УДК 614.8

В.И. Королёв[1,2], А.А. Новиков[2], А.П. Кузьмин[2], А.Н. Шориков[2]
([1]ИПИ РАН, [2]ЗАО "РНТ"; e-mail: vkorolev@ipiran.ru)

МЕТОДОЛОГИЯ ПОСТРОЕНИЯ МОДЕЛИ УГРОЗ БЕЗОПАСНОСТИ ТЕРРИТОРИАЛЬНО-РАСПРЕДЕЛЁННЫХ ОБЪЕКТОВ

Предлагается методология построения модели угроз безопасности для территориально распределённых объектов с многофункциональным целевым предназначением. Методология основана на представлении опасных событий и явлений в виде субъектно-объектных отношений и использовании соответствующей терминологии.

Ключевые слова: модель угроз безопасности, классификация, ситуационный анализ, уязвимости.

V.I. Korolev, A.A. Novikov, A.P. Kuzmin, A.N. Shorikov

METHODOLOGY FOR CONSTRUCTING THE MODEL OF SECURITY THREATS OF TERRITORIALLY DISTRIBUTED OBJECT

Proposes a methodology to the construction of a model of security threats for territorially distributed objects with multifunctional target purpose. A methodology is based on representation of dangerous events and the phenomena in the form of subject-object relations and use of the corresponding terminology.

Key words: model of security threats, classification, situation analysis, vulnerabilities.

Постановка задачи

Основа эффективного обеспечения безопасности любого объекта – создание достоверной модели угроз безопасности, содержащей ранжированные по выбранным показателям угрозы безопасности и их источники, а также определяющей возможные последствия от реализации этих угроз – вред, ущерб.

В общем случае модель угроз безопасности – информационная модель, содержащая совокупность сведений, характеризующих состояние безопасности объекта при возникновении определённых опасных событий, процессов, явлений, а также отношений объекта с внешним миром.

По способу представления эти модели относятся, как правило, к вербальным информационным моделям, формирующимся в описательном виде в результате логических умозаключений и сопоставительного анализа при структуризации и определении взаимосвязи основных компонентов [1] – в нашем случае источников угроз безопасности и объектов в части обеспечения их безопасности.

Эти факторы требуют специфического подхода к методологии построения модели угроз безопасности, к выработке логики проведения сопоставительного анализа и формирования последующих утверждений.

С точки зрения обеспечения безопасности, наиболее сложными являются территориально-распределённые объекты (системы) с многофункциональным целевым предназначением.

К сожалению, целостной и связной методологии построения моделей угроз для подобного рода сложных объектов в настоящее время не сложилось.

В данной статье сделана попытка упорядочить основные положения и приёмы для формирования единого методологического подхода к созданию модели угроз, с учётом существующих практических реализаций и имеющегося опыта разработки.

Особенности территориально-распределённого объекта безопасности

Территориально-распределённые объекты (ТРО) являются сложными и многофункциональными, представляются при решении проблемы безопасности как ***единое целое формирование***, объединяемое общей границей либо по признаку административного деления, либо по признаку принадлежности или владения, либо по признаку функционального назначения. В общем случае они включают в себя определённое количество требующих обеспечения безопасности составляющих объектов, как правило, неоднородных по своим характеристикам, назначению, условиям размещения, важности и, следовательно, имеющих свои особенности в части угроз безопасности, их блокирования и нейтрализации.

Для территориально-распределённого объекта целесообразно создавать базовую модель угроз безопасности и на её основе для конкретных объектов разрабатывать частные модели угроз безопасности.

Цель разработки и общая характеристика базовой модели угроз безопасности

Задачей базовой модели угроз безопасности территориально-распределённого объекта (***Модель***) является определение и систематизация основных угроз, реализация которых может нанести вред или создать ситуацию потенциальной возможности нанесения вреда физическим лицам, находящимся на территории ТРО, процессам их деятельности, а также нанести ущерб материально-техническим объектам, обеспечивающим эту деятельность. Обобщая поставленную задачу, цель разработки – представление в виде прогнозной модели совокупности опасных факторов (угрозы безопасности, их источники и характеристики), которые нарушают безопасность (как состояние) ТРО в целом и входящих в него объектов.

Определим элементы Модели: ***предметные элементы***, образующие конструкцию предметной области, поэтому требующие анализа и рассмотрения при построении Модели, ***базовые элементы*** – непосредственно угрозы безопасности и ***характеристические элементы***, фиксирующие свойства и показатели предметных и базовых элементов.

В качестве предметных элементов Модели могут быть выделены следующие:

• ***предметная область*** – безопасность как состояние и обеспечение безопасности как деятельность в отношении территориально-распределённого объекта;

• ***объекты безопасности*** – составные части и/или компоненты, входящие в состав территориально-распределённого объекта и требующие обеспечения безопасности, в том числе физические лица, их сообщества и объединения;

• ***субъекты угроз безопасности*:**

– носители угроз, когда ими являются физические лица, социальные группы и объединения, профессиональные и неформальные структуры, порождающие угрозы (***носители угроз***);

– источники угроз природного и техногенного характера, явления и процессы, порождающие данные типы угроз (***источники угроз***);

• ***субъекты обеспечения безопасности*** – субъекты (физические лица, профессиональные объединения и структуры), которые обеспечивают безопасность объектов, являются носителями активности противодействия угрозам на объектах безопасности.

Базовыми элементами Модели являются ***угрозы безопасности***, классифицированные по выбранным критериям и соотносимые через свои характеристики с субъектами угроз безопасности и объектами безопасности.

Характеристическими элементами Модели могут быть:

• основные признаки возникновения или проявления угроз безопасности (***признаки угроз***);

• виды возможных опасных воздействий на объекты безопасности, которые следует отнести к угрозам безопасности (***виды угроз***);

• способы и формы реализации этих опасных воздействий на объекты безопасности (***способы и формы реализации угроз***);

• уязвимости, которые предопределяют возможность реализации конкретных угроз безопасности (***уязвимости объекта безопасности***);

• возможные последствия от реализации угроз безопасности, которые отражают вред физическим лицам, ущерб материально-техническим объектам (***последствия реализации угроз***).

Совокупность рассматриваемых объектов безопасности, возможных угроз и способов их реализации в отношении данных объектов, определение источников возникновения угроз, способов и форм их проявления, возможных последствий позволяют заложить информационные и технологические основы для решения следующих основных задач по обеспечению безопасности:

– прогнозирование, выявление, анализ и оценка угроз безопасности;

– разработка и применение комплекса мер, связанных с выявлением и предупреждением угроз безопасности;

– определение, формирование организационной структуры противодействия угрозам безопасности ТРО и подготовка субъектов обеспечения безопасности к противодействию;

– координация деятельности субъектов обеспечения безопасности.

Модель должна позволить сформировать основу для разработки политики безопасности ТРО, концептуальных и организационно-технических решений в целях создания ***комплексной системы обеспечения безопасности (КСОБ)***.

Отражая базовый характер по отношению к совокупности входящих в ТРО объектов безопасности, Модель должна:

– содержать достаточно полную классифицированную совокупность угроз, свойственных всем объектам безопасности;

– позволить в интересах субъектов обеспечения безопасности сформировать единый понятийный аппарат при идентификации угроз, синтезировать ***нормативно-справочную информацию (НСИ)*** для управления безопасностью, обеспечения процессов подготовки и принятия решений по противодействию и ликвидации последствий реализации угроз;

– включать обобщенные характеристики, необходимые для оценки и представления развития ситуаций в случае реализации угроз.

Субъектно-объектные отношения в области безопасности

При разработке Модели предлагается использовать методологию исследования и представления предметной области в виде субъектно-объектных отношений.

Исследовательский подход, связанный с анализом субъектно-объектных отношений, является теоретической базой для достаточно многих научных направлений. Этот подход основан на изучении двух категорий – "субъекта" и "объекта", взаимодействие которых происходит в окружающей среде.

В общем случае, ***субъект*** – носитель предметно-практической деятельности или познания (физическое лицо, социальная группа или организационная структура), источник активности, направленной на объект.

В свою очередь под ***объектом*** понимается всё, что существует в реальной действительности. Это физические лица, материально-технические объекты, предметы, явления или процессы, на которые направлена предметно-практическая и познавательная деятельность субъекта.

Субъектно-объектные отношения – набор показателей, характеристик, действий, отражающих сущность активности субъекта по отношению к объекту.

Как правило, сущность активности отождествляется с видом деятельности, так как в общем случае субъектами является физические лица, их группы и структуры.

На сложных объектах реализуется достаточно большое разнообразие видов деятельности. Все физические лица и их объединения являются ***субъектами*** в субъектно-объектных отношениях в рамках определённых видов деятельности.

Субъектно-объектные отношения в области безопасности имеют свою специфику, а использование в данном случае понятий "субъект" и "объект" требует пояснения и уточнения.

Одной из первых работ, в которой субъектно-объектные отношения использовались как способ создания моделей безопасности, была модель безопасности операционных систем Харрисона, Руззо и Ульмана – 1976 год. Были введены понятия "субъекта" как активной сущности и "объекта" как пассивной сущности, при этом в качестве субъектно-объектных отношений рассматриваются ***отношения доступа и действий*** (права доступа) [4, 5]. При этом в качестве субъекта предлагается рассматривать ***не только физическое лицо***, но и активизированные в процессах ***технические средства***, откуда следует возможность в различных ситуациях и процессах присвоения техническому объекту роли либо субъекта, либо объекта.

В качестве субъектно-объектных отношений рассматриваются ***угрозы безопасности*** определённого ***субъекта угроз безопасности*** по отношению к определённому ***объекту безопасности.*** В такой постановке сделана попытка сформулировать подход к субъектно-объектным отношениям в работе [3]:

"К субъектам и объектам безопасности относятся любые системы (социальные, природные, технические и т.п.), которые обладают определённой совокупностью свойств. Различие между ними заключается в том, что объекту безопасности принадлежат привлекательные для субъекта безопасности свойства, а субъект безопасности обладает способностью к уничтожению (повреждению, изъятию, видоизменению, завладению и т.п.) этих свойств".

В то же время объект безопасности противостоит субъекту безопасности с помощью определённого вида деятельности и имеющегося в его распоряжении арсенала способов и средств. Таким образом, ***взаимодействие между субъектами и объектами в области безопасности носит двусторонний характер***.

Развивая этот подход, следует сделать ряд выводов и утверждений, которые обосновывают корректность введённых ранее элементов Модели.

1. В целях однозначной идентификации предметной области разрабатываемой Модели в качестве субъектов целесообразно использовать понятие "субъект угрозы безопасности" как активная сущность различной природы, влияющая на состояние безопасности объекта безопасности.

2. ***Субъектами угроз безопасности*** могут быть: ***физические лица*** и их сообщества – носители угроз; ***природные явления*** и ***техногенные образования*** (объекты, системы) – источники угроз.

3. В качестве вида субъектно-объектных отношений рассматриваются угрозы безопасности.

4. Объектами безопасности могут быть:

– физические лица, находящиеся на территории объекта, их объединения по сферам и видам деятельности;

– территориально-ландшафтные объекты, образующие природный ландшафт территориально-распределённого объекта;

– материально-технические объекты (здания и строительные объекты различного назначения, технические средства и инженерно-технические системы жизнеобеспечения материально-технических объектов, транспортные объекты и объекты транспортной инфраструктуры);

– системы (информационно-телекоммуникационные системы, технологические системы и другие обеспечивающие определённую деятельность системы, которые необходимо выделить как отдельные объекты безопасности);

– процессы (бизнес-процессы, процессы управления и обеспечения жизнедеятельности, технологические процессы инженерно-технических и информационно-телекоммуникационных систем);

– общественно-социальные мероприятия (политические, спортивные, культурные, развлекательные и другие), проводимые на объектах и территории ТРО.

5. Очевидна необходимость выделения из состава физических лиц (объектов безопасности) группы субъектов обеспечения безопасности (обеспечение безопасности – как вид деятельности), которые являются носителями активности противодействия угрозам безопасности. ***Субъекты обеспечения безопасности*** – отдельные физические лица и сформированные из них организационные структуры (правоохранительные органы, оперативные штабы, пункты и центры управления, ситуационные центры, различного назначения службы безопасности объектов ТРО и т.д.), выполняющие функции по защите объектов безопасности и/или ликвидации последствий реализации угроз безопасности. При этом понимается, что для выполнения своих функций они оснащены соответствующими инженерно-техническими средствами и информационно-технологическими системами.

6. Возможны ситуации, при которых объекты безопасности приобретают роль субъекта угроз безопасности. При этом возникает вторичная угроза безопасности.

Классификация угроз безопасности и образующие блоки Модели

Существует большое количество схем и моделей классификации угроз безопасности по видам, приведённых в официальных документах, в научно-технической литературе, в информационных ресурсах Интернета. Выдвигаются различные классификационные критерии, ориентированные на их использование при построении классификационных схем в определённых приложениях. Наиболее употребляемыми, следовательно, наиболее значимыми критериями являются: местонахождение источника опасности по отношению к объекту безопасности (внутренний, внешний); характер угрозы, определяемый источником и спецификой; сферы и области человеческой деятельности, на которые направлена угроза; уровень субъективных оценок вреда и ущерба угрозы при её реализации.

Ввиду разнородности критериев общность предлагаемых схем и моделей классификации заключается в блочном принципе их построения. Классификационное дерево от угрозы безопасности строится в отношении каждого критерия.

Оценка угроз в части вреда и ущерба как классификационный критерий в большей степени является меткой, показателем для угроз безопасности, выделяемых по другим классификационным критериям.

Критерий местонахождения опасности, безусловно, является чрезвычайно важным для своевременного обнаружения угроз и реагирования на них со стороны КСОБ. Поэтому деление угроз безопасности на внутренние и внешние угрозы имеет большую практическую значимость. Однако следует учитывать, что воздействие многих угроз в отношении территориально-распределённых объектов имеет трансграничный характер по отношению к входящим в него объектам безопасности. Поэтому классификация по этому критерию выделенных по другим критериям угроз в большей степени предметна при разработке частных объектовых моделей угроз безопасности.

В Модели, которая является базовой для территориально-распределённого объекта, представляется целесообразным в качестве основных определяющих критериев классификации угроз безопасности рассматривать следующие:

- характер угрозы (относительно первичных источников и специфики);
- сферы и области деятельности, на которые направлена угроза и/или она наиболее критична (сферы реализации угроз).

Соответственно выделяются два классификационных блока.

Первый блок соотносится с ***идентификацией угроз*** относительно первичных источников – угрозы антропогенные (Т1), техногенные (Т2), стихийные (Т3).

Второй блок позволяет структурировать угрозы от первичных источников по отношению к сферам их реализации (Т4), предоставляя возможность для формирования видов деструктивного влияния на конкретные объекты безопасности. По данному критерию можно выделить виды угроз безопасности для каждой самостоятельной сферы деятельности – производственной, общественно-социальной, политической, военной, экономической, информационной, экологической и т.д. Второй блок ориентирует направление аналитической работы в отношении реально появляющихся угроз безопасности от источника, позволяет осуществлять подготовку принятия решений субъектами обеспечения безопасности при угрозах конкретным объектам безопасности.

Виды объектов безопасности были предложены ранее и образуют отдельный классификационный блок. Аналитическую работу и подготовку принятия решений целесообразно также представить в виде блока противодействия угрозам, в рамках которого формируются основные атрибуты противодействия и ликвидации последствий реализации угроз безопасности. К ним отнесены характеристические элементы Модели: признаки возникновения угроз, возможные последствия реализации этих угроз и, в постановочном виде, – политика безопасности, силы и средства противодействия и ликвидации последствий реализации угроз. Перечисленные блоки являются образующими для базовой модели угроз безопасности.

Концептуальное представление Модели отражено на обобщённой классификационной схеме (рис. 1).

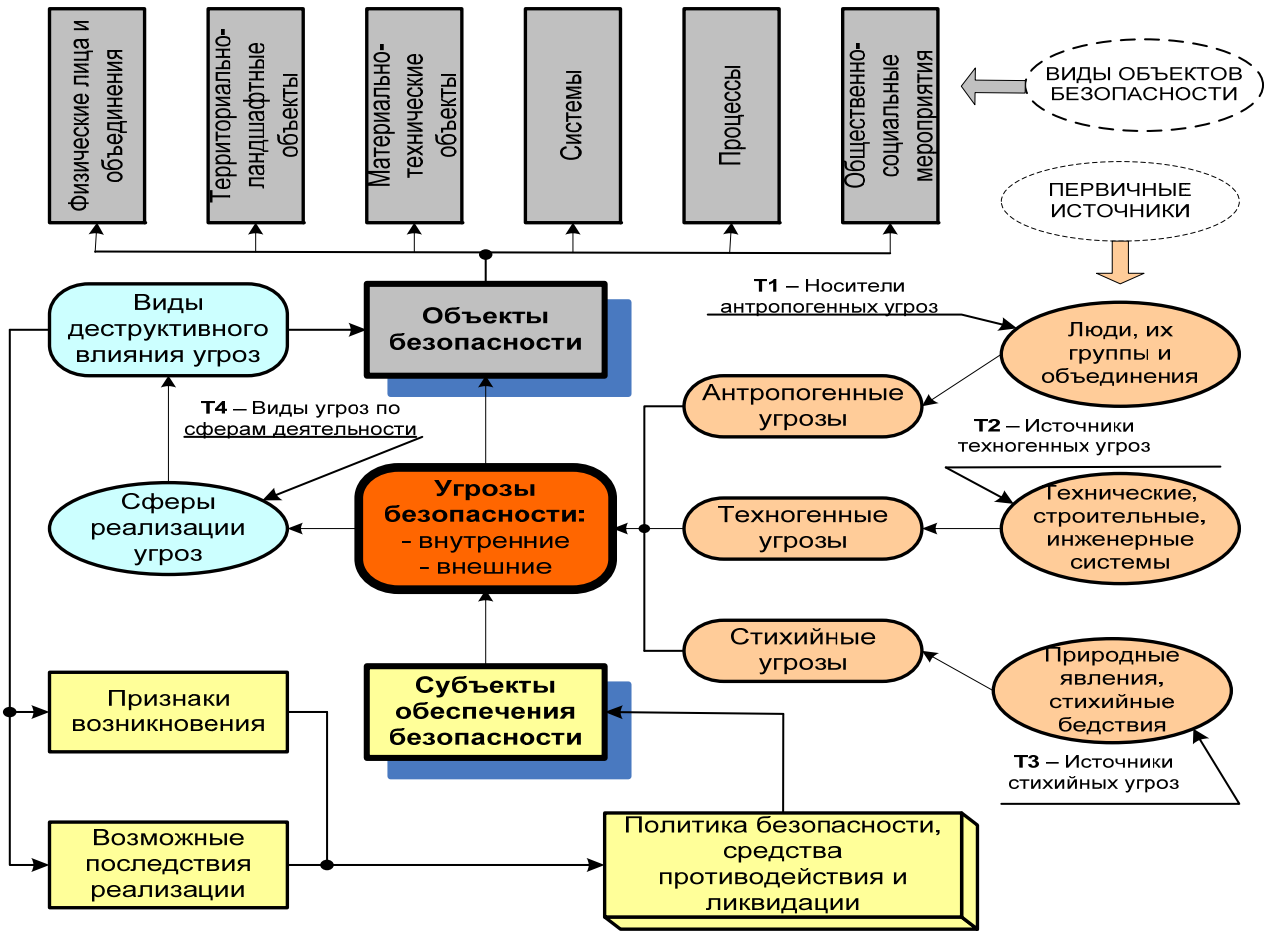

Рис. 1. Обобщённая классификационная схема базовой модели угроз безопасности

Ситуационный подход при анализе субъектно-объектных отношений безопасности

Построение модели угроз безопасности базируется на логических умозаключениях, сопоставительном анализе, структуризации и определении взаимосвязей субъектов угроз безопасности и объектов безопасности на основе субъектно-объектных отношений. В качестве субъектно-объектных отношений рассматриваются угрозы безопасности.

Ситуация – "сочетание условий и обстоятельств, создающих определённую обстановку, положение". Возьмём это понятие как базисное при формировании методологического подхода к построению модели угроз безопасности.

Главная задача, которую необходимо решить, это построение базовых элементов Модели: выявление угроз безопасности для входящих в ТРО объектов безопасности и формирование их классифицированного перечня.

Каждая угроза безопасности создаёт ситуацию (***условия и обстоятельства***), при которой возможно нанесение вреда или ущерба (***определённая обстановка, положение***) объекту безопасности. Угроза безопасности исходит от определённого субъекта угроз безопасности и направлена с определённой целью или случайно на объект безопасности. Эта очевидная предпосылка формирует ***сущность ситуационного подхода***: необходимо рассмотреть возмож-

ные ситуации нарушения состояния безопасности, выполнить анализ субъектно-объектных отношений безопасности в конкретной ситуации, принять решение о выделении угрозы безопасности определённого вида и включении её в классификационную схему по соответствующему критерию.

Основным инструментом реализации ситуационного подхода является ситуационный анализ. По своей направленности ситуационный анализ субъектно-объектных отношений безопасности аналогичен ситуационному анализу, который является частью ситуационного управления [7]. При этом следует отметить, что одним из базовых режимов функционирования КСОБ является режим ситуационного управления безопасностью за счёт мониторинга состояния и событий, а угрозы безопасности с их характеристиками в этом случае могут играть роль прогнозируемых эталонных ситуаций.

Этапы проведения ситуационного анализа в рамках ситуационного управления достаточно проработаны в методическом плане [8]. Однако в нашем случае, на этапе создания Модели ситуационный анализ направлен не на непосредственное осуществление управления безопасностью, а на принятие решений по совокупности угроз безопасности и формированию их характеристик.

Примеры схем формирования ситуаций и субъектно-объектных отношений показаны на рис. 2.

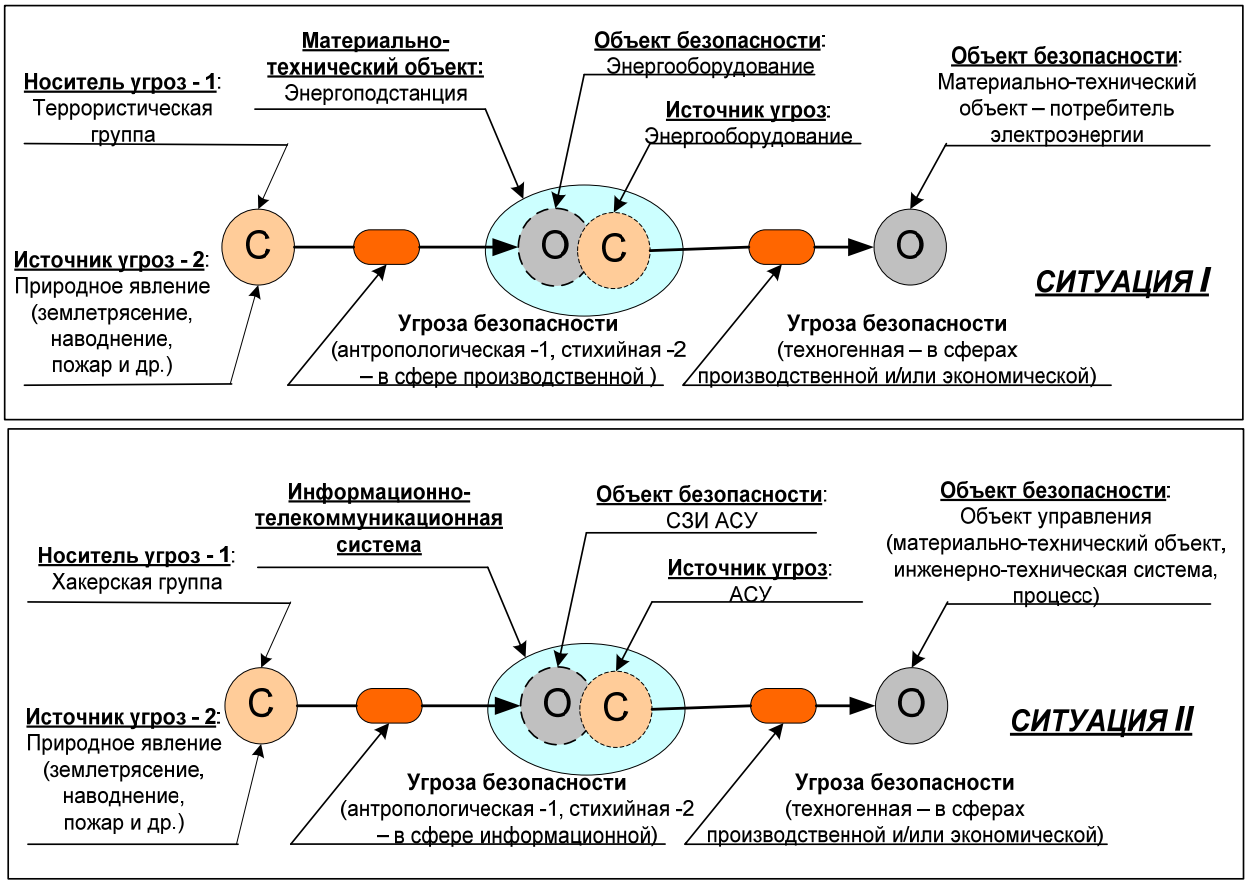

Рис. 2. Примеры формирования субъектно-объектных отношений безопасности

Ситуация образуется входящими компонентами.

Причиной возникновения определённой ситуации являются субъекты угроз безопасности (**С**), обладающие потенциальной возможностью деструктивной активности: носители угроз безопасности – в отношении физических лиц и их объединений, источники угроз безопасности – при угрозах природного и техногенного характера.

Деструктивная активность направлена на объекты безопасности (**О**).

Между субъектами угроз безопасности и объектами безопасности возникают субъектно-объектные отношения в виде угроз безопасности.

Субъектно-объектные отношения связаны со сценарием прогнозируемого развития ситуации, который формируется, исходя из характеристик и свойств субъекта угроз безопасности и объекта безопасности.

Анализ сценария развития ситуации должен обеспечить формирование характеристик, связанных с угрозами безопасности, оценку вероятности перехода угрозы безопасности в реальное событие и значимости последствий этого события (вред, ущерб) в отношении объекта безопасности. Конечным продуктом анализа сценария развития ситуации является именованная классифицированная угроза безопасности и принятие решения о включении её в Модель в качестве базового элемента.

На рис. 2 также показано, что ситуация может быть сложной, связанной с возникновением вторичной угрозы безопасности, когда роль объекта безопасности после реализации определённых угроз может переходить в роль субъекта угроз безопасности.

Из предлагаемой общей методологической схемы ситуационного анализа субъектно-объектных отношений безопасности следует ориентировочная структура Модели как конечного системного нормативного документа. Она должна включать в себя:

- объекты безопасности (анализ, описание), входящие в ТРО, с их характеристиками и особенностями в части безопасности, выделенными уязвимостями;
- модель нарушителя для всех прогнозируемых вариантов нарушения безопасности со стороны носителей угроз безопасности (физические лица и их объединения), как внутренних, так и внешних;
- источники угроз безопасности стихийного (природного) и техногенного характера (анализ, описание), как внутренние, так и по прогнозам влияющие на объекты безопасности из окружающей ТРО среды;
- базовые элементы Модели – угрозы безопасности, которые могут быть представлены в структурированном описательном виде или в формате структурированной функционально-факторной таблицы с определением ожидаемых ситуаций по строкам, с указанием по разделам столбцов общих характеристик и показателей.

При необходимости детализации угроз безопасности в Модели целесообразно формировать отдельные таблицы-классификаторы угроз безопасности, отражая сущности их наполнения и формальные идентификационные коды.

Общее представление о базовой части Модели – совокупности угроз безопасности – дано на рис. 3. На этой схеме также показано, что сформированная на основании Модели информационная база КСОБ позволит субъектам обеспечения безопасности оперативно реагировать на возникающие, реализуемые или реализованные угрозы и предпринимать соответствующие меры противодействия для ликвидации последствий реализации угроз на различных этапах их возможного проявления.

Резюме

Предлагаемый методологический подход к построению модели угроз безопасности для территориально распределённых объектов с многофункциональным целевым предназначением не претендует на однозначность и универсальность применения. Однако он выработан на основании анализа и с учётом достаточно большого объёма литературных источников теоретической и практической направленности. Как методика, он апробирован при разработке конкретных систем обеспечения безопасности. Учитывая исключительную актуальность задачи, представляется, что предлагаемый материал будет полезен для дальнейшего развития и становления методологии построения моделей угроз безопасности, разрабатываемых для сложных объектов.

Литература

1. ***Курносов Ю.В., Конотопов П.Ю.*** Вербальные или понятийные модели. http://do.gendocs.ru/docs/index_15903.html?page=13.

2. ***Национальный*** форум информационной безопасности "ИНФОФОРУМ". www.infoforum.ru.

3. ***Белов В.П., Голяков А.Д., Талалаев Д.В.*** Объектно-субъектный подход к безопасности. Управление риском, № 1, 2006. www.niitm.spb.ru>common/doc_view.php?file=36.

4. ***Корт С.С.*** Теоретические основы защиты информации // М.: "Гелиос АРВ", 2004.

5. ***Зегжда Д.П., Ивашко А.М.*** Основы безопасности информационных систем // М.: "Горячая линия – Телеком", 2000.

6. ***Прохожев А.А.*** Общая теория национальной безопасности. Виды угроз безопасности, 2005. http://bugabooks.com/book/136-obshhaya-teoriya-nacionalnoj-bezopasnosti/30-2-vidy-ugroz-bezopasnosti.html.

7. ***Joe Taik Kirn.*** Management contingency / Пер. Соколова М. Ситуационный подход к управлению // Государственное управление. Словарь-справочник (по материалам "International Encyclopedia of Public Politic and Administration"). ООО "Изд-во "Петрополис", 2000.

8. ***Учебный*** центр МГУТУ – www.ipkit.ru. Основные этапы ситуационного анализа http://bbest.ru/razryprresh/sitnacanaliz/osnetsitanal.

Статья опубликована 14 мая 2013 г.

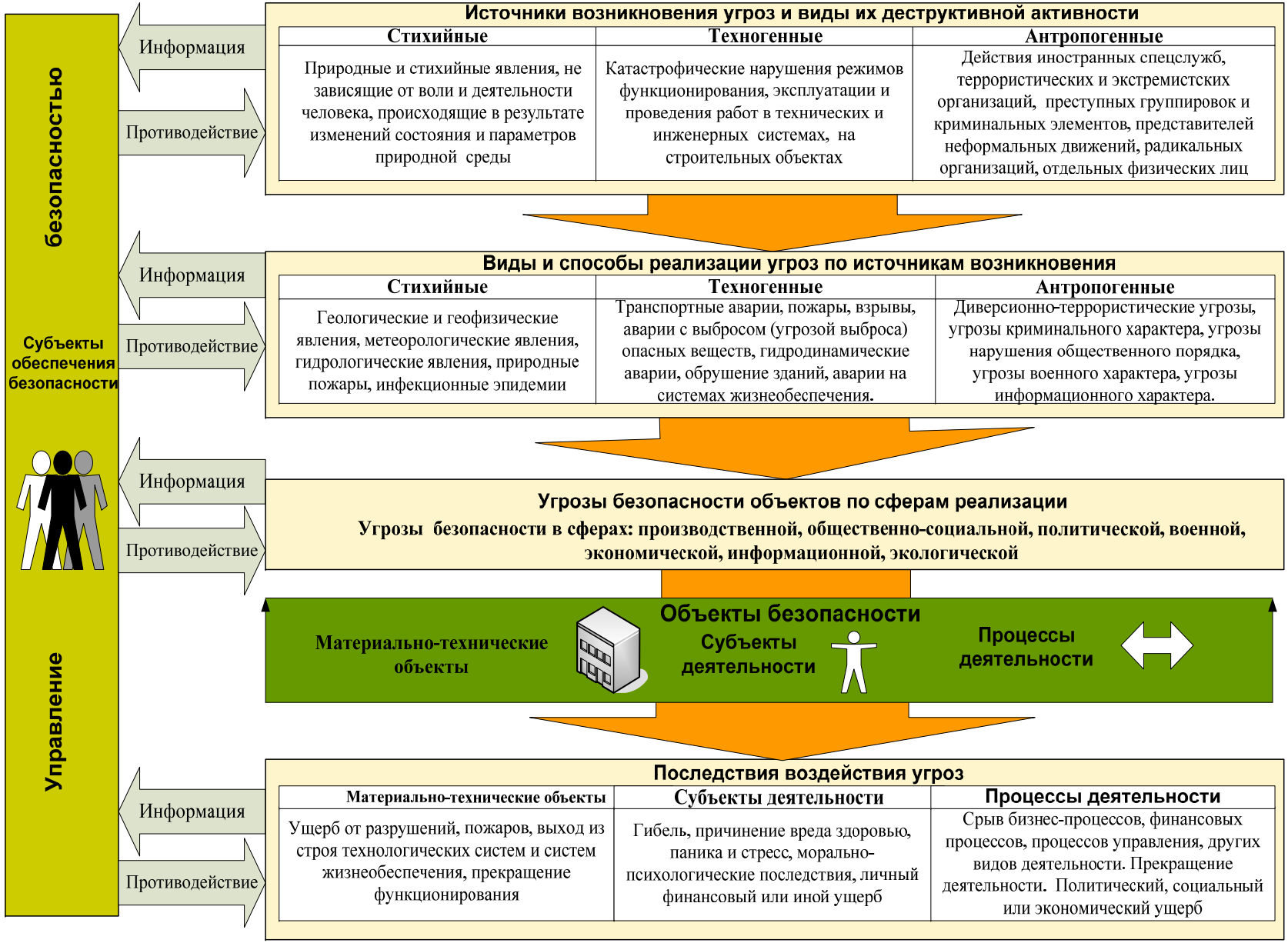

Рис. 3. Общее представление угроз безопасности