АВТОМАТИЗИРОВАННЫЙ КОМПЛЕКС СРЕДСТВ ОБЕСПЕЧЕНИЯ АНТИТЕРРОРИСТИЧЕСКОЙ БЕЗОПАСНОСТИ НА ПРИМЕРЕ ТРАНСПОРТНОГО КОМПЛЕКСА

Кононов А.А., Стиславский А.Б., Цыгичко В.Н., Черешкин Д.С.

УДК 004.94

Кононов А.А., Стиславский А.Б., Цыгичко В.Н., Черешкин Д.С. **Автоматизированный комплекс средств обеспечения антитеррористической безопасности на примере транспортного комплекса.**

Аннотация. В статье описывается созданный коллективом разработчиков ИСА РАН аппаратно-программный комплекс «РискДетектор», реализующий в режиме диалога ЭВМ—пользователь основные процедуры обеспечения транспортной безопасности, определенные директивными документами. Идеология комплекса была разработана и опубликована ранее и предполагает, что система управления рисками нарушения транспортной безопасности строится на основе категорирования объектов транспортной инфраструктуры и транспортных средств путем оценки возможного ущерба при реализации угроз террористического воздействия.

Ключевые слова: антитеррористическая безопасность, риски нарушения транспортной безопасности, управление рисками, профили защиты, оценка уязвимости, модель угроз.

Kononov A.A., Stislavskiy A.B., Tsygichko V.N., Chereshkin D.S. **The automated complex of means of maintenance of antiterrorist safety on an example of a transport complex.**

Abstract. Hardware-software complex «RiskDetektor» (ISA of Russian Academy of Sciences) is described in the article. This Complex realizes in a mode of dialogue the computer—the user the basic procedures of maintenance of the transport safety, defined by directive documents. The ideology of a complex has been developed and published earlier and assumes that the control system of risks of infringement of transport safety is constructed on a basis of categorization of transport objects by an estimation of a possible damage at realization threats of terrorist influence.

Keywords: counterterrorist safety, risks of transport security, a risk management, profiles of protection, vulnerability estimation, a model of threats.

1. Введение. В настоящее время одним из главных приоритетов государства в области обеспечения национальной безопасности страны является борьба с растущими террористическими угрозами. Антитеррористическая борьба предполагает, прежде всего, активизацию деятельности государства по защите инфраструктуры и населения страны от террористических проявлений, в том числе и в транспортном комплексе. Опасные объекты транспортной инфраструктуры России в разной степени защищены от террористических угроз в соответствии с требованиями, принятыми в каждом виде транспорта. Однако, как показывает печальный опыт в нашей стране и за рубежом, этой защиты оказывается недостаточно для предотвращения крупных техногенных катастроф и террористических актов. До настоящего времени в стране не существует эффективной системы выработки требова-

ний к защите объектов транспортной инфраструктуры на основе мониторинга угроз транспортной безопасности. Практически отсутствуют централизованная система мониторинга состояния безопасности опасных объектов транспортной инфраструктуры и система контроля выполнения требований по обеспечению транспортной безопасности. Решение этих задач должна взять на себя создаваемая в настоящее время единая система обеспечения транспортной безопасности страны, функционирование которой предусмотрено федеральным законом «О транспортной безопасности».

Первым шагом на этом пути должно стать решение актуальной научной проблемы — создание методологии, методического инструментария и программных средств для выработки требований по обеспечению безопасности объектов транспортной инфраструктуры и мониторинга полноты и качества выполнения этих требований. В статье описывается аппаратно-программный комплекс, реализующий основные процедуры обеспечения безопасности на транспорте на основе разработанной авторами концепции.

2. Основные положения Концепции обеспечения транспортной безопасности. Использованная при создании аппаратно-программного комплекса (АПК) концепция обеспечения безопасности объектов транспортной инфраструктуры и транспортных средств на основе категорирования опубликована [1–3] и обсуждалась на двух Международных форумах по безопасности. Кратко рассмотрим только ряд основных ее положений.

Для определения минимального объема финансовых средств, необходимых для создания и эксплуатации единой государственной системы обеспечения транспортной безопасности, и рационального распределения выделяемых средств, нужно определить требуемый уровень защиты опасных объектов* транспорта всех видов в зависимости от степени их опасности по потенциальному ущербу с учетом вероятности (степени риска) совершения на них террористической атаки и ее негативных политических последствий.

Эта задача решается на основе идентификации и категорирования объектов транспорта, что обеспечивает выделение объектов, требующих постоянного контроля за их безопасностью, и дифференциации требований к системам их антитеррористической и противокриминальной защиты. Другими словами, учитывая очень большое число и,

* Здесь и далее под объектами транспорта понимаются объекты транспортной инфраструктуры и транспортные средства.

с одной стороны, разнообразие такого рода объектов, а с другой — их функциональное единство (например, множество одинаковых по функциям, но различных по «мощности» аэропортов, вокзалов, морских и речных портов, транспортных средств и т. д.), необходимо провести их ранжирование (категорирование) по характерным признакам. Эта процедура позволяет выделить типовые объекты транспорта в каждой категории и далее формировать типовые требования и решения по обеспечению безопасности.

Требованиями к защите объектов транспорта должны обеспечиваться минимально необходимые и достаточные уровни безопасности в соответствии с установленными категориями их потенциальной опасности, с учетом критериев оценки возможного ущерба интересам личности, общества и государства.

Концепция предусматривает, что оценка эффективности имеющейся или создаваемой на объекте транспорта системы обеспечения транспортной безопасности выполняется на основе оценки рисков нарушения безопасности, возникающих при невыполнении или не полном выполнении комплекса директивных требований по защите всех уязвимостей объекта транспорта (оценка уязвимости). Соответственно, управление безопасностью объекта транспорта ориентировано на снижение рисков нарушения безопасности объекта, т. е. на выполнение всего комплекса директивных требований, соответствующего имеющейся категории объекта.

Система обеспечения транспортной безопасности на основе категорирования, в соответствиями статьей 2 Федерального Закона «О транспортной безопасности», предполагает последовательное решение следующих задач:

— предварительный анализ текущего состояния уязвимости объекта;

— идентификацию и категорирование опасных объектов;

— индексацию всех типов опасных объектов и транспортных средств в соответствии с категорией и внутривидовой классификацией объекта;

— построение моделей угроз для каждого типа объектов транспорта;

— оценку допустимой стоимости системы обеспечения безопасности каждого типа объектов транспорта с учетом его индекса и размера потенциального ущерба;

— построение профилей защиты для каждого типа объектов транспорта в соответствии с их индексом, моделями угроз и допустимой стоимостью системы защиты;

— формирование требований для каждого типа объектов транспорта в соответствии с его индексом и профилем защиты;

— оценку уязвимости объектов транспорта в зависимости от степени выполнения на них требований по обеспечению безопасности;

— периодический контроль (мониторинг) выполнения требований по обеспечению безопасности на опасных объектах транспортной инфраструктуры;

— составление плана повышения защищенности объекта (данный план составляет субъект транспортной инфраструктуры по результатам мониторинга и на основании официального заключения по оценке уязвимости объекта), план в свою очередь утверждается в установленном порядке.

Перечисленные задачи решаются путем последовательной реализации специальных вычислительных процедур, состав которых приведен на рис. 1.

Рис. 1. Процедуры решения задач обеспечения безопасности.

3. Практика применения АПК «РискДетектор» для решения задач обеспечения транспортной безопасности. В АПК разработаны и реализованы алгоритмы решения (рис. 2–4) всех входящих в данную процедуру задач.

Алгоритмы реализуются АПК «РискДетектор», который представляет собой комбинацию двух самостоятельных взаимосвязных составляющих — «РискДетектор-Анализ» и «РискДетектор-Контроль». Отметим, что комплекс «РискДетектор-Анализ» обеспечивает реализацию процедур 1А, 2А и 3А, образующих верхнюю ветвь проблемного поля (см. рис. 1). В большинстве случаев это задачи, решаемые на уровне руководства того вида транспорта, к которому принадлежит данный объект, а результаты полученных решений являются типовыми для всех аналогичных объектов.

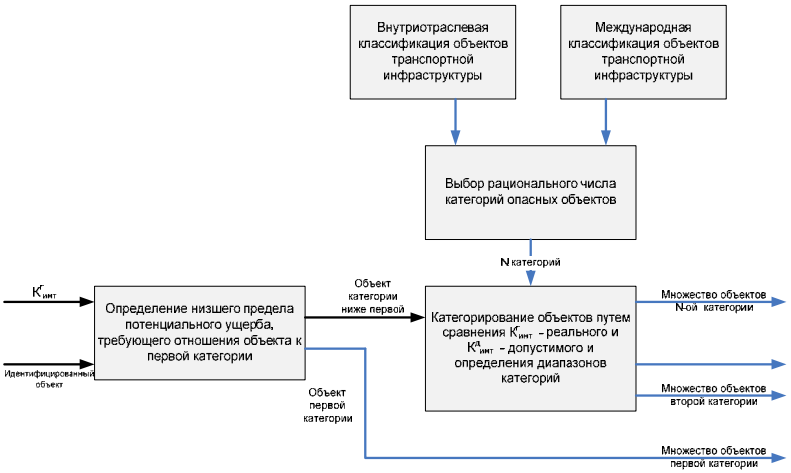

Рис. 2. Структурный алгоритм выполнения процедуры «Категорирование».

Эта «ветвь» комплекса обеспечивает решение следующих задач:

— построение модели угроз и модели нарушителя;

— идентификацию критически важных объектов (КВО) данного вида транспорта;

— идентификацию критических точек и рисков реализации террористических актов по КВО данного типа;

— оценку уязвимостей КВО данного типа;

— категорирование объектов транспорта;

— определение стоимостных параметров мероприятий по обеспечению безопасности;

— анализ системы требований по обеспечению безопасности объектов транспорта;

— ведение реестра категорированных объектов транспорта.

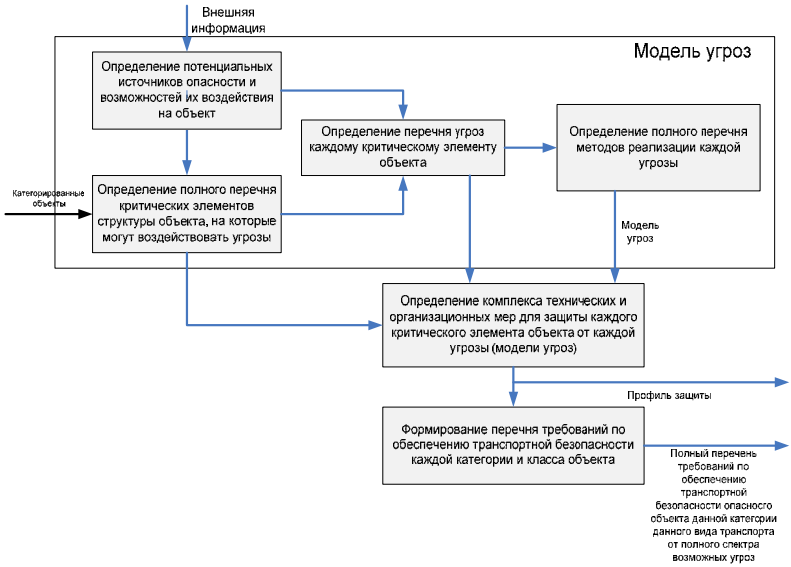

Рис. 3. Структурный алгоритм выполнения процедуры «Построение профилей защиты объекта».

Вторая часть комплекса — «РискДетектор-Контроль» — решает задачи процедур 1К—4К («нижняя ветвь» процедур на рис. 1). Предполагается, что эта часть комплекса будет использоваться непосредственно на объекте для решения следующих задач:

— определение состава нормативных требований по обеспечению безопасности объекта *i*-й категории и построение профилей защиты для критических точек объекта;

— контроль выполнения требований по обеспечению безопасности;

— выявление уязвимых мест и оценка уязвимости объекта;

— ведение досье по проблемам безопасности;

— формирование и ведение «Паспорта безопасности объекта»;

— разработка вариантов комплексов мер и средств защиты и выбор лучшего по критерию эффективность — стоимость.

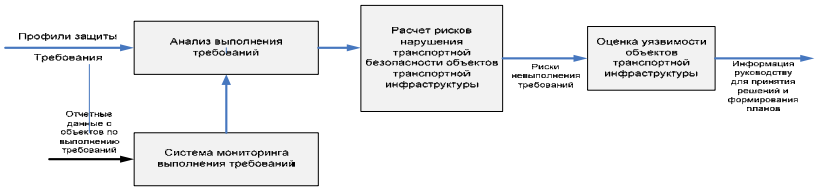

Рис. 4. Операции, реализующие процедуру «Оценка уязвимости».

На рис. 5 дана схема АПК «РискДетектор» с выделением верхней и нижней «ветвей».

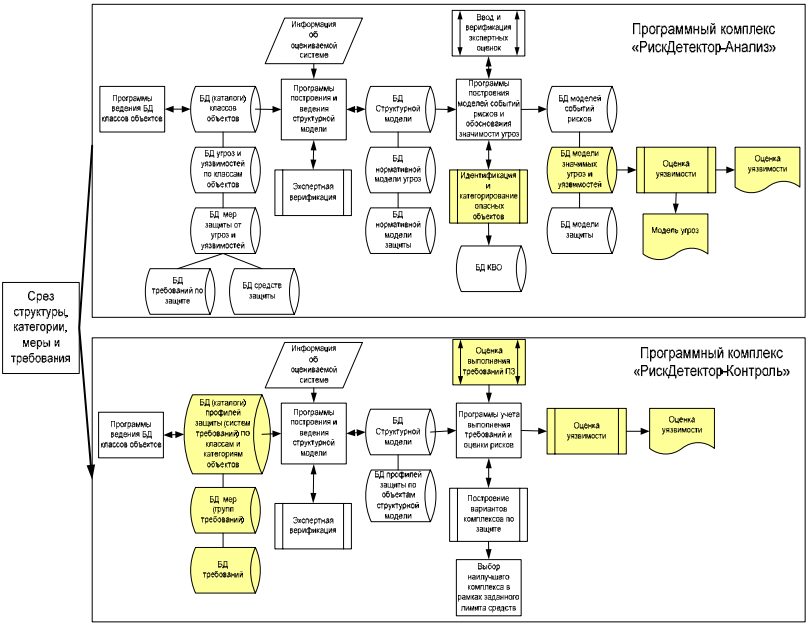

Рис. 5. Схема АПК «РискДетектор».

На рис. 6 приведены диалоговое окно «Построение структурной модели объекта — выделение и оценка уязвимостей (расчеты моделей рисков объекта)» и соответствующая документальная форма.

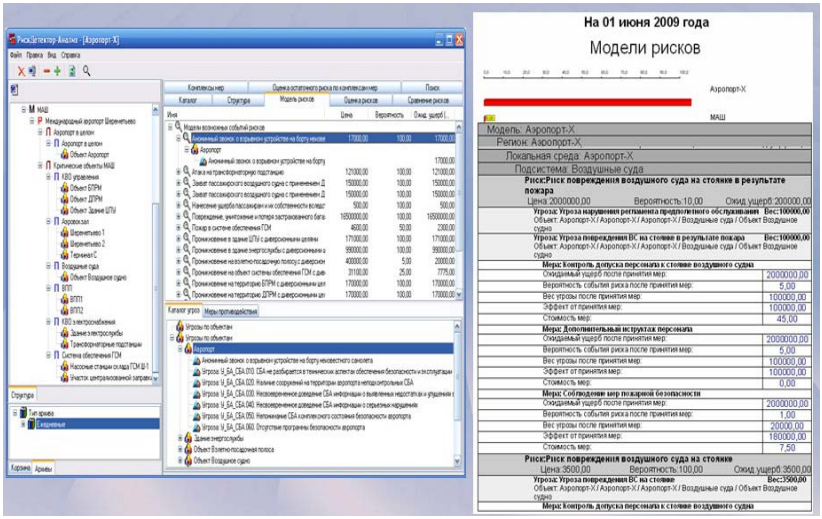

Рис. 6. Задача «Построение структурной модели объекта — выделение и оценка уязвимостей».

Приведенные на рис. 7 диалоговое окно и соответствующий результирующий документ показывают результаты решения задачи оценки уязвимостей объекта и лимитов затрат на их устранение.

АПК «РискДетектор» в автоматизированном режиме на основе данных, характеризующих рассматриваемый объект (критические точки, модель угроз, классность объекта), рассчитывает категорию объекта. На примере приведенных на рис. 8 диалоговом окне и результирующем документе показаны полученные результаты — определена категория объекта.

В соответствии с разработанной в концепции системе определения диапазонов ущерба категорий опасности рассматриваемый объект следует отнести к первой категории опасности.

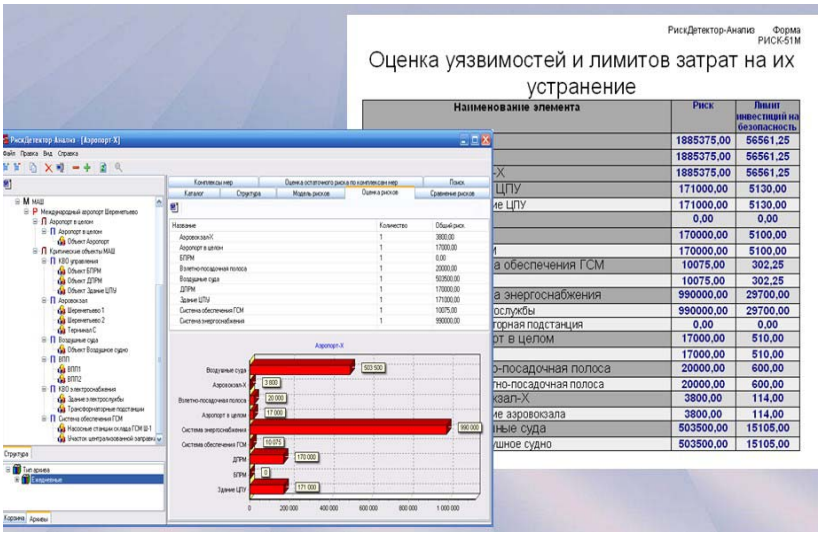

Рис. 7. Задача «Оценка уязвимостей».

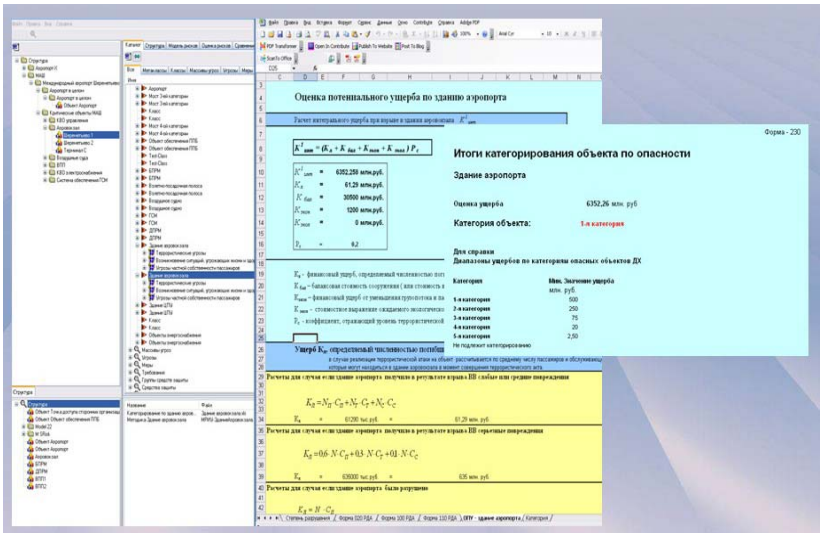

Рис. 8. Задача «Определение категории объекта».

Следующая важная задача, решаемая комплексом — это формирование, на основе анализа, определенных ранее критических точек объекта и всей совокупности имеющихся нормативных требований по обеспечению безопасности объекта транспорта профилей защиты объекта, т. е. наборов требований, выполнение которых обеспечивает защиту критических точек от всех возможных методов реализации угроз. На основании профилей защиты осуществляется, с учетом ограничений по стоимости защиты, выбор организационных мер и технических средств. Диалоговое окно и документальная форма выполнения этой задачи показаны на рис. 9.

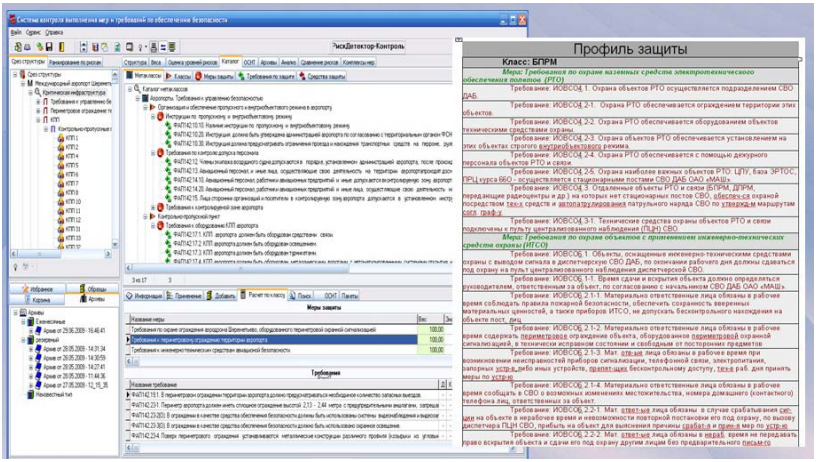

Рис. 9. Задача «Построение профилей защиты».

Важная задача — довести до всех исполнителей полученные профили защиты объекта. При этом преследуется ряд целей. Во-первых, каждый исполнитель получает в концентрированном виде набор тех требований и средств, которые он должен выполнять на своем рабочем месте. Во-вторых, руководство службой безопасности имеет возможность конкретно настаивать на выполнении направленного исполнителю всего комплекса требований. Одновременно руководство службой безопасности может запросить от исполнителя отчет по выполнению требований, что далее используется для расчетов рисков реализации угроз на объекте, т. е. для оценки реальной уязвимости объекта.

На рис. 10 приведены формы решения задачи «Доведение до исполнителей требований и регистрация их ответов по выполнению требований».

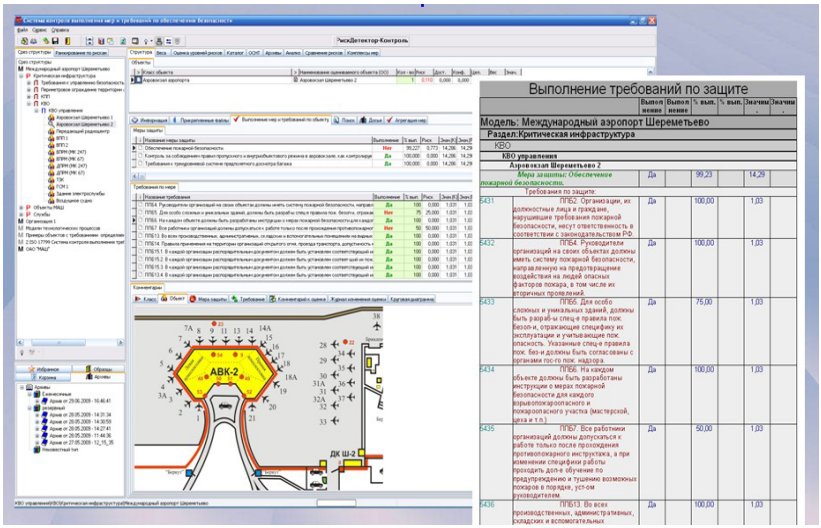

Рис. 10. Информирование исполнителей о требованиях по обеспечению безопасности.

И, наконец, на рис. 11, показаны результаты расчетов рисков реализации всей совокупности угроз по всем критическим точкам объекта и по объекту в целом. Основой для расчетов рисков служат отчеты исполнителей по выполнению ими профилей защиты.

Из приведенного примера видно, что по некоторым критическим точкам риск реализации террористических угроз чрезмерно велик и требуется проведение мероприятий по повышению реального уровня выполнения профиля защиты.

4. Заключение. Использование комплекса «РискДетектор» позволяет:

— обеспечить систематический мониторинг состояния безопасности объекта;

— минимизировать средства на обеспечение защиты объекта;

— обеспечить контроль работы соответствующих подразделений и выполнения необходимых работ.

Отличительной чертой комплекса является способность быстрой адаптации для обеспечения любых видов безопасности — информационной, технико-технологической, кадровой, экологической и др. Такая способность подтверждается пятилетней эксплуатацией его в ЦБ РФ для обеспечения информационной безопасности систем безналичных расчетов. В настоящее время комплекс проходит апробацию в реальных условиях ОАО «Международный аэропорт Шереметьево».

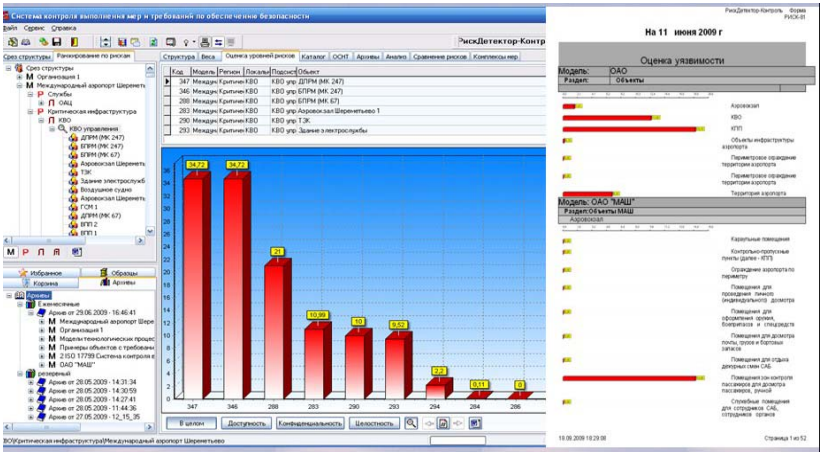

Рис. 11. Расчет рисков реализации совокупности угроз.

Литература

1. *Кононов А.А., Стиславский А.Б., Цыгичко В.Н.* Управление рисками нарушения транспортной безопасности. М.: АС-Траст, 2008. 210 с.
2. *Черешкин Д.С., Цыгичко В.Н., Козлов Ю.П., Кононов А.А.* Концепция категорирования потенциально опасных объектов национальной транспортной инфраструктуры // Тр. ИСА РАН. 2007. Т. 31. С. 5–20.
3. *Стиславский А.Б., Козлов Ю.П.* Концепция реализации основных положений Закона о транспортной безопасности // Материалы VII Междунар. науч.-практической конф. «Терроризм и безопасность на транспорте» М., 2009. С. 49–64.

Кононов Александр Анатольевич — канд. техн. наук; старший научный сотрудник лаборатории 0-1 «Информатизация и информационная безопасность» Учреждения Российской академии наук Институт системного анализа РАН (ИСА РАН). Область научных интересов: развитие и использование информационных, компьютерных и коммуникационных технологий в различных сферах общественной жизни, создание автоматизированных систем безопасности. Число научных публикаций — 130. kaa@isa.ru; ИСА РАН, пр. 60-летия Октября, д.9, г. Москва, 117312, РФ; р.т. +7(499)135-5043, факс +7(499)135-5043.

Kononov Alexander Anatolevich — Ph.D. in Technical; senior researcher of Laboratory 0-1 «Information and information safety», Institute of Systems Analysis of the Russian Academy of Sciences (ISA RAS). Research interests: development and use of information, computer and communication technologies in various spheres of a public life, creation of the automated systems of safety. The number of publications — 130. kaa@isa.ru; ISA RAS, 9, 60 let Octyabria, Moscow, 117312, Russia; office phone +7(499)135-5043, fax +7(499)135-5043.

Стиславский Александр Борисович — канд. экон. наук; докторант Учреждения Российской академии наук Институт системного анализа РАН (ИСА РАН). Область научных интересов: развитие и использование информационных, компьютерных и коммуникационных технологий в различных сферах общественной жизни, создание автоматизированных систем безопасности. Число научных публикаций — 56. astislav@telecom-group.ru; ИСА РАН, пр. 60-летия Октября, д.9, г. Москва, 117312, РФ; р.т. +7(495)960-6688, факс +7(499)135-5043.

Stislavskiy Alexander Borisovich — Ph.D. in Economics; doctorant of Institute of Systems Analysis of the Russian Academy of Sciences (ISA RAS). Research interests: development and use of information, computer and communication technologies in various spheres of a public life, creation of the automated systems of safety. The number of publications — 56. astislav@telecom-group.ru; ISA RAS, 9, 60 let Octyabria, Moscow, 117312, Russia; mobile phone +7(495)960-6688, fax +7(499)135-5043.

Цыгичко Виталий Николаевич — д-р техн. наук; профессор, главный научный сотрудник лаборатории 0-1 «Информатизация и информационная безопасность» докторант Учреждения Российской академии наук Институт системного анализа РАН (ИСА РАН). Область научных интересов: развитие и использование информационных, компьютерных и коммуникационных технологий в различных сферах общественной жизни, создание автоматизированных систем безопасности. Число научных публикаций — 215. vtsygichko@inbox.ru; ИСА РАН, пр. 60-летия Октября, д.9, г. Москва, 117312, РФ; р.т. +7(499)135-5043, факс +7(499)135-5043.

Tsygichko Vitaliy Nikolaevich — D.Sc. in Technical; professor; main researcher of Laboratory 0-1 «Information and information safety», Institute of Systems Analysis of the Russian Academy of Sciences (ISA RAS). Research interests: development and use of information, computer and communication technologies in various spheres of a public life, creation of the automated systems of safety. The number of publications — 215. vtsygichko@inbox.ru; ISA RAS, 9, 60 let Octyabria, Moscow, 117312, Russia; office phone +7(499)135-5043, fax +7(499)135-5043.

Черешкин Дмитрий Семенович — д-р техн. наук; профессор, заведующий лаборатории 0-1 «Информатизация и информационная безопасность» докторант Учреждения Российской академии наук Институт системного анализа РАН (ИСА РАН). Область научных интересов: развитие и использование информационных, компьютерных и коммуникационных технологий в различных сферах общественной жизни, создание автоматизированных систем безопасности. Число научных публикаций — 272. cheresh@isa.ru; ИСА РАН, просп. 60-летия Октября, д.9, г. Москва, 117312, РФ; р.т. +7(499)135-5043, факс +7(499)135-5043.

Chereshkin Dmitri Semenovich — D.Sc. in Technical; professor; manager of Laboratory 0-1 «Information and information safety», Institute of Systems Analysis of the Russian Academy of Sciences (ISA RAS). Research interests: development and use of information, computer and communication technologies in various spheres of a public life, creation of the automated systems of safety. The number of publications — 272. cheresh@isa.ru; ISA RAS, 9, 60 let Octyabria, Moscow, 117312, Russia; office phone +7(499)135-5043, fax +7(499)135-5043.

Поддержка исследований. В публикации представлены результаты исследований, поддержанные договором между ИСА РАН и ФГУП ГосНИИ ГА № 12-2008-П от 29.12.08.

Рекомендовано СПИИРАН, директор Р.М. Юсупов , чл.-корр. РАН.
Статья поступила в редакцию 01.02.2010.

РЕФЕРАТ

Кононов А.А., Стиславский А.Б., Цыгичко В.Н., Черешкин Д.С. **Автоматизированный комплекс средств обеспечения антитеррористической безопасности на примере транспортного комплекса.**

Обеспечение антитеррористической безопасности объектов хозяйственного комплекса страны в настоящее время представляет собой важную задачу. Ее полноценное решение подразумевает создание методологии, методического инструментария и программных средств для выработки требований по обеспечению безопасности. В работе рассматриваются вопросы обеспечения транспортной безопасности.

Концепция обеспечения безопасности объектов транспортной инфраструктуры и транспортных средств строится на основе их категорирования по величине потенциального ущерба, который может быть нанесен при реализации возможных угроз. Процедура категорирования позволяет выделить типовые объекты транспорта в каждой категории и далее формировать типовые требования и решения по обеспечению безопасности.

Система обеспечения транспортной безопасности на основе категорирования предполагает последовательное решение следующих задач:

— предварительный анализ текущего состояния уязвимости объекта;

— идентификация и категорирование опасных объектов;

— индексацию всех типов опасных объектов и транспортных средств в соответствии с категорией и внутривидовой классификацией объекта;

— построение моделей угроз для каждого типа объектов транспорта;

— оценку допустимой стоимости системы обеспечения безопасности каждого типа объектов транспорта с учетом его индекса и величины потенциального ущерба;

— построение профилей защиты для каждого типа объектов транспорта в соответствии с их индексом, моделями угроз и допустимой стоимостью системы защиты;

— формирование требований для каждого типа объектов транспорта в соответствии с его индексом и профилем защиты;

— оценку уязвимости объектов транспорта в зависимости от степени выполнения на них требований по обеспечению безопасности;

— периодический контроль (мониторинг) выполнения требований по обеспечению безопасности на опасных объектах транспортной инфраструктуры;

— составление плана повышения защищенности объекта (данный план составляет субъект транспортной инфраструктуры по результатам мониторинга и на основании официального заключения по оценке уязвимости объекта), план в свою очередь утверждается в установленном порядке.

Представленный АПК «РискДетектор» осуществляет решение всех указанных задач, что иллюстрируется приведенными результатами его работы на примере гипотетического объекта — крупного международного аэропорта.

SUMMARY

Kononov A.A., Stislavskiy A.B., Tsygichko V.N., Chereshkin D.S. **The automated complex of means of maintenance of antiterrorist safety on an example of a transport complex.**

Maintenance of antiterrorist safety of objects of an economic complex of the country represents now the important problem. Its high-grade decision means creation of methodology, methodical toolkit and software for development of requirements on safety. In work questions of maintenance of transport safety are considered.

The concept of safety of objects of a transport infrastructure and vehicles is under construction on the basis of them categorization on size of a potential damage which can be put at realization of possible threats. Procedure of categorization allows to allocate typical objects of transport in each category and further to form typical requirements and decisions on safety.

The system of maintenance of transport safety on a basis categorization assumes the consecutive decision of following problems:

— The preliminary analysis of a current condition of vulnerability of object;

— Identification and categorization dangerous objects;

— Indexation of all types of dangerous objects and vehicles according to a category and interspecific classification of object;

— Construction of models of threats for each type of objects of transport;

— An estimation of admissible cost of system of safety of each type of objects of transport taking into its index and size of a potential damage;

— Construction of profiles of protection for each type of objects of transport according to their index, models of threats and admissible cost of system of protection;

— Formation of requirements for each type of objects of transport according to its index and a protection profile;

— An estimation of vulnerability of objects of transport depending on performance degree on them of requirements on safety;

— The periodic control (monitoring) of performance of requirements on safety on dangerous objects of a transport infrastructure;

— By results of monitoring and on the basis of the official conclusion according to vulnerability of object, the subject of a transport infrastructure makes the plan of increase of security of object which affirms when due hereunder.

Presented hardware-program complex "RiskDetector" carries out the decision of all specified problems that is illustrated by the resulted results of its work on an example of hypothetical object — the large international airport.