ПОДХОД К КЛАССИФИКАЦИИ УЯЗВИМОСТЕЙ КИБЕРНЕТИЧЕСКОЙ БЕЗОПАСНОСТИ СОЦИАЛЬНОТЕХНИЧЕСКИХ СИСТЕМ

Рубан И.В.

Харьковский национальный университет радиоэлектроники

Decomposition of social-technical systems to identify vulnerabilities and to develop structures and principles of construction of systems for combating cyber attacks.

Анализ реализованных кибернетических атак показывает, что они осуществляются при наличии внешних каналов несанкционированного доступа в систему или действий инсайдера [1,2,3]. Это обусловлено тем, что кибернетическая атака является реализацией угрозы посредством субъекта системы с использованием уязвимости компьютерной подсистемы для модификации управляющих воздействий с целью нарушения процесса функционирования.

Механизм действия кибернетической атаки состоит из основных этапов:

1. Заражение системы и поиск целевого программного обеспечения оборудования.
2. Захват управления.
3. Воздействие на технологический процесс управления, разрушение инфраструктуры, вывод из строя оборудования.

Исходя из этого, уязвимости социальнотехнических систем можно классифицировать следующим образом: уязвимости инфраструктуры, средств управления, элементов технологического процесса и средств контроля. Основным инструментом разработки комплексной системы безопасности кибернетических систем является декомпозиция таких систем на основе процессного подхода, что позвлило выделить четыре основных уровня:

- уровень кибернетической безопасности взаимодействия с внешней средой;
- уровень кибернетической безопасности процессов (взаимодействия подсистем);
- уровень кибернетической безопасности подсистемы;
- уровень кибернетической безопасности объекта.

Такой подход позволяет разрабатывать мультиагентные нейросетевые решения для построения кибернетических систем безопасности социальнотехнических систем.

Литература

1. http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet
2. Бурков В.Н., Грацианский Е.В., Дзюбко С.И., Щепкин А.В. Модели и механизмы управления безопасностью. Серия «Безопасность». - СИНТЕГ, 2001, 160 с.
3. Чирилло Дж. - Обнаружение хакерских атак.- СПб.: 2003.- 864 с.: ил.