СТРУКТУРНО-ИНФОРМАЦИОННЫЕ АСПЕКТЫ БЕЗОПАСНОСТИ СЛОЖНЫХ СИСТЕМ

Л.С. СТРИГАЛЕВ

В современных условиях резко возросла актуальность создания высокоэффективных систем и средств безопасности. Необходим анализ и обновление традиционной парадигмы безопасности. Безопасность — неотъемлемое эмерджентное свойство сложной системы; это свойство структуры системы в ее четверке: система, структура, цель, технология [1]. Чем выше качество безопасности, тем более устойчива структура системы. В структуре системы заложена ее цель, порождающая технологию системы; угрозу представляет все то, что способно причинить вред структуре системы. Безопасность, как и у живых организмов, должна охватывать все структурные уровни.

У человека, например, сеть «датчиков» контролирует все жизненно важные органы, которые имеют многочисленные проекции (на коже такие проекции используются в акупунктуре и акупрессуре). Дополнительная, интеллектуальная безопасность человека, связана с тремя уровнями целеполагания: генетическим, неосознанным (условный и каузальный рефлексы; ментальность, привычка) и осознанным. Заметим, что именно неосознанному уровню в значительной степени обязаны, техногенные катастрофы.

В заключение отметим, что важен не только «охват» структуры защищаемой системы «нервной сетью», но и обеспечение заданного качества функционирования такой сети. В этой связи необходимы соответствующие методы и средства оценки качества информационного метаболизма. Ограничения на объем тезисов не позволяют детализировать данный аспект, который является достаточно хорошо проработанным в рамках информационного подхода применительно к системам обнаружения объектов.

Литература

1. Стригалев Л.С. // Экономическое развитие общества: инновации, информатизация, системный подход: Материалы Междунар. научно-экономической конф. 22–23 апреля 2008 г. Минск, 2008 С. 257–226.

КРИТЕРИИ ОЦЕНКИ КАЧЕСТВА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Л.С. СТРИГАЛЕВ

Оценка качества средств защиты информации занимает далеко не последнее место в проблемной среде индустрии компьютерной безопасности. Такие оценки необходимы при разработке и оптимизации средств защиты информации, а также при выборе средств защиты для реализации политики безопасности.

Стандарты в области компьютерной безопасности отображают вопросы методологии, менеджмента, включая управление и контроль рисков, но не содержат критерии оценки качества средств безопасности. Последнее обстоятельство способствует маркетинговым играм. Например, как отмечается в ряде источников, манипулируя критериями и условиями проведения эксперимента можно практически любой антивирус представить как наилучший. Подобное возможно для всех средств и систем, работа которых связана с двумя видами ошибок: ложное обнаружение и пропуск объекта. Более того иногда количественные оценки результатов машинных и даже натурных экспериментов могут превышать предельные возможности исследуемых систем (результат «подгонки» под требования ТЗ при отсутствии оценки предельных возможностей системы).