УДК 004.056

МЕТОДЫ И МОДЕЛИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТОВ ТРАНСПОРТНОЙ ИНФРАСТРУКТУРЫ, ОТНЕСЕННЫХ К КРИТИЧЕСКИ ВАЖНЫМ ДЛЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РФ ОБЪЕКТАМ

Соколов С.С.

ФГБОУ ВО «Государственный университет морского и речного флота имени адмирала С.О. Макарова», Санкт-Петербург, Россия (198035, г. Санкт-Петербург, ул. Двинская, 5/7), e-mail: sokolovss@gumrf.ru.

В статье рассматривается законодательное представление понятия «объект информатизации», «транспортная безопасность», «критически важные объекты». На основании такого рассмотрения делается вывод о необходимости обеспечения комплексной безопасности объектов информатизации на транспорте как критически важных объектов, основываясь на эффективном синтезе методов обеспечения информационной и транспортной безопасности. Проблема комплексного обеспечения их безопасности связана с многогранностью процессов их функционирования и управления ими и включает в себя все четыре вида защиты: правовая, техническая, криптографическая и физическая. В целях исключения избыточности в реализации защитных мер информации можно говорить о первостепенной необходимости проработки физических мероприятий по защите объектов информатизации, которые должны рассматриваться с точки зрения минимизации общей избыточности, включая и программно-аппаратные способы защиты. Также в статье приведено описание процесса оценки уязвимостей и угроз транспортных объектов, приведена классификация таких угроз. Вторая часть статьи полностью посвящена методам и моделям обеспечения безопасности транспортных объектов, при этом объект, на которое направлено действие, рассматривается как совокупность из трех составляющих: объект транспортной инфраструктуры, транспортное средство, груз (или пассажиры).

Ключевые слова: критически важные объекты, безопасность объектов транспортной инфраструктуры, объекты информатизации транспортной сферы, безопасность на транспорте, безопасность транспортных средств.

METHODS AND MODELS OF ENSURING INFORMATION SECURITY OF THE OBJECTS OF TRANSPORT INFRASTRUCTURE REFERRED TO OBJECTS, CRUCIAL FOR NATIONAL SECURITY OF THE RUSSIAN FEDERATION

Sokolov S.S.

FPBE U HE «Admiral Makarov State University of Maritime and Inland Shipping», St. Petersburg, Russia (198035, St. Petersburg, Dvinskaya St., 5/7), e-mail: sokolovss@gumrf.ru

In article legislative representation of the concept "object of informatization", "transport safety", "crucial objects" is considered. On the basis of such consideration the conclusion about need of ensuring complex safety of objects of informatization on transport as crucial objects, based on effective synthesis of methods of ensuring information and transport security is drawn.The problem of complex ensuring their safety is connected with versatility of their functioning processes and management of them and includes all four types of protection: legal, technical, cryptographic and physical. For a redundancy exception in realization of protective measures of information it is possible to speak about paramount need of physical study actions for protection of informatization objects which have to be considered from the point of view minimization of the general redundancy, including also hardware-software ways of protection.Also the description of process an assessment of vulnerabilities and threats of transport objects is provided in article, classification of such threats is given.The second part of article is completely devoted to methods and models of safety of transport objects, thus the object on which action is directed is considered, as set from three components: object of transport infrastructure, vehicle, freight (or passengers).

Keywords: crucial objects, safety of transport infrastructure objects, objects of informatization of the transport sphere, safety on transport, safety of vehicles.

Вопросы обеспечения информационной безопасности объектов транспортной инфраструктуры в последние несколько лет находятся на первом месте во всех процессах жизнедеятельности транспортной отрасли. Особенную роль безопасность на транспорте стала

играть в связи с взаимной интеграцией российского и западного рынков и в условиях конкурентной борьбы [1].

Интенсификация транспортных процессов ставит новые задачи, решение которых необходимо повсеместно сопровождать современным технологическим ростом [3], это все, как следствие, порождает новые угрозы и необходимость формирования обновленной основы для их предотвращения.

Безопасность объектов транспортной инфраструктуры

Согласно ГОСТ Р 51275-2006 «Защита информации. Объект информатизации…» под «объектом информатизации понимается совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией…». Федеральный закон от 9 февраля 2007 г. № 16-ФЗ «О транспортной безопасности» определяет понятие транспортной безопасности следующим образом: «транспортная безопасность – состояние защищенности объектов транспортной инфраструктуры и транспортных средств от актов незаконного вмешательства». В связи с предпосылками, заложенными на законодательном уровне, можно говорить, что понятие комплексного обеспечения безопасности объектов транспортной инфраструктуры (ОТИ) как объектов информатизации тесно связано с понятием обеспечения транспортной безопасности и во многом зависит от принятых мер обеспечения безопасности автоматизированных систем управления (АСУ) ОТИ [2, 4, 9], так и мероприятий обеспечения физической защиты.

Транспортная безопасность и критически важные для национальной безопасности РФ объекты

В последние годы приняты соответствующие Федеральные законы и подзаконные акты, регламентирующие деятельность в области обеспечения транспортной безопасности, определяющие угрозы безопасности и механизмы их предотвращения, а также устранения последствий в случае наступления внештатных, чрезвычайных ситуаций.

В соответствии с «Основными направлениями государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации» (утв. Президентом Российской Федерации Д. Медведевым 3 февраля 2012 г., № 803) под критически важным объектом инфраструктуры РФ понимается «объект, нарушение (или прекращение) функционирования которого приводит к потере управления, разрушению инфраструктуры, необратимому негативному изменению (или разрушению) экономики страны, субъекта Российской Федерации либо административно- территориальной единицы или существенному ухудшению безопасности жизнедеятельности населения, проживающего на этих территориях, на длительный срок».

При обеспечении безопасности ОТИ необходимо учитывать, что в соответствии с методикой отнесения объектов государственной собственности к критически важным объектам (КВО), утвержденной министерством по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий, для национальной безопасности Российской Федерации ряд ОТИ относятся к КВО, в первую очередь, в связи с тем, что среди них подавляющее большинство являются организациями, обеспечивающими функционирование инфраструктуры общегосударственного значения, в частности, железнодорожного, авиационного и морского транспорта. Проблема комплексного обеспечения их безопасности связана с многогранностью процессов их функционирования и управления ими и включает в себя все четыре вида защиты, определённые в ГОСТе ФСТЭК РФ «Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах…» (далее - Требования): правовая, техническая, криптографическая и физическая. Также указанные Требования определяют и роль физических мер в структуре мер обеспечения безопасности: «в целях исключения избыточности в реализации защитных мер информации, если принятые в ОИ меры по физической безопасности (СФЗ – система физической защиты) обеспечивают блокирование 4 угроз безопасности информации, отдельные меры защиты информации могут не применяться». Таким образом, можно говорить о первостепенной необходимости проработки физических мероприятий по защите ОИ, которые должны рассматриваться с точки зрения минимизации общей избыточности, включая и программно-аппаратные способы защиты.

Структура объекта информатизации транспортной отрасли

Проведенный анализ действующего законодательства позволил определить объект информатизации, на который направлено действие по обеспечению информационной и транспортной безопасности в рамках данного исследования, как совокупность трех взаимосвязанных составляющих: объект транспортной инфраструктуры (ОТИ), транспортное средство (ТС), груз (или пассажиры).

В соответствии с методикой отнесения объектов государственной собственности к критически важным объектам для национальной безопасности Российской Федерации, на основании п.3 «Состав и содержание исходных данных для проведения расчетов» можно считать, что объекты транспортной сферы относятся к критически важным по принципу вхождения в группу «Организации, обеспечивающие функционирование инфраструктуры общегосударственного значения, в частности информационно-коммуникационные, электросвязи и почты, железнодорожного, авиационного и морского транспорта, магистральных газо- и нефтепроводов, инженерные сооружения (мосты, тоннели)».

На основе проведенного анализа федерального и ведомственного законодательства (норм и правил), в рамках комплексного обеспечения защищенности объектов транспортной инфраструктуры, можно сделать вывод о необходимости создания единой комплексной системы обеспечения управления, информационной безопасности и безопасности функционирования ОТИ и ТС.

Для достижения поставленной цели, в первую очередь, необходимо определить концепцию и модель обеспечения информационной безопасности и защиты информации, обрабатываемой в процессе функционирования ОТИ и ТС, которая преследовала бы цель: эффективный синтез имеющегося программно-аппаратного обеспечения процессов безопасного функционирования транспортной отрасли [5, 8].

Оценка уязвимости и угроз транспортных объектов

Для правильного понимания безопасности как состояния защищённости системы необходимо определить возможные уязвимости системы и угрозы, направленные на ее дестабилизацию.

Алгоритм обеспечения оценки данных уязвимостей, включает следующие основные этапы (рис. 1).

На основе оценки уязвимостей, анализа законодательства РФ и анализа чрезвычайных ситуаций можно определить следующие основные угрозы безопасности ОТИ: угроза захвата; угроза взрыва; угроза размещения или попытки размещения взрывных устройств; угроза поражения опасными веществами; угроза захвата критического элемента ОТИ; угроза взрыва критического элемента ОТИ; угроза размещения или попытки размещения на критическом элементе ОТИ взрывных устройств; угроза блокирования; угроза хищения; угроза разглашения.

Обеспечения безопасности транспортных объектов

Далее необходимо определить более развернутые характеристики и структуры понятий обеспечения безопасности составных элементов объекта информатизации, на который направлено действие по обеспечению информационной и транспортной безопасности в рамках данного исследования.

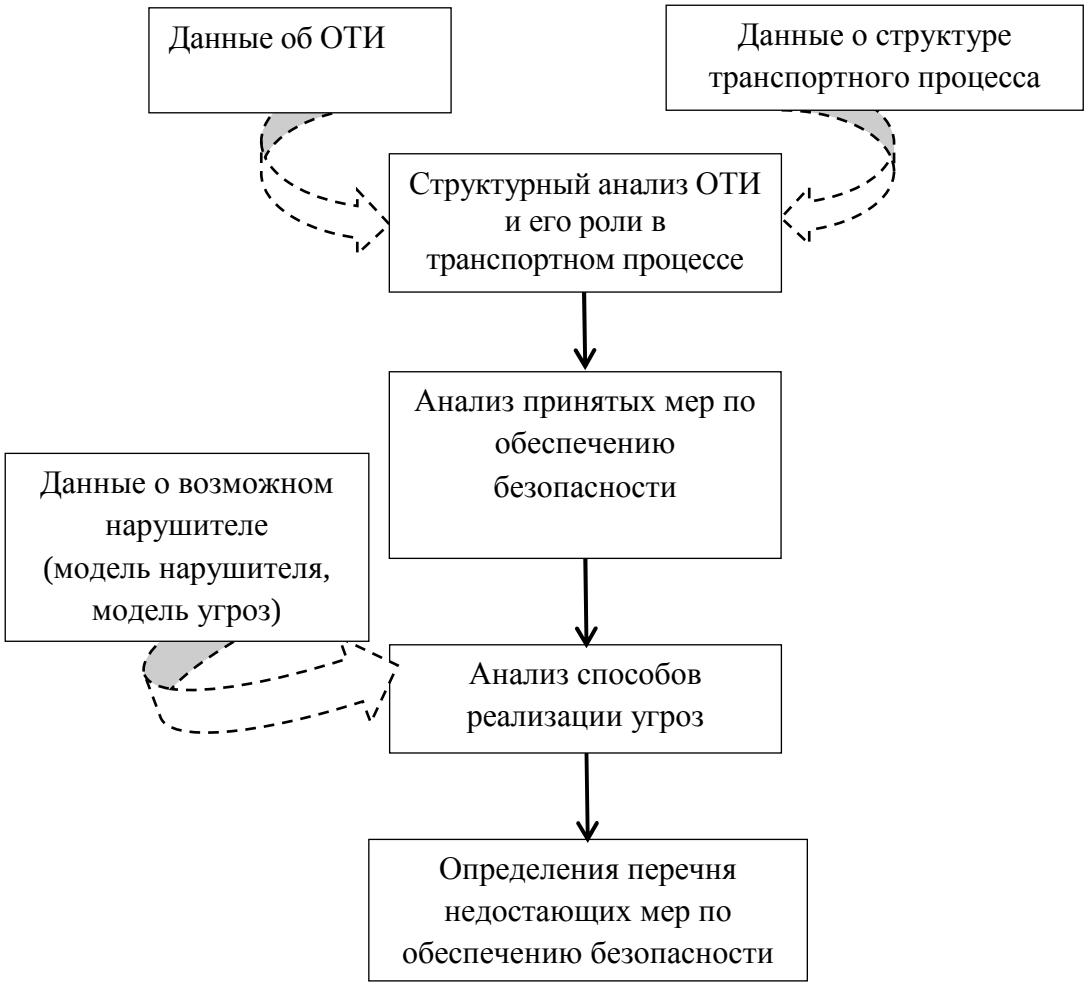

Рис. 1. Алгоритм оценки уязвимостей ОТИ

Так, в частности, безопасность функционирования ОТИ очень сильно зависит от характера объектов и их взаимодействия с внешней средой. Если исключить груз и транспортные средства из понятия транспортной инфраструктуры, то можно определить следующие объекты, рассмотрение которых приводится в первой части обеспечения информационной и транспортной безопасности: транспортные пути (дороги, ж/д пути, моря и реки, воздушные коридоры, трубы), транспортно-логистические узлы [7].

Обеспечение безопасности автомобильных дорог и железнодорожных транспортных путей должно основываться в первую очередь на качестве их строительства (прокладки) и поддержания, а также на принятых мерах антитеррористической защиты, что выходит за рамки данной работы. В случае с рассматриваемыми в работе видами транспортных путей речь в основном идет о строительстве на стабильных почвах, требующих применения стандартных методов прокладки, крепления и т.д. Воздушные пути не требуют прокладки (в физическом смысле этого процесса).

Совершенно другие обстоятельства на водном транспорте: водные пути внутреннего водного транспорта для обеспечения гарантированных глубин требуют выбора отдельных технологий и техники для прокладки, что зачастую недостаточно финансируемо и весьма

зависимо от местности.

На внутренних водных путях основным методом обеспечения заданных габаритов судовых ходов и улучшения судоходных условий являются дноуглубительные работы. Дноуглубительные работы выполняются с помощью землечерпательных снарядов (земснарядов), которые извлекают и удаляют грунт с затруднительных для судоходства участков речного русла.

Безопасность транспортно-логистического узла (ТЛУ) определяется в первую очередь защитой территории самого узла и прилегающих территорий, потенциально опасных для осуществления противоправных действий. Безопасность ТЛУ в широком смысле представляет собой систему комплексных мер по обеспечению безопасности ТЛУ, транспорта и сотрудников.

Основное направление обеспечения безопасности ТЛУ заключается в обеспечении безопасных условий труда персонала и своевременности, а также правильности осуществления операций с грузом и транспортом, особенно в аварийно-опасных зонах. В том числе сюда входит минимизация вредных для здоровья человека воздействий.

Другой стороной обеспечения безопасности ТЛУ является повышение уровня оперативности и корректности устранения последствий катастроф, реализации противоправных действий, ошибок машин/механизмов, персонала и других узлов.

Правильное обеспечение безопасности ТЛУ возможно при реализации следующих мероприятий:

- обучение и аттестация сотрудников на курсах транспортной и промышленной безопасности;
- своевременная и правильная идентификация угроз и величины последствий их реализации;
- составление модели нарушителя;
- разработка системы обеспечения безопасности ТЛУ, включающей в себя нормативно-правовой, организационный и программно-технический компоненты;
- выделение достаточного объема средств и реализация разработанной системы;
- своевременное обновление ресурсов ТЛУ;
- проведение регулярных проверок готовности персонала и технических средств к внештатным ситуациям.

Безопасность ТС зависит от трех основных факторов:

- безопасность транспортной единицы;
- безопасная эксплуатация транспорта;
- безопасность транспортных путей.

Безопасность транспортной единицы зависит в свою очередь и от производителя и от кампании, занимающейся сервисное обслуживание [10].

По вопросу безопасной эксплуатации транспорта существует достаточно много руководящих документов и стандартов. Здесь мы имеем в качестве основных следующие предпосылки: человеческий фактор, необходимость снижения рисков возникновения чрезвычайных ситуаций, рассмотрению которых последнее время посвящается много работ как в области профессиональной и психологической подготовки, так и в области создания автоматизированных систем управления транспортом.

Что же касается безопасности транспортных путей – здесь много субъективных факторов появляется при рассмотрении конкретного вида транспорта. Более подробно рассмотрим вопросы эксплуатации водных транспортных артерий. Основные задачи стоят при обеспечении внутренних водных путей (ВВП).

Под безопасностью груза можно понимать как его физическую сохранность, так и экологическую безопасность.

Физическая сохранность груза включает как вопросы физической охраны, так и вопросы правильного размещения и дальнейшей перевозки. Вопросы рационального размещения груза должны быть рассмотрены отдельно [6].

Рассматривая безопасную перевозку особо опасных грузов можно отметить, что согласно данным ООН доля опасных грузов в мировом грузообороте постоянно растет и в настоящее время достигает почти половины его. С перевозками опасных грузов связан существенный потенциал рисков возникновения чрезвычайных происшествий. Актуальна необходимость в мероприятиях по сведению этого потенциала к уровню остаточных рисков, приемлемому для общества и государства.

Заключение

В заключении следует отметить, что к обеспечению безопасности объектов транспортной инфраструктуры необходимо подходить комплексно. Только при согласованном участии несколько ведомств возможно и нужно разработать систему мер, средств и механизмов формирования среды централизованного взаимодействия всех участников транспортного процесса в защищенном исполнении, основанной на принципах физической, нормативно-правовой, программно-технической, криптографической защиты.

При организации такой системы централизованного управления и централизованного обеспечения безопасности следует учитывать, что понятие безопасности объекта транспортной инфраструктуры является комплексным и объединяет в себе меры как транспортной, так и информационной безопасности, рассматривая при этом объект, на который направлено действие по обеспечению безопасности, как структурный объект с

различными составными частями разного уровня организации и с разными принципами функционирования и управления.

Список литературы

1. Ныркov А.П. Автоматизация управления мультимодальными перевозками / Ныркov А.П., Соколов С.С., Ежгуров В.Н., Мальцев В.А. // Вестник государственного университета морского и речного флота им. адмирала С.О. Макарова. – 2013. - № 2. – С. 74-78.
2. Ныркov А.П. Помехозащищенность как фактор обеспечения стабильной работы сети передачи данных на транспорте / Ныркov А.П., Соколов С.С., Белоусов А.С. // Сборник научных трудов Sworld. – 2013. – Т. 8. - № 1. – С. 5-9.
3. Ныркov А.П. Автоматизированное управление транспортными системами / Ныркov А.П., Соколов С.С., Шнуренко А.А. – СПб., 2013 – 325 стр.
4. Соколов С.С. Функциональная структура автоматизированной системы управления транспортно-складской инфраструктурой / Соколов С.С., Беляева Н.А. // Вестник государственного университета морского и речного флота им. адмирала С.О. Макарова. – 2012. - № 3. – С. 124а-129.
5. Соколов С.С. Математическое и алгоритмическое обеспечение оперативного управления транспортно-логистическими комплексами / Соколов С.С. // диссертация на соискание ученой степени кандидата технических наук / Государственный университет морского и речного флота имени адмирала С.О. Макарова. – СПб., 2011.
6. Соколов С.С. Математическая модель рационального размещения груза в трюмах судна / Соколов С.С. // Вестник государственного университета морского и речного флота им. адмирала С.О. Макарова. – 2010. - № 3. – С. 89а-92.
7. Соколов С.С. Модель угроз информационной безопасности организаций / Соколов С.С. // Вестник государственного университета морского и речного флота им. адмирала С.О. Макарова. 2009. № 2. С. 176-180.
8. Соколов С.С. Процесс обеспечения транспортной безопасности как объект автоматизации / Соколов С.С. // Фундаментальные исследования. – 2014. - № 11-1. – С. 46-51.
9. Чёрный С.Г. Применение механизма информационных интеллектуальных моделей в системах автоматического управления / Чёрный С.Г. // Вестник Херсонского национального технического университета. – 2012. - № 1 (44). – С. 215-220.

10. Черный С.Г. Системный анализ процессов синергетики для судоходной отрасли / Черный С.Г. // Транспорт: наука, техника, управление. – 2014. - № 8. – С. 12-15.

Рецензенты:

Ныркov А.П., д.т.н., профессор, заведующий кафедрой «Комплексное обеспечение информационной безопасности автоматизированных систем», ФГБОУ ФО «ГУМРФ имени адмирала С.О. Макарова», г. Санкт-Петербург;

Гаскаров В.Д., д.т.н., профессор, профессор кафедры «Комплексное обеспечение информационной безопасности автоматизированных систем», ФГБОУ ФО «ГУМРФ имени адмирала С.О. Макарова», г. Санкт-Петербург.