобразованиям по сравнению с советским периодом, когда вырабатывались действующие ныне основные принципы функционирования железнодорожного транспорта.

К настоящему моменту, когда сложившиеся реалии буквально заставляют начать серьезные разработки вопросов обеспечения информационной безопасности на Белорусской железной дороге, активно проявляются рассогласования между общепринятыми методами, путями организации систем информационной безопасности и организационно-структурными, технологическими, техническими особенностями функционирования Белорусской магистрали.

Рассмотрим последовательность необходимых действий в данном направлении применительно к сложившимся особенностям железнодорожного транспорта Республики Беларусь.

При планировании обследования систем применения информационных технологий специализированное подразделение или организация (имеющие соответствующие лицензии, подготовленных специалистов и опыт работы в данной области) исходят из того, что информационные системы на объекте защиты проектируются, функционируют и развиваются на основе централизованной единой политики. Подобный подход справедлив как для унитарных предприятий, так и для холдингов (или, с точки зрения законодательства Республики Беларусь, объединений), к которым относится и Белорусская железная дорога.

Однако на Белорусской железной дороге сложилась и до настоящего момента функционирует организационная схема существования большого количества юридических лиц (по состоянию на апрель 2006 года 93 юридических лица), привести которые к единым централизованным программам объективно оказалось возможным только по ключевым технологическим задачам. В области же информатизации централизованно развивалось лишь несколько крупных программ, обусловленных технологией эксплуатации железнодорожного транспорта, таких, как автоматизированная система организации управления перевозками (АСОУП), система организации пассажирских перевозок («Экспресс»). Большинство же задач, даже столь важных, как системы бухучета, материального учета, управления процессами теплоэнергетики и т. п., развивалось на уровне юридических лиц по самым разнообразным направлениям.

Таким образом, в ходе обследования систем информатизации Белорусской железной дороги причастным специалистам пришлось в первую очередь проводить учет имеющихся в данных подразделениях сил и средств. Как свидетельствуют полученные результаты, складывающаяся картина существенно отличается от первоначально представлявшейся, что, соответственно, вызывает корректировки действий по всем последующим этапам работы.

Еще более сложной явилась задача актуализации перечня угроз информационной безопасности на конкретных объектах железнодорожного транспорта. Теоретически эта работа заключается в аппроксимации основных известных угроз безопасности информационных систем применительно к структуре, техническим и технологическим процессам, организационным и техническим возможностям конкретного объекта. При этом на первое место выходит задача анализа уже имевшихся сбоев и нарушений (по всем причинам) нормального функционирования информационных устройств. Однако на данном этапе вскрылось следующее значимое обстоятельство: на Белорусской железной дороге во всех без исключения организациях нарушен основной принцип соотнесения работ по информационной безопасности с собственно производственной составляющей информатизационных процессов – разделение производственной и контрольной деятельности.

По существу деятельности в области обеспечения информационной безопасности следует понимать, что работа в данном направлении в первую очередь является режимной и контролирующей. В Республике Беларусь подобный подход закреплен в решениях межведомственных структур, уполномоченных организовывать работу по указанному вопросу на государственном уровне. В частности, в 2004 году Межведомственной комиссией при Совете безопасности Республики Беларусь было поддержано предложение Совета Министров Республики Беларусь о том, что обеспечение информационной безопасности в органах государственного управления и организациях, подчиненных правительству Республики Беларусь, следует организовывать на основе режимных подразделений с использованием опыта работы по защите информации закрытого характера.

В части же, касающейся Белорусской железной дороги, реализация действующих в настоящее время минимальных необходимых требований информационной безопасности находится в ведении подразделений информатизации (вычислительные центры, отделы и группы информационных технологий). Очевидно, что в таком случае работниками указанных подразделений предпринимаются существенные усилия для придания латентного характера любым сбоям и отклонениям от нормального функционирования информационных систем и аппаратуры. Это ведет к тому, что наряду с невозможностью проведения учета и анализа сбоев, а также потенциальных угроз информационной безопасности, отсутствует почва для проведения компетентных расследований информатизационных инцидентов, установления в них объективной и субъективной составляющих и, что наиболее важно, выявления возможных умышленных действий, лежащих в основе таких инцидентов. В подобных условиях для качественного решения стоящих задач необходимо в работах по актуализации угроз информационной безопасности на объекте защиты максимально широко задействовать независимых специалистов, компетентных в технологических процессах конкретного объекта. Это дает возможность наиболее полно в сложившихся условиях соотнести потенциальные угрозы информационной безопасности с особенностями функционирования объекта защиты,

выделить характерные для данного объекта защиты угрозы, на недопущение и пресечение которых должно быть направлено первоочередное внимание при разработке профиля защиты.

Деятельность по определению угроз объекту защиты по сути представляет собой сортировку актуальных и потенциальных угроз по параметрам отношения к ущербу, который эти угрозы могут причинить объекту защиты с учетом конкретных условий функционирования объекта. Критерии этой деятельности в общем виде могут быть представлены в виде формулы

$$\frac{A}{B}\,k > 1,$$

где A – затраты, которые необходимо будет понести при возникновении поражения объекта от вредоносного фактора; B – затраты, необходимые для локализации угрозы и (или) устранения ее последствий; k – коэффициент условий функционирования объекта, включающий как объективные обстоятельства (технические и технологические особенности, правовое поле деятельности объекта защиты), так и субъективные (волевые стремления руководства по организации работ в сфере информационной безопасности).

Коэффициент k может варьироваться в пределах от 0 до 1. Если принять его за константу для конкретного объекта защиты, то критерий выбора угрозы будет зависеть только от параметров A и B. В отношении выделенных угроз, удовлетворяющих вышеприведенным условиям, и должна строиться деятельность по разработке систем защиты.

Особенности реализации данного этапа на железнодорожном транспорте, в первую очередь, определяются крайне разнородным составом составляющих коэффициента условий функционирования объекта защиты (k). Действительно, различные предприятия железнодорожного транспорта, входящие в структуру одной железнодорожной администрации, в частности Белорусской железной дороги, существенно различаются по техническим особенностям функционирования, по технологиям, применяющимся в производственном процессе, а также по регламентирующей правовой базе.

Для примера обратимся к функционированию сортировочной станции и вагонного депо. Для данных структурных подразделений отделения железной дороги справедливы различия по всем приведенным в предыдущем абзаце критериям. Соответственно разнятся и информационные задачи, задействованные в процессе работы этих предприятий. Однако оба они входят в топологию системы информатизации железной дороги, что, в свою очередь, определяет необходимость увязки общепринятых принципов обеспечения информационной безопасности с типовыми ведомственными требованиями в данной области, а также с конкретными условиями профиля защиты информационных систем конкретного предприятия.

В части, касающейся этапа мониторинга системы обеспечения информационной безопасности железной дороги, справедливо следующее.

Под мониторингом понимается практическая проверка системы на наличие критичных уязвимостей методами, идентичными применяемым субъектами угроз информационной безопасности. Таким образом, осуществляющей мониторинг структурой моделируется санкционированная внешняя и (или) внутренняя атака на информационную систему, а также производятся иные неблагоприятные воздействия, аналогичные последствиям реализации актуальных угроз информационной безопасности. В случае неадекватной реакции системы можно говорить о недостатках в обеспечении ее безопасного функционирования.

Вместе с тем, необходимо учитывать и тот факт, что железнодорожный транспорт является организацией непрерывного функционирования, объектом повышенной опасности, а также местом массового пребывания людей. Очевидно, что при таких условиях применять активный мониторинг информационных систем, жизненно важных для функционирования предприятий железнодорожного транспорта, тем самым искусственно создавая условия их отказа, недопустимо. Поэтому на данном этапе ключевое значение приобретает работа по виртуальному моделированию аварийных ситуаций, расчету оптимального пути их нейтрализации, а также органичному внедрению полученных наработок в действующие технологии информационного процесса и работ по обеспечению его безопасности.

В заключение хотелось бы остановиться на юридически-правовых аспектах, имеющих значение для организации деятельности по обеспечению информационной безопасности и в наибольшей степени характерных именно для Белорусской железной дороги.

Как было сказано выше, обеспечение информационной безопасности, по сути, в значительной степени является режимной деятельностью, т. е. деятельностью, вводящей определенные ограничительные требования. Такого рода работа в обязательном порядке должна быть выверена и согласована с действующей нормативной базой как государственной, так и ведомственной. Вместе с тем, на железнодорожном транспорте по сравнению с подавляющим большинством отраслей народного хозяйства в наибольшей степени действуют регламенты, основанные на международных и межправительственных соглашениях. Причем

это касается как организационных, так и чисто технологических, производственных аспектов деятельности железнодорожного транспорта.

Основные правила перевозок грузов и пассажиров, правила технической эксплуатации пути, подвижного состава, устройств безопасности, СЦБ и связи, энергетики и т.п. едины для железнодорожных администраций либо в рамках Совета по железнодорожному транспорту, либо Организации сотрудничества железных дорог. Наряду с этим, предприятия конкретной железнодорожной администрации ведут свою деятельность в соответствующем государственном правовом и нормативном поле, которые, как правило, существенно различаются. Таким образом, в построении системы режимной деятельности в сфере защиты информационных систем приходится учитывать все эти зачастую трудно совместимые факторы.

Указанное положение справедливо для всех железнодорожных администраций государств-членов Совета по железнодорожному транспорту и ОСЖД. Однако в наибольшей степени это касается Белорусской железной дороги, являющейся транзитной дорогой и по существу своего производственного процесса вынужденной теснейшим образом сотрудничать во всех причастных областях как с ближайшими соседями, так и с отдаленными железнодорожными администрациями (например железными дорогами Монголии).

Таким образом, при разработке требований системы обеспечения информационной безопасности необходимо увязывать их не только с положениями национального законодательства, но и с действующими железнодорожными организационно-технологическими условиями международного характера.

Практика показала, что в ходе работы по созданию полноценно работающей системы обеспечения информационной безопасности Белорусской железной дороги большая часть усилий будет затрачена не на реализации общих усредненных штампов и подходов к этой работе, а именно на адаптации полученных результатов к особенностям функционирования железнодорожного транспорта Республики Беларусь. Тем более значимая и непростая задача стоит перед причастными специалистами, которые должны быть в полном смысле этого слова экспертами в двух таких специфичных областях, как информационные технологии и железнодорожный транспорт. Именно умение эффективно работать на стыке отраслей и определит успех деятельности в данном вопросе.

Получено 28.09.2006

S. P. Kalyutchik. Particular Features of Organizing Activities to Provide Information safety at the Belarusian Railway.

In the article we view some principles of unfolding and functioning of the system that provides information safety of an enterprise while taking into account general specific features of railway transport activities and of the Belarusian Railway in particular. Approaches and rules of unfolding the systems that provide information safety are reviewed from the standpoint of international practice in this field. The norms of such activities are adapted for the conditions of the Belarusian Railway taking into account both specific features of the railway transport and state norms currently in force.

Вестник Белорусского государственного университета транспорта: Наука и транспорт. 2006. № 1-2(12-13)

УДК 656.2.08

Д. В. КАПСКИЙ, кандидат технических наук; Е. Н. КОТ, старший преподаватель; С. Н. КАРАСЕВИЧ, аспирант; Белорусский национальный технический университет, г. Минск

ИССЛЕДОВАНИЕ ОПАСНОСТИ ВЗАИМОДЕЙСТВИЯ ПЕШЕХОДНЫХ И ПОВОРОТНЫХ ТРАНСПОРТНЫХ ПОТОКОВ МЕТОДОМ КОНФЛИКТНЫХ СИТУАЦИЙ

Статья посвящена решению проблемы обеспечения безопасности дорожного движения на регулируемых перекрестках при организации конфликтного движения поворотного транспорта и пешеходов. Выполнен анализ дорожно-транспортных происшествий в ряде крупных городов стран Содружества Независимых Государств. С использованием метода конфликтных ситуаций прогнозирования аварийности на конфликтных объектах проанализированы существующие варианты организации дорожного движения в Республике Беларусь. Рассмотрены результаты экспериментальных исследований конфликтных ситуаций, возникающих на пешеходных переходах г. Минска и г. Гродно. Приведены результаты исследований конфликтного взаимодействия и техническое решение рассматриваемого вопроса. В результате исследований даны рекомендации по совершенствованию управления на таких объектах улично-дорожной сети, приведены мероприятия и технические средства для повышения эффективности движения.