СПИСОК ЛИТЕРАТУРЫ:

1. *Мирошниченко В. М.* Национальная безопасность Российской Федерации. Обеспечение и организация управления: книга. М: Экзамен, 2002.
2. *Боридько С. И., Забелинский А. А., Коваленко Ю. И., Тараскин М. М.* Защита информации в организациях: методика исследования угроз, уязвимостей и рисков: монография. М.: МИНИТ, 2011.
3. *Лихтарников Л. М., Сукачев Т. Г.* Курс лекций по математической логике (учебное пособие). Новгород: Новгородский государственный педагогический институт, 1993.
4. Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 29 декабря 2005 г. № 447-ст).

А. А. Тихомиров, А. И. Труфанов, А. Россодивита

МОДЕЛЬ ВЗАИМОДЕЙСТВУЮЩИХ СТВОЛОВЫХ СЕТЕЙ В РЕШЕНИИ ЗАДАЧ ТОПОЛОГИЧЕСКОЙ УСТОЙЧИВОСТИ СЛОЖНЫХ СИСТЕМ

Введение. В теории комплексных сетей, которая ярко заявила о себе в [1], окончательно сформировалась, интенсивно и глубоко прорабатывалась в течение последнего десятилетия, сети принято разделять на социальные, биологические и технологические. При этом основной исследовательский интерес базируется на платформе топологически изощренных, но однородных обособленных невзаимодействующих сетей, представляемых плоскими конструкциями классической теории графов. В то же время признано, что существует необходимость в изучении взаимосвязанных сетей [2], с помощью которых можно было бы адекватно описать сложные системы и учесть основные особенности взаимодействия и взаимовлияния их элементов. Практика информационной безопасности с традиционной стратификацией мер на этическую, правовую организационную, техническую, физическую и математическую компоненты и новой сетевой интерпретацией предполагает обязательность их комплексного применения, тем самым подтверждая эту необходимость.

Метод. Для построения сетевой модели, отражающей связи, характерные для реальных систем, во-первых, использовался заявленный ранее подход «кружева единых сетей», или CNL, в представлении стволовых сетей [3], т. е. тройками (S, T, C), где S является непустым множеством стволов, T — непустым множеством тематических слоев, а $C = (C_1, C_2, .. ., C_l)$ представляет собой набор бинарных отношений на множестве S, где C_i соответствует тематический слой i. В отличие от традиционной «плоской» комплексной сети, стволовая сеть изображается в виде объемной структуры. Во-вторых, принималась во внимание различная природа сетей и представляющих их акторов. Следуя [4], комбинации разнородных сетей предлагается называть композитными сетями.

Основные результаты. В настоящей работе определена новая — композитная — стволовая сеть как множество S-сетей, описанных на клумбах $B = \{B_1, B_2, .. B_m\}$, которые представляют собой непересекающиеся множества стволов. Тогда ассоциации — мультиплеты (пары, тройки…), включающие в себя неповторяющиеся стволы различных клумб (S_i, S_k, S_i, …), так называемые букеты, объясняют функционирование реального объекта. Другими словами, букеты составлены из стволов, последние крепят узлы многослойной сети одного и того же характера, например узлы транспортной сети — авиалиний, железных дорог, линий речного транспорта, автобусных маршрутов… Нами сознательно введена новая простая терминология для преодоления междисциплинарных

барьеров вокруг CNL. Заявляемая модель сети — композитная стволовая — предполагает связи между узлами как бинарные отношения трех типов: связь-«крепление» (B-связь), описывающая взаимодействие узлов одного и того же ствола; связь-«соединение» (C-связь), для узлов заданного слоя обособленной стволовой сети (отдельной клумбы) подобно связи в традиционной «плоской» комплексной сети; наконец, связь-«зависимость» (D-связь), управляющая взаимодействием между узлами различных стволов (принадлежащих различным клумбам) одного и того же букета. Такая детализация связей способствует глубокому пониманию реальных сетевых процессов и объективной постановке задач при моделировании атак на отдельные элементы сети (узлы, стволы, букеты, клумбы, слои, B-, C- и D-связи) и их комбинации. В рамках данной модели элементы сети реальной критической инфраструктуры рассматриваются как стволы, которые являются автономными или взаимосвязанными и взаимозависимыми как внутри, так и за пределами государства, региона и местной территории. Так, большинство объектов критической инфраструктуры, являющихся собственностью федеральных, региональных или местных органов власти или частного сектора, могут быть стратифицированы по различным слоям и соответствующим клумбам, одновременно оставаясь связанными с другими системами той же или иной природы. Композитное стволовое представление сети также дает возможность учесть многие топологические уязвимости реальных систем, что позволило дополнить классификационную схему атак [5].

Выводы. Предложена модель, формализующая сложные взаимодействия элементов сетей различной природы. Предполагается особо успешным и значимым применение данной модели к задачам управления чрезвычайными ситуациями. Сопутствующая классификация атакующих действий может быть полезна при анализе уязвимости не только абстрактных сетевых моделей, но и реальных систем.

СПИСОК ЛИТЕРАТУРЫ:

1. *Barabási A.-L., Albert R., Jeong H.* Mean-field theory for scale-free random networks // Physica A. 1999. Vol. 272. P. 173–187.
2. *Gao J., Buldyrev S. V., Stanley H. E., Havlin S.* Networks formed from interdependent networks // Nature Physics. 2012. Vol. 8. P. 40–48. URL: http://www.nature.com/nphys/journal/v8/n1/pdf/nphys2180.pdf (дата обращения: 21.12.2012).
3. *Тихомиров А. А., Труфанов А. И., Носырева Л. Л., Носырева Е. В.* Математическое описание стволовых сетей // Труды XVII Байкальской Всероссийской конференции. Т. 3. Иркутск, 2012. С. 149–153.
4. *Cheng H. K., Guo H.* Computer Virus Propagation in a Network Organization: The Interplay between Social and Technological Networks. Working Paper № 08-24, October 2008. – 28 p. URL: http://archive.nyu.edu/bitstream/2451/29495/2/Cheng_Guo_08-24.pdf (дата обращения: 21.12.2012).
5. *Тихомиров А. А., Труфанов А. И., Дмитриенко В. Н., Россодивита А., Шубников Е. В.* Классификация атак в имитационных исследованиях уязвимости комплексных сетей // Безопасность информационных технологий. 2012. № 1. С. 46–52.

Г. И. Хоруженко, М. А. Пудовкин

О СВОЙСТВАХ ЛИНЕЙНОГО АЛГОРИТМА РАЗВЕРТЫВАНИЯ КЛЮЧА БЛОЧНОЙ ШИФРСИСТЕМЫ SMALLPRESENT

Обобщенная блочная шифрсистема SmallPresent была представлена в работе [1] с целью детального исследования атак на блочную шифрсистему PRESENT. Так, например, в работах