Построение профилей защиты категорированных объектов транспортной инфраструктуры

А.Б. Стиславский

Аннотация. Одной из важнейших задач, решаемых в рамках автоматизированной системы обеспечения транспортной безопасности (АС ОБ), является построение профилей защиты категорированного объекта, т.е. определение типового состава комплекса средств и мероприятий, обеспечивающих приемлемый уровень безопасности всего множества объектов данной категории и данного вида транспорта. В процессе решения поставленной задачи необходимо решить две сопряженные – построение модели угроз данной категории объектов и провести оценку допустимой стоимости системы обеспечения безопасности объекта. В статье рассматривается решение совокупности поставленных задач в АС ОБ.

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

Введение

Автоматизированная система обеспечения безопасности (АС ОБ) критически важных объектов любого вида инфраструктуры – транспортной, энергетической, информационной и т.д. – обычно функционирует в условиях ряда специфических для любой инфраструктуры особенностей. Далее в качестве примера рассматривается транспортная инфраструктура, для которой такими особенностями являются:

- очень большое число разнообразных объектов, требующих защиты, например, только в дорожной службе имеется более 3000 различного типа мостовых сооружений, в гражданской авиации более 400 аэропортов и т.д.;

- множество однотипных, но различных по своим характеристикам объектов, выполняющих аналогичные функции, но «разного масштаба», например, по пропускной способности - ж/д вокзалы в Москве, городах типа Елец, станционные сооружения платформ и т.д., различные типы транспортных средств;

- высокая сложность объектов, безопасность которых необходимо обеспечивать, например, крупный аэропорт, ж/д пересадочный узел, самолет и т.д.

Для эффективности процесса обеспечения безопасности множества критически важных объектов (КВО) транспортной инфраструктуры и транспортных средств возникает необходимость в их классификации, выделении типовых объектов[1] каждого класса и создании единой методологии управления процессом обеспечения безопасности объектов единого типа и одной категории для данного вида транспорта. Например, должна быть единой методология обеспечения безопасности для всех мостовых сооружений *i- ого* класса (категории). Этот процесс получил название процесса категорирования всех КВО данного вида инфраструктуры, в частности, транспортной.

[1] Для краткости изложения здесь и далее под объектами транспортной инфраструктуры понимаются как сами объекты, так и соответствующие транспортные средства.

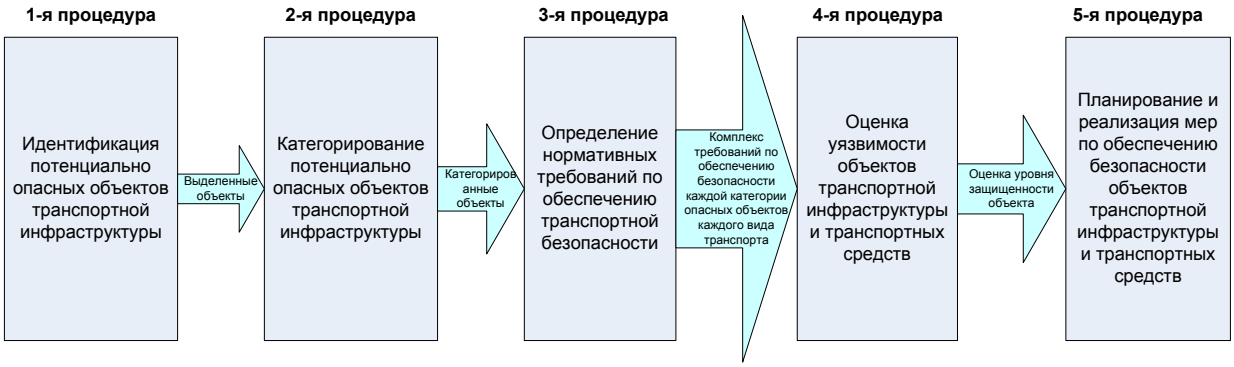

Рис. 1. Состав и взаимосвязь процедур реализации основных положений Закона о транспортной безопасности

Принимаем, что такой процесс успешно проведен и в дальнейшем рассмотрении имеем дело с категорированным, т.е. отнесенным к соответствующему типу, объектом. Для нас категорирование означает только то, что АС ОБ должна выдавать решения по обеспечению безопасности с учетом типичности данного вида объектов.

1. Процесс обеспечения транспортной безопасности как решение комплекса взаимосвязанных процедур

Для обеспечения безопасности объектов транспортной инфраструктуры в Законе о транспортной безопасности [1] и в [2] указан состав взаимосвязанных процедур, которые должны быть реализованы в составе АС ОБ. На Рис.1 показаны эти процедуры.

В соответствии с [3] предполагается, что управление процессом обеспечения безопасности объекта транспортной инфраструктуры будет осуществляться АС ОБ путем управления рисками ее нарушения. Соответственно (процедура 4 на Рис. 1), риски определяются на основе информации о полном или частичном выполнении всего множества требований (Законы, Указы, Правительственные постановления, международные соглашения и т.д.), определяющих транспортную безопасность на данном объекте.

На основе вышеизложенного можно сделать вывод, что важнейшей процедурой, можно считать процедуру 3 - «Определение нормативных требований по обеспечению транспортной безопасности». Очевидно, что каждая процедура представляет собой совокупность обязательных к исполнению операций, каждая из которых включает в себя необходимые источники информации и алгоритмы, реализующие преобразование и расчет данных.

На Рис.2 приведена схема взаимосвязи операций, реализующих процедуру 3.

2. Построение модели угроз критически важному объекту транспортной инфраструктуры

Наиболее значимыми, несомненно, являются операции «Построение модели угроз» и «Определение комплекса технических и организационных мер для защиты каждого критического элемента объекта от каждой угрозы (построение профиля защиты)».

Все операции реализуются на основании разработанного итерационного алгоритма и позволяют предоставить пользователю конкретные предложения по обеспечению транспортной безопасности объекта в целом и всех образующих его элементов. При этом определенная ранее категория объекта является значимым фактором с точки зрения выполнения перечисленных выше операций, поскольку категория определяет ранги необходимых требований по обеспечению транспортной безопасности и типизацию полученных решений.

В качестве исходных операций процедуры проводится выявление и составление полного перечня критически важных элементов структуры объекта, определение их «критических» точек, т.е. тех точек, в которых может быть реализована угроза.

Построение модели угроз критическому элементу типового объекта данного вида

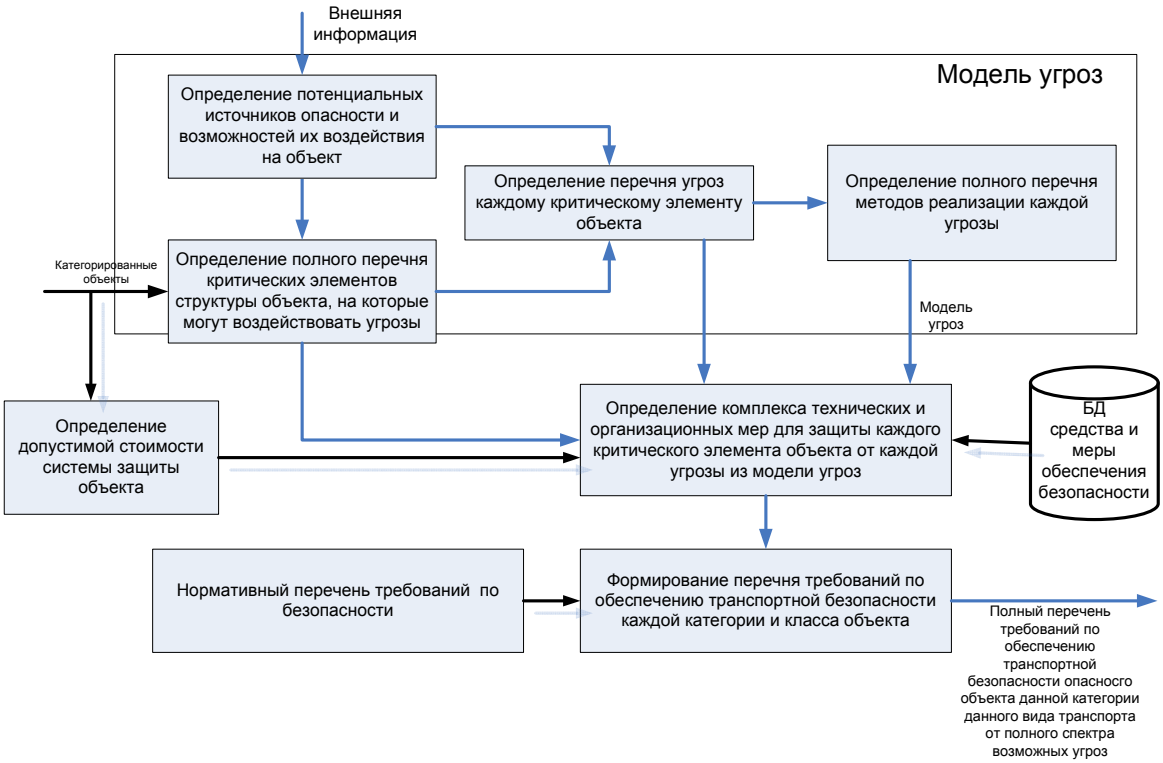

Рис. 2. Состав операций, реализующих процедуру
«Определение нормативных требований по обеспечению транспортной безопасности»

транспорта транспортной инфраструктуры является важным шагом в обеспечении транспортной безопасности. Под моделью угроз понимается весь спектр возможных воздействий со стороны потенциальных источников опасностей на критические элементы объекта.

Модель угроз является общей для всех одинаковых элементов типовых объектов всех категорий. Например, одна модель угроз для всех аэропортов и элементов их инфраструктуры для всех категорий опасности. Модели угроз закрепляются в качестве нормативов для всех объектов транспортной инфраструктуры. Определение полного спектра угроз и возможных способов их реализации для каждого защищаемого объекта является исходным моментом для построения системы обеспечения его безопасности.

Обеспечение безопасности любого объекта транспортной инфраструктуры предполагает определенный комплекс мер противодействия угрозам этому объекту. Чаще всего в реальной жизни приходится сталкиваться не с прямой, т.е. открыто высказанной возможностью нанесения ущерба, а с потенциальной (возможной) опасностью. Эта потенциальная опасность и определяется термином «угроза». Угроза определяется существованием или появлением источника потенциальной опасности.

Главным и трудно предсказуемым источником опасности является противоправная террористическая и криминальная деятельность отдельных людей, террористических или преступных групп и сообществ, а в отдельных случаях и государств, порождающая «террористические и криминальные угрозы». Большинство систем обеспечения безопасности создается для противодействия именно террористическим и криминальным угрозам. К ним относятся и системы обеспечения транспортной безопасности.

Каждый источник потенциальной опасности объективно порождает спектр угроз для каждого конкретного объекта, который однозначно определяется характером возможных действий источника потенциальной опасности и характерными особенностями, структурой и составом критических элементов объекта, который может подвергнуться опасности.

Таким образом, угрозы конкретному объекту существуют объективно, если имеется потенциальный источник опасности, но в тоже

время каждая угроза может быть или не быть реализована, т.е. реализация угрозы носит случайный характер. Оценка вероятности реализации каждой конкретной угрозы является сложной и часто неразрешимой объективными методами задачей, поскольку реализация угрозы определяется чаще всего непредсказуемыми факторами.

Разрешение неопределенности, связанной с реализацией угроз, достигается построением системы безопасности на основе принципа равной защищенности. Этот принцип лежит в основе разработки требований по обеспечению безопасности критических объектов транспортной инфраструктуры.

Рассмотренные понятия, связанные с определением угроз, позволяют выстроить принципиальную схему их взаимодействия в виде модели угроз отдельному объекту, группе или классу однородных объектов. Например, все аэропорты могут быть признаны однородными объектами относительно спектра угроз критическим элементам их инфраструктуры, поскольку аэропорты всех классов по внутриотраслевой классификации имеют одинаковую инфраструктуру и отличаются друг от друга только масштабом деятельности и характеристиками критических элементов.

Совокупность всех известных и возможных на данный момент времени угроз и способов их реализации критическим элементам объекта составляет **модель угроз** этому объекту.

Для рассматриваемого случая (объект транспортной инфраструктуры – аэропорт) построение модели угроз может быть проиллюстрировано с помощью таблицы, где в первом столбце указаны операции, а во втором – результаты их выполнения.

3. Формирование профилей защиты категорированному критически важному объекту транспортной инфраструктуры

После построения модели угроз, когда определены возможные опасности для всей совокупности критических точек объекта, начинается формирование для них профилей защиты. Под формированием профилей защиты понимается определение типового состава требова-

Выполняемая операция	Результат
Определяются потенциальные источники опасности, их возможности по воздействию на объект и возможные способы реализации этого воздействия	Потенциальные источники опасности: террористические организации в России и мире и относящиеся к ним террористические группы; бандформирования и криминальные организованные группы; отдельные личности с нарушением психики. Возможности воздействия на объект и способы реализации: проникновение на территорию объекта и нанесение ущерба (разрушение, прекращение нормальной деятельности и т.д.); захват транспортного средства.
Определяются критические элементы объекта, по которым возможно воздействие потенциального источника опасности	Критические элементы объекта: определяются на основе анализа структуры объекта; обычно к ним относят внешний периметр, входы и КПП, жизненно важные системы и установки (например, систему управления движением и т.д.); транспортные средства (самолет, автобус, судно и др.).
Для каждого критического элемента объекта определяется перечень возможных угроз со стороны потенциального источника опасности	Перечень возможных угроз для *i-го* критического элемента: анализ мирового и отечественного опыта показывает, что для критических элементов объекта транспортной инфраструктуры практически имеется только одна угроза – несанкционированное проникновение на объект с проносом оружия, ВВ или ОВ.
Для каждой угрозы определяются возможные способы ее реализации	Возможные способы реализации угрозы: рассматриваются все возможные способы несанкционированного проникновения группы или одиночки на территорию объекта – вооруженный прорыв, подкуп персонала, через служебные и технологические входы, путем преодоления внешнего периметра и т.д.

ний по обеспечению безопасности объекта и реализующего эти требования комплекса средств и мероприятий, обеспечивающих приемлемый уровень безопасности всего множества объектов данной категории и данного вида транспорта.

Построение профилей защиты требует обязательного создания ряда баз данных, в частности:

- упорядоченное описание всех критических элементов объекта и всех имеющихся критических точек (т.е. точек возможных реализаций угроз);
- максимально полный перечень требований к обеспечению безопасности, имеющихся во всех отечественных и зарубежных директивных документах (Законы, Указы Президента, постановления Правительства, ведомственные руководящие материалы, приказы министра и т.д., требования и рекомендации международных организаций);
- регламентные требования по инженерно-технической оснащенности объектов защиты, в которые входят: средства инженерно-технической защиты, системы охранной сигнализации, системы контроля и управления доступом (СКУД), системы охранного телевидения (СОТ) и видеонаблюдения, средства и системы оповещения, системы оперативной связи, системы досмотра, системы мониторинга транспортных средств (СМТС);
- каталоги технических средств, содержащие их функциональные характеристики и стоимость.

На основании разработанного алгоритма для каждой критической точки и потенциально возможных для нее способов реализации угроз проводится выборка всех требований по обеспечению безопасности. Полученная выборка формирует первую часть профиля защиты. При этом учитывается, что рассматриваемые критически опасные элементы объекта являются типовыми для всех объектов данного типа и данного типа транспорта. Например, все аэропорты имеют КО элементы – здание аэровокзала, взлетно-посадочные полосы, топливно-заправочный узел и т.д.

Вторая часть профиля защиты формируется на основе выборки технических средств и/или организационных мероприятий, обеспечивающих реальное выполнение определенных ранее требований.

Полный профиль защиты объединяет обе указанные выше части.

Далее проводится оценка стоимости реализации сформированного профиля защиты. Сегодня принято, что стоимость всех применяемых средств защиты не должна превышать 3% от величины возможного ущерба при реализации угрозы[2]. Если стоимость всей защиты не превышает этого значения, то данный профиль определяется как типовой для всех подобных объектов соответствующего вида транспорта. Если стоимость выше, то в соответствии с уровнем допустимых затрат корректируются профили защиты и перечень требований по обеспечению безопасности.

Для скорректированных требований и профиля защиты определяется величина риска невыполнения первоначально заданных требований, на основании чего лица, ответственные за обеспечение безопасности, должны директивно утвердить, принимается или отвергается данный профиль защиты.

Если полученная величина риска не удовлетворяет лицо, принимающее решение, то требования по безопасности дополняются, профиль защиты усиливается в соответствии с принятой допустимой степенью риска, а его стоимость увеличивается.

Если средств на реализацию профиля защиты для всех категорий опасных объектов недостаточно, то они распределяются по старшинству категорий, сначала для 1-й категории, затем для 2-й категории и т.д.

4. Оценка эффективности сформулированного профиля защиты

Одним из существенных требований к разработке профиля защиты объекта, является требование чтобы вводимые меры защиты и деятельность системы безопасности не должны

[2] Такое значение приемлемой стоимости типового профиля защиты объекта соответствует мировой практике – максимальная страховка морских грузов, принятая лондонской страховой компанией Ллойд, не превышает 3% от полной стоимости груза.

препятствовать нормальному функционированию охраняемого объекта. Это требование многократно подчеркивается в международных правилах обеспечения безопасности функционирования различных видов транспорта.

Суть проблемы состоит в следующем. Каждое средство защиты, применяемое для охраны объекта, может в той или иной степени отрицательно влиять на качество функционирования объекта. Оценка этого негативного эффекта обычно проводится через изменение какого-либо критичного параметра функционирования объекта. Для объектов транспортной инфраструктуры в качестве такого параметра обычно выступают временные циклы функционирования критических элементов объекта.

При формировании профиля защиты критических элементов типовых объектов транспортной инфраструктуры в качестве показателя достаточности защиты выступает критерий «величина риска нарушения безопасности критических элементов объектов – стоимость системы защиты».

Принципиальный вид зависимости величины риска нарушения безопасности P критического элемента объекта транспортной инфраструктуры от стоимости его защиты S представлен на Рис. 3.

Зависимость на Рис.3. можно прокомментировать следующим образом. При небольших затратах на защиту уровень риска остается высоким. По достижении некоторого порогового значения (1) затрат их дальнейшее увеличение дает высокий эффект, который заканчивается по достижении точки насыщения (2), когда дальнейшие затраты мало повышают эффективность защиты. При выборе рационального профиля защиты необходимо исходить из того факта, что никакие, даже самые лучшие меры, никогда не могут обеспечить полную защиту объекта или его критического элемента, т.е. всегда остается некоторая вероятность нарушения их безопасности. Задача состоит в том, чтобы для каждого критического элемента и объекта в целом найти точку перегиба 2 (Рис.3), т.е. определить минимальные затраты на их защиту, соответствующие допустимому уровню риска. Эта задача решается путем введения понятия страхования рисков нарушения безопасности объектов транспортной инфраструктуры.

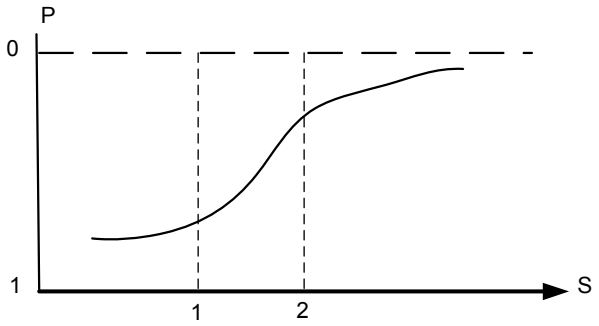

Рис.3. Зависимость величины риска P от затрат S на защиту объекта или его критического элемента

Принято считать, что система защиты стоимостью в 3% от потенциального ущерба объекту транспортной инфраструктуры при реализации террористической атаки должна, в принципе, обеспечить допустимый уровень риска нарушения его безопасности. Однако определение допустимого уровня риска для опасных объектов транспортной инфраструктуры остается серьезной научной и практической проблемой. Сложность ее решения определяется тем, что защита опасных объектов осуществляется человеко-машинной системой, где человеческий фактор играет решающую роль. Оценка эффективности технических систем охраны не является сложной задачей, поскольку определяется их техническими и надежностными характеристиками, в то время как учет человеческого фактора в системах обеспечения безопасности до сих пор остается нерешенной проблемой.

В международной практике, связанной с обеспечением транспортной безопасности, принято, что полное выполнение требований по безопасности функционирования какого-либо вида транспорта, зафиксированных в международных стандартах и рекомендуемых практике, обеспечивает достаточный для настоящего времени уровень безопасности. При такой постановке вопрос об определении количественного значения уровня допустимого риска снимается, а оценивается только риск неполного выполнения требований безопасности.

Эти требования периодически уточняются и дополняются в связи с появлением новых угроз безопасности и должны быть основой для разработки национальных программ обеспечения безопасности для всех видов транспорта. Для гармо-

низации законодательства стран-участников конвенций по безопасности функционирования видов транспорта международные организации, занимающиеся вопросами транспортной безопасности, рекомендуют включать международные стандарты и рекомендуемую практику в национальные программы обеспечения безопасности на транспорте в той же формулировке, что и в официальных документах этих организаций.

Кроме того, рекомендуется использовать международные стандарты и рекомендуемую практику обеспечения транспортной безопасности при осуществлении как международных, так и внутренних перевозок и отражать это положение в национальных программах.

Заключение

Проведенная структуризация достаточно сложной процедуры формирования профиля защиты категорированного объекта транспортной инфраструктуры является типовой методикой для всех категорированных критически опасных объектов данного типа и данного вида транспорта. Методика позволяет связать стоимость защиты с рисками реализации угроз объекту, оперативно корректировать как систему требований и средств защиты, так и распределение выделяемых для этого средств.

Предложенная в статье методика успешно реализована в виде аппаратно-программного комплекса, который в настоящее время проходит опытную эксплуатацию в Международном аэропорту Шереметьево.

Литература

1. Закон РФ «О транспортной безопасности».
2. А.А. Кононов, А.Б. Стиславский, В.Н. Цыгичко. Управление рисками нарушения транспортной безопасности. – М., АС-Траст, 2008.
3. Ю.П. Козлов. Создание системы транспортной безопасности. – М. Транспортная безопасность. 2005, №4.

Стиславский Александр Борисович. Кандидат экономических наук, докторант ИСА РАН.