

ПОСТРОЕНИЕ СТРУКТУРЫ ПОКАЗАТЕЛЕЙ ЭФФЕКТИВНОСТИ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНТЕРЕСАХ ОЦЕНКИ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

Практика построения и совершенствования систем вообще и систем оценки характеристик механизмов обеспечения защиты компьютерной информации в частности характеризуется попытками использования системного подхода к этой деятельности на основе новейших технологий.

Основной идеей системного подхода является комплексность, многосторонность рассмотрения проблем. Это позволяет формировать адекватные представления о различных аспектах исследуемого объекта. Акцент на необходимости построения единого целого в отличие от построения компонентов и подсистем — основная особенность системного подхода.

Вместе с тем попытки практического приложения системного подхода в сфере оценки характеристик механизмов обеспечения защиты компьютерной информации наталкиваются на ряд трудностей при определении требований к системе показателей и организации процессов моделирования и принятия решений при исследовании отдельных характеристик защищенности информационных процессов в компьютерных системах.

Решение данной проблемы в рамках системного подхода предполагает разработку методологии оценки защищенности информационных процессов в компьютерных системах, отражающую:

1. Целевую системность. Синтез системы показателей для оценки защищенности информационных процессов в компьютерных системах рассматривается как понятие, которое является составной частью более общего понятия — совершенствования механизмов защиты компьютерной информации;

2. Методологическую системность. Исследование и разработку проблем синтеза системы показателей для оценки защищенности информационных процессов в компьютерных системах необходимо вести с единых методологических позиций с учетом всех факторов;

3. Организационную системность. Организация и управление работ по синтезу системы такого рода показателей;

4. Правовую системность. Разработка нормативной базы, регулирующей способы получения характеристик защищенности информационных процессов в компьютерных системах.

Системный подход как общеметодологическая предпосылка дополняется существованием иных предпосылок решения проблемы на новом технологическом уровне: наличие постоянно развиваемой общей научно-методологической базы структурного синтеза, современных и перспективных средств измерения и оценки характеристик защищенности информационных процессов в компьютерных системах; начавшееся осознание необходимости новых подходов к рассматриваемой проблеме и появление некоторого опыта ее решения.

Основу методологии синтеза системы показателей для оценки защищенности информационных процессов в компьютерных системах составляет ряд теоретических положений, базовым из которых является положение о системе показателей эффективности противодействия угрозам информационной безопасности компьютерных систем.

Данное положение формулируется следующим образом.

Существует система показателей эффективности противодействия угрозам информационной безопасности, адекватно оценивающая защищенность информационных процессов в компьютерных системах.

С целью доказательства данного утверждения выделим такие характерные свойства и закономерности системы, как устойчивость, поведение, равновесие, целостность, бесконечность, интегративность, иерархичность, коммуникативность [1], и обоснуем их состоятельность применительно к множеству показателей эффективности противодействия угрозам информационной безопасности компьютерных систем как к инструменту оценки защищенности их информационных процессов.

Целостность проявляется в том, что свойства системы показателей не являются суммой свойств отдельных показателей и в то же время зависят от их свойств; новые взаимоотношения системы показателей как единого целого со свойствами механизмов защиты компьютерной информации отличны от взаимодействия с ней отдельных элементов; цель может быть определена путем изучения свойств системы как целого.

Системе показателей эффективности противодействия угрозам информационной безопасности компьютерных систем как целостной системе присущи неаддитивность и структура.

Бесконечность отражает невозможность полного познания и всестороннего представления системы показателей эффективности противодействия угрозам информационной безопасности компьютерных систем конечным множеством качественных и количественных показателей.

Интегративность определяет причины формирования целостности рассматриваемой системы, ее сохранения в условиях неоднородности и противоречивости показателей эффективности противодействия угрозам информационной безопасности.

Коммуникативность системы показателей эффективности противодействия угрозам информационной безопасности компьютерных систем характеризует ее единство с оцениваемыми характеристиками механизмов обеспечения защиты компьютерной информации, дает представление о том, что система представляет собой элемент системы более высокого уровня (например, системы показателей обеспечения защищенности сегментов информационной сферы), а сами элементы выступают как системы более низкого уровня.

Иерархичность — свойство системы показателей эффективности противодействия угрозам информационной безопасности компьютерных систем, вытекающее из свойств бесконечности и целостности, означает, что каждый элемент в декомпозиции системы может рассматриваться как целостная система, элементы которой, в свою очередь, могут быть представлены как системы, а сама система — как компонент более широкой системы.

Иерархичность имеет важнейшую особенность — проявление закономерности целостности системы показателей эффективности противодействия угрозам информационной безопасности компьютерных систем на каждом уровне иерархии, в результате чего на каждом уровне возникают новые свойства, которые не могут быть выведены как сумма свойств отдельных показателей. При этом важно, что не только объединение элементов в каждом узле приводит к появлению новых свойств, которых у них не было, и утрате некоторых свойств элементов, но и что каждый подчиненный член иерархии приобретает новые свойства, отсутствующие у него в изолированном состоянии.

Непрерывность рассматриваемой системы — непрерывное изменение ее состояния, выраженное в непрерывной структурной перестройке системы показателей вследствие постоянного совершенствования аппарата моделирования механизмов защиты информации.

Саморазвитие — способность и свойство системы показателей эффективности противодействия угрозам информационной безопасности компьютерных систем находиться в непрерывном процессе возникновения и разрешения противоречий.

Самоорганизация — способность системы показателей эффективности противодействия угрозам информационной безопасности компьютерных систем в условиях возникающих противоречий изменять свою структуру и корректировать цель.

Устойчивость — способность сохранения качественной определенности при изменении структуры системы показателей эффективности противодействия угрозам информационной безопасности компьютерных систем и функций ее элементов.

Устойчивость системы обеспечивается такими элементами самоорганизации, как дифференциация и лабильность.

Дифференциация — стремление системы показателей эффективности противодействия угрозам информационной безопасности компьютерных систем к структурному и функциональному разнообразию показателей, которое не только обеспечивает условия возникновения, но и определяет способность системы быстро приспосабливаться к меняющимся характеристикам механизмов защиты компьютерной информации.

Лабильность — широкие возможности показателей по оценке отдельных свойств механизмов защиты информации при сохранении устойчивости структуры системы показателей в целом.

С учетом рассмотренных свойств систем можно утверждать, что множество показателей эффективности противодействия угрозам информационной безопасности компьютерных систем, представляющее совокупность взаимосвязанных и взаимодействующих показателей, выполняющих определенные функции, объединенных единой целью, является системой в силу соответствия следующим основным признакам:

- наличие цели, определяющей ее назначение как системы оценки защищенности информационных ресурсов компьютерных систем;
- устойчивость;
- наличие действий системы в соответствии с поставленными целями и обстановкой, обуславливающих оценку защищенности компьютерной информации как особый вид деятельности;
- наличие информации о внешней среде — механизмах защиты информации;
- наличие большого количества взаимосвязанных и взаимодействующих элементов;
- иерархичность структуры, представляющей деление системы на подсистемы;
- динамичность системы — изменение состояний и количества элементов.

В совокупности указанные предпосылки создают основу создания научно-методологической базы для исследования вопросов обеспечения защищенности компьютерной информации.

СПИСОК ЛИТЕРАТУРЫ:

1. Минаев В. А., Скрыль С. В., Дворянkin С. В. и др. Информатика: учебник для высших учебных заведений МВД России. Том 1: Информатика: Концептуальные основы. М.: Маросейка, 2008. — 464 с.