МНОГОКРИТЕРИАЛЬНЫЙ ПОДХОД К КАТЕГОРИРОВАНИЮ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ С ПОЗИЦИИ ИХ ФИЗИЧЕСКОЙ ЗАЩИТЫ

О.В. Мелех, Е.П. Максимович, М.А. Талалуева, В.К. Фисенко

Категорирование объектов информатизации с позиции их физической защиты представляет собой достаточно сложную задачу, так как при этом необходимо учитывать целый ряд разнородных факторов, которые определяют задачу категорирования как многокритериальную.

В настоящее время детально проработано категорирование объектов по промышленной безопасности, категорирование помещений и зданий по пожарной безопасности, взрывоопасности, а также объектов информатизации с позиции их информационной безопасности [1–3]. Вопросы категорирования объектов информатизации с позиции физической защиты в известных и доступных нам источниках остаются до сих пор открытыми, хотя задача категорирования с позиции физической защиты является актуальной особенно применительно к критически важным объектам информатизации.

В настоящем докладе сделана попытка формирования подхода к категорированию объектов информатизации с позиции физической защиты. При этом мы старались использовать методологические подходы и методики применяемые к другим объектам и используемые при этом показатели и критерии принятия решений. Целью категорирования объектов информатизации является разбиение объектов информатизации на группы типовых с тем, чтобы в последующем разработать типовые количественные и качественные требования к системам физической защиты объектов информатизации и обоснованного выбора технических средств (систем) физической защиты.

При выборе показателей и критериев категорирования необходимо учитывать значимость, потенциальную опасность, специфику функционирования и уровень физической защиты объекта информатизации.

В качестве показателя значимости объекта мы рекомендуем следующие:

- объект информатизации местного значения (поселок, город);
- объект информатизации районного значения;
- объект информатизации областного значения;
- объект информатизации республиканского значения.

Потенциальная опасность нарушения информационной безопасности объекта информатизации определяется важностью информации, которая используется для управления технологическими процессами критически важного объекта. Фактически речь идет о создании чрезвычайной ситуации, обусловленной нарушением управлением технологическими процессами. При этом предполагается использовать в качестве показателей виды чрезвычайных ситуаций (местного значения, районного значения, областного значения, республиканского значения), а для каждого вида устанавливаются параметры:

- число пострадавших;
- нарушение условий жизнедеятельности;
- размер материального ущерба;

• размеры зоны чрезвычайной ситуации.

В качестве показателя специфики функционирования могут быть приняты

• автономный объект информатизации обработки информации;

• возможность передачи и использования информации другим объектам;

• распределенный способ применения объекта информатизации.

Целесообразно на наш взгляд использовать также показатели уровня физической защиты. Предлагается использовать следующие показатели уровня физической защиты:

• базовый уровень физической защиты, при котором защита объекта информатизации осуществляется средствами критически важного объекта;

• расширенный уровень физической защиты, при котором базовый уровень дополняется средствами непосредственной физической защиты от несанкционированного доступа к объекту информатизации;

• усиленный уровень физической защиты, при котором расширенный уровень дополняется специальными средствами, связанными со значимостью объекта информатизации, его потенциальной опасностью и условиями функционирования.

Сущность разбиения объектов информатизации на классы однотипных с точки зрения физической защиты заключается в разбиении множества объектов на непересекающиеся подмножества [4]. Решение этой задачи осуществляется в два этапа.

На первом этапе определяется множество показателей и их допустимых значений (признаковое пространство). Если множество значений каждого из показателей разбить по определенным правилам на непересекающиеся группы, то по каждому показателю могут быть выделены области его значений, в пределах которых требования к физической защите являются неизменными. Однако этого недостаточно. Для различных типовых объектов информатизации разбиение проводится не по одному, а по множеству показателей. Причем каждый показатель определяется множеством значений. Оценка значения показателя характеризует вклад в формирование требований по физической защите объекта информатизации. Следовательно, разбиение множества объектов информатизации на непересекающиеся группы производится не по одному, а по множеству показателей и их значений таким образом, чтобы в пределах одной группы требования к физической защите оставались неизменными.

На втором этапе определяется функция близости и критерий разбиения на множестве объектов информатизации с использованием множества показателей и их значений и формируется заданное число категорий типовых объектов информатизации.

Литература

1. *Анищенко В.В. и др.* // Комплексная защита информации. Минск: Ин-т техн. Кибернетики НАН Беларуси, 2000. С. 5–21.

2. *Гражданкин А.И.* Критически важные для национальной безопасности опасные производственные объекты. Показатели, критерии и порядок категорирования ОПО http://accident.fromru.com/Aticle/KVO_OPO.htm.

3. Поручения Правительства РФ № К-П4-11907 от 7 июля 2001 г. и № КП-П4-14832 от 22 августа 2001 г. "О создании методик категорирования объектов науки, промышленности и жизнеобеспечения по степени их потенциальной опасности и диверсионно-террористической уязвимости". М, 2001.

4. *Дюран Б., Оделл П.* Кластерный анализ. Пер. с англ. Е.З. Демиденко. Под ред. А.Я. Боярского. М., "Статистика", 1977.