на большом числе пользователей сетями ОП. Под термином «риск» понимается последствие реализуемых угроз ИБ [1, 2].

7. Риск при реализации угроз DoS ОКС-7 в результате фальсификации указанных сообщений подсистем МТР3 отражается на пользователях сетями ОП (ТфОП/ISDN, GSM, IN) в части:

- отказа в установлении соединения;
- отказа в предоставлении всех или определенных услуг интеллектуальной сети;
- ухудшения качества обслуживания.

8. Риск при реализации угроз DoS ОКС-7 может относиться к следующим соединениям:

а) в ТфОП/ISDN — международным, междугородним или местным;

б) в GSM — внутри одного региона страны, между разными регионами страны, между мобильными абонентами разных стран;

в) между абонентами ТфОП/ISDN и абонентами GSM;

г) в сети GSM мобильных абонентов домашней сети и абонентов-роумеров.

9. Заинтересованными в защите от угроз DoS ОКС-7 являются [3]:

- пользователи в отношении доверия к сети и услугам, предоставляемым конкретным оператором/поставщиком услуг;
- операторы сетей и поставщики услуг в обеспечении защиты своих эксплуатационных и коммерческих интересов, в выполнении своих обязательств перед населением;
- органы государственной власти в выполнении директив и законов, с тем чтобы обеспечить готовность предоставления услуг и добросовестную конкуренцию.

СПИСОК ЛИТЕРАТУРЫ:

1. *Драйберг Ли, Хьюитт Джефф.* Система сигнализации № 7 (SS7/ОКС7) протоколы, структура и применение. М.: Вильямс, 2006.
2. *Бельфер Р. А., Горшков Ю. Г.* Система сигнализации ОКС-7. Требования к QoS и организация программного обеспечения сетевого уровня. Учебное пособие МТУСИ. М.: ООО «Информсвязьиздат», 2007.
3. *Бельфер Р. А., Горшков Ю. Г., Даннави М. Н.* Алгоритмы в сетях связи общего пользования России // Электросвязь. 2008. № 8.

Н. В. Дмитриенко, А. И. Труфанов,
Иркутский государственный технический университет,
Р. Е. Лапорт, Ф. Ю. Линькова,
Университет г. Питтсбурга, Пенсильвания, США,
Е. В. Шубников
НИИ терапии, Сибирское отделение Российской Академии медицинских наук, Новосибирск

АРХИТЕКТУРА СВЯЗЕЙ УЧАСТНИКОВ ПРОЕКТА SUPERCOURSE И АНАЛИЗ ЕЕ УЯЗВИМОСТИ

Выполнен анализ связей в рамках интернет-проекта Supercourse. Исследованы топология и динамика сети, определены параметры, важные для понимания развития сети и ее безопасности.

Международный некоммерческий образовательный интернет-проект Supercourse [1] представляет собой инициативу по созданию библиотеки бесплатных лекций в области здравоохранения. На сегодняшний день участниками проекта являются более 55000 ученых и врачей из 174 стран, разместившие уже более 3500 презентаций в формате PowerPoint на 26 языках мира. Многие лекции посвящены проблемам терроризма, биотерроризма, биологической, информационной и общей безопасности. В данном исследовании Supercourse рассматривался как сложная эволюционирующая структура, которая дополняет сеть традиционного соавторства. Аналогично [2] в качестве узлов рассматривались авторы лекций, которые также имеют связи — соавторство в традиционных изданиях. Изучались такие параметры, как плотность распределения числа связей участников проекта, диаметр, коэффициент кластеризации, размер максимального кластера. Установлено, что средний диаметр сети авторов без учета объединяющей базы Supercourse характеризуется достаточно малой величиной ~ 6, что объясняется не спецификой предметной области, но склонностью авторов данного интернет-проекта к сотрудничеству. Оценка уязвимости сети к случайным и целенаправленным (направленным на кластеры) (за исключением SUPERCOURSE-концентратора) атакам указывает на безусловную ее стойкость.

СПИСОК ЛИТЕРАТУРЫ:

1. http://www.pitt.edu/~super1/.
2. *Barabási A. L., Jeong H., Neda Z., Ravasz E., Schubert A., Vicsek T.* Evolution of the social network of scientific collaborations. Physica A 311. 2002. P. 590–614.

А. А. Долгин
Московский энергетический институт (технический университет)

ПРОЦЕСС АНАЛИЗА ЗАЩИЩЕННОСТИ КАК ЧАСТЬ МОДЕЛИ АДАПТИВНОЙ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

В докладе рассмотрены модель адаптивной безопасности компьютерных систем и процесс анализа защищенности как ее часть. Практическим аспектом работы стало создание сканера уязвимостей системного уровня — DAScanner.

Снижение проблем в информационной безопасности требует адаптивного, высокочувствительного к изменениям, работающего в реальном режиме времени механизма. Модель адаптивной безопасности — именно такой подход, который позволяет контролировать, обнаруживать и реагировать в реальном режиме времени на риски безопасности, используя правильно спроектированные и хорошо управляемые процессы и средства.

Обеспечение безопасности в соответствии с данной моделью описывается как процесс, содержащий:

- технологию анализа защищенности (security assessment) или поиска уязвимостей (vulnerabilities assessment);
- технологию обнаружения атак (intrusion detection);
- адаптивный компонент, который включает в себя и расширяет две первые технологии.