РАЗДЕЛ I
УПРАВЛЕНИЕ РИСКАМИ
КРИТИЧЕСКИХ СИСТЕМ И ИНФРАСТРУКТУР

Использование категорирования в обеспечении безопасности критических инфраструктур национального масштаба

В. А. Пучков, Д. С. Черешкин,
К. В. Черныш, А. А. Кононов

Основой жизнедеятельности любой системы, являются обслуживающие её инфраструктуры. Инфраструктуры, нарушение функционирования которых влечет за собой нарушение функционирования обслуживаемой ими системы с тяжелыми последствиями и значительным ущербом, являются критическими. Любая инфраструктура может быть структурирована и представлена как система взаимосвязанных объектов. В критических инфраструктурах (КИ) большинство объектов, могут быть определены как критически важные объекты (КВО). Это связано с тем, что объекты, составляющие инфраструктуры, как правило, в значительной степени взаимосвязаны и взаимозависимы, и нарушение нормального функционирования любого из них может вести к цепной реакции нарушения нормального функционирования других объектов, как самой КИ, так и обслуживаемых систем с тяжелыми последствиями и значительным ущербом. То есть критичность объектов КИ может обуславливаться как критичностью обслуживаемых структур, так и критичностью выполняемых этими объектами функций в общей функциональности КИ.

Для больших КИ, критических инфраструктур национального масштаба, таких как, транспортная, финансовая, энергетическая, информационно-телекоммуникационная, существует проблема большого ко-

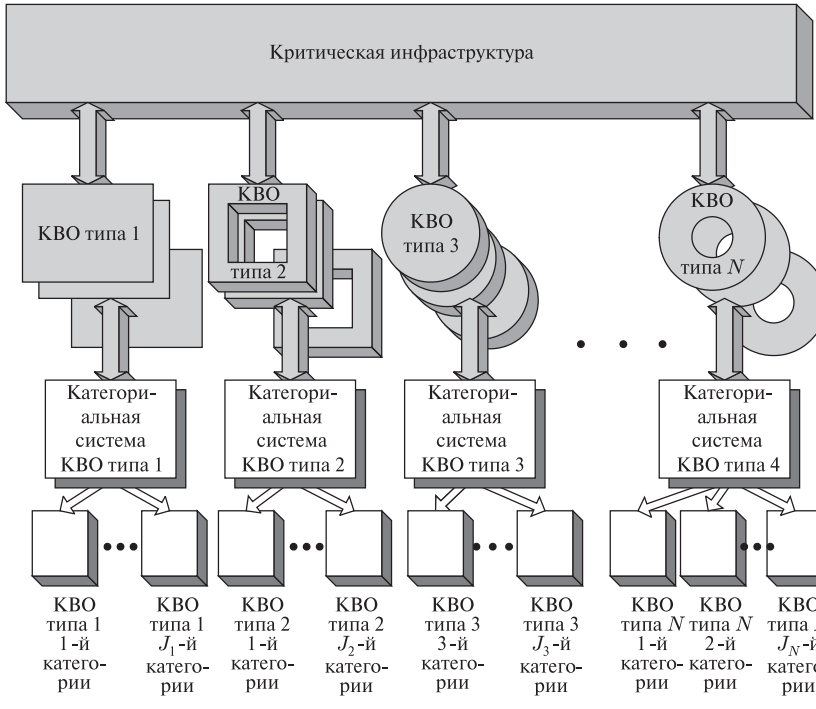

Рис. 1. Схема категорирования критически важных объекты (КВО) разных типов составляющие критическую инфраструктуру

личества КВО, образующих эти КИ. Обеспечение безопасности такого рода КИ нуждается в особых приемах управления их безопасностью. Так, возникающая проблема большого количества КВО, безопасность которых должна регламентироваться и контролироваться, может решаться через использование того обстоятельства, что большие инфраструктуры включают в себя большое количество одинаковых по классу и типу объектов (рис. 1). Это открывает возможность воспользоваться такими приемами, как типизация, классификация и последующее категорирование объектов одного класса и типа по опасности, которую может представлять нарушение их безопасного функционирования. Такой подход позволяет создать основу решения всех ключевых задач управления безопасностью критических инфраструктур, таких как, определение рациональных систем требований безопасности (профилей защиты — ПЗ) КВО КИ, контроль выполнения требований ПЗ на всех критических объектах, выявление уязвимостей, основных источников

рисков, определение наиболее эффективных комплексов мероприятий по повышению защищенности КВО.

Важность категорирования по опасности объясняется тем, что, несмотря на всю схожесть объектов одного типа, уровень их критичности может быть далеко не одинаков, и обусловлено это может быть множеством факторов, таких как:

- разный уровень загруженности, пропускной способности, производительности и т. п.;
- разный уровень критичности, зависимых от рассматриваемого, объектов, процессов и функций;
- разный уровень безопасности окружающей среды каждого из рассматриваемых однотипных объектов.

Для того, чтобы отразить эти различия среди объектов одного типа могут существовать классификационные шкалы. То есть объекты уже могут быть каким-то образом проклассифицированы. Если это так, то это может облегчить определение категориальных характеристик, признаков и построение категориальной шкалы, при категорировании объектов по опасности (рис. 2).

Категорирование КВО по опасности дает возможность:

- присвоить каждому из них обозначающий категорию идентификатор, который позволит лучше ориентироваться при принятии решений по управлению безопасностью этих КВО;
- унифицировать и оптимизировать системы требований по безопасности к сходным по типу и по уровню опасности объектов;
- разрабатывать общие для каждой категории планы повышения их безопасности.

Унификация требований облегчает задачу контроля безопасности КИ, но предполагаемые этими требованиями меры защиты должны быть адекватны реально существующим угрозам и пропорциональны их опасности. Меры защиты могут увеличивать издержки и снижать функциональность объектов, поэтому их избыток негативен для объекта и КИ. Недостаточно защищенный объект, в свою очередь, создает угрозу безопасности КИ и обслуживаемым системам. Именно категорирование по опасности позволяет находить рациональные решения без больших затрат.

Альтернативой категорированию могут быть процедуры построения моделей угроз, оценка уязвимостей, построение моделей защиты и систем требований по каждому объекту. Но стоимость и трудоемкость

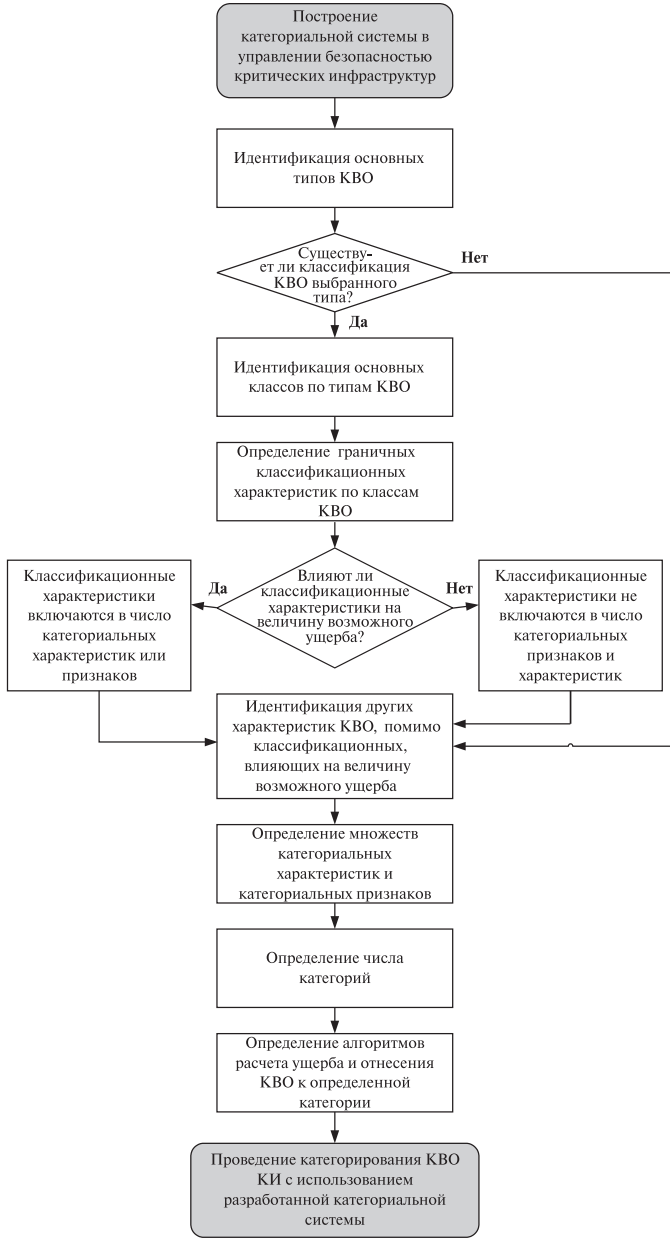

Рис. 2. Основные этапы построения категориальной системы в управлении безопасностью

решения этих задач, а также организационное, техническое и технологическое развитие КИ и обслуживаемых ими структур, обуславливающее необходимость периодического повторения этих процедур, делают их практически неосуществимыми для всех КВО. Категорирование дает возможность выполнять эти процедуры только для типовых объектов каждой категории (подкатегории), а потом применять выработанные таким образом решения по защите, включая системы требований безопасности, ко всем объектам выбранной категории.

Категорированию объектов должно предшествовать построение категориальной системы. ***Категориальная система*** представляет собой совокупность категориальных характеристик, шкал и признаков, необходимых для категорирования объектов с заданной конкретной целью. Так же в категориальную систему входят алгоритмы определения значений показателей категориальных характеристик из значений показателей категориальных признаков. Категориальную систему следует отличать от системы категорий, которая может включать в себя множество категориальных систем для категорирования объектов по разным направлениям и с разными целями.

В процессе построения категориальной системы, прежде всего, должны быть определены категориальные характеристики отвечающие целям категорирования. В принципе, они могут носить как количественный, так и качественный характер. В простейшем случае выделяется одна главная категориальная характеристика, именно на ее основе строится базовая категориальная шкала. При категорировании по опасности, в качестве такой категориальной характеристики может быть принята величина максимального возможного ущерба, который может быть нанесен при нарушении безопасного функционирования КВО. Категориальная шкала определяет те граничные значения числового показателя категориальной характеристики, которые позволят отделять объекты одной категории от объектов другой. Если категорирование используется для целей построения систем требований по безопасности, одной базовой категориальной шкалы может не хватить даже для одного класса объектов, поэтому в рамках каждой категории могут выстраиваться дополнительные шкалы подкатегорий. При категорировании по опасности потребность в использовании подкатегорий может возникнуть из-за особенностей внешней среды в которой могут существовать категорируемые объекты. Например, рядом с КВО одной КИ, могут располагаться КВО другой КИ, что значительно увеличивает опасность КВО обеих инфраструктур и не может не влиять на ужесточение систем требований безопасности по таким КВО в обеих инфраструк-

турах. В этом случае для построения подкатегориальной шкалы, в качестве дополнительной категориальной характеристики может использоваться показатель расстояния до КВО другой инфраструктуры.

Но в общем случае даже базовая категориальная шкала может строиться на многомерной системе категориальных характеристик. В таком случае должна разрабатываться система правил или алгоритмов, учитывающих значимости отдельных характеристик и сводящих показатели к единому значению на обобщающей категориальной шкале, что в отдельных случаях может значительно осложнить задачу категорирования. Поэтому при построении категориальной системы следует рассматривать возможность перевода неосновных показателей из числа категориальных характеристик в число категориальных признаков.

В отличие от категориальных характеристик, которые желательно сводить к минимуму, категориальные признаки могут быть разнообразны и многочисленны. В их роли могут выступать все те показатели, которые могут способствовать определению категории объекта, то есть расчету, или экспертной оценке величины категориальных характеристик КВО. Но и при определении множества категориальных признаков, тоже стоит избавляться от наличия функционально, или с высокими коэффициентами корреляции, связанных показателей, которые могут усложнить расчеты и при этом лишь дублировать результат.

Если КВО имеют сложную структуру, в них в свою очередь могут быть выделены критические составляющие. В этом случае категорирование по опасности КВО КИ следует начинать с категорирования критических типов их составляющих, выполняя для каждого из этих типов все те операции категорирования, что были описаны для КВО в целом. Выполнять категорирование по типам критических составляющих следует в целом для всей критической инфраструктуры. Это не только повышает качество анализа моделей угроз, уязвимостей и выработки систем требований безопасности, но и снижает трудоемкость процедур категорирования КВО КИ за счет использования общих для всех КВО решений по отдельным критическим составляющим. Значительно снижает трудоемкость работ по категорированию и выбор единой категориальной шкалы ущерба для всех типов КВО и их критических составляющих.

На рис. 2 показаны основные этапы построения категориальной системы.

То, что категорирование КВО в ближайшие годы может стать важнейшим инструментом обеспечения безопасности критических инфра-

структур, можно судить по официально принятым документам [1–3]. В Федеральном законе «О транспортной безопасности» прямо указывается, что категорирование объектов транспортной инфраструктуры и транспортных средств является одной из важнейших задач обеспечения транспортной безопасности.

В этой связи, с учетом масштабов задач, которые должны решаться, встает вопрос об автоматизации процедур категорирования. В Институте системного анализа РАН разработаны программные комплексы, которые обеспечивают такого рода автоматизацию [4–6]. Программный комплекс «РискМенеджер-Анализ» дает возможность построить модели угроз, модели событий рисков, выявить уязвимости и определить систему мер повышения защищенности типовых объектов по каждой категории. Программный комплекс «РискМенеджер-Контроль» дает возможность построить профили защиты по каждой категории объектов, разработать и разослать по объектам формы с категориальными признаками, потом через электронную почту собрать и обработать эти формы, заполненные исходными данными, и на основании полученной информации определить категорию каждого объекта. Далее «РискМенеджер-Контроль» позволяет разослать по каждому объекту формы с требованиями безопасности, провести аудит выполнения этих требований, определить уязвимости по каждому объекту и рассчитать риски, а также и разработать планы мероприятий по повышению защищенности объектов каждой категории.

Литература

1. Федеральный Закон «О транспортной безопасности» от 9 февраля 2007 г. № ФЗ–16.
2. «Основы государственной политики в области обеспечения безопасности населения Российской Федерации и защищенности критически важных и потенциально опасных объектов от угроз техногенного, природного характера и террористических актов».
3. Постановление Правительства Российской Федерации от 23 марта 2006 г. № 411–рс «Об утверждении перечня критически важных и опасных объектов Российской Федерации».
4. *Черешкин Д. С., Кононов А. А.* Проблемы развития инфраструктуры защиты информации в рамках национальной информационной инфраструктуры // Acta Academia. International Informatization Academy in Consultative Status (Cathegory I) with United Nations Branch of R. Молдова, Кишинев, 2000. С. 24–27.

5. *Черешкин Д. С., Кононов А. А., Сичкарук А. В.* Задачи управления киберрисками региональных критических инфраструктур // V Санкт-Петербургская Межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007)». Санкт-Петербург, 23–25 октября 2007 г.: Материалы конференции. СПб., 2007. С. 17–18.
6. *Кононов А. А., Сичкарук А. В., Черныш К. В.* Задачи управления киберрисками и кибербезопасностью критических инфраструктур национального масштаба // Проблемы управления рисками и безопасностью: Труды Института системного анализа Российской академии наук. Т. 31. М.: Издательство ЛКИ/URSS, 2007. С. 95–98.