7. Standards Board of ISACA. Continuous Auditing: Is It Fantasy Or Reality. URL: http://www.isaca.org/Content/ContentGroups/Journal1/20023/Continuous_Auditing_Is_It_Fantasy_or_Reality_.htm (16.01.2007).
8. *Scarfone K., Mell P.* Nist Special Publication 800-94, 2007: «Guide to Intrusion Detection and Prevention Systems».
9. *Zurutuza U., Uribeetxeberria R.* A methodology for continuous computer security auditing. Mondragon: Mondragon University Press, 2004.
10. *Searcy D., Woodroof B.* Continuous Auditing: Leveraging Technology // The CPA Journal. 2003. № 5.
11. CORAS project. URL: http://coras.sourceforge.net/ (21.01.2007).
12. AS/NZS 4360. Risk Management. Канберра: Australian Standard, 2006.

А. В. Бабаш
Российский государственный социальный университет, Москва

АКТУАЛЬНЫЕ ПРОБЛЕМЫ КРИПТОГРАФИИ

Указываются способы построения приближенных моделей шифрующих автоматов с целью построения методов их криптоанализа.

Одна из проблем криптоанализа и синтеза шифров состоит в построении «удачных» приближенных моделей функционирования шифрсистем. Удачная модель строится исходя из заданной шифрсистемы-оригинала и определяется условиями и целями задачи. Например, целью может быть определение ключа по заданной информации или открытого текста. Удачность модели трактуется как возможность нахождения решения поставленной задачи сначала для разработанной модели системы и возможность эффективного использования этой информации для решения начальной задачи для оригинала. Простейшим примером удачной модели является модель гомоморфного образа шифрующего автомата с меньшим числом состояний, чем у оригинала. Перечислим основные идеи подхода.

1. Обобщение гомоморфизма шифрующих автоматов путем замены отображений в определении гомоморфизма на а) бинарные отношения и б) автоматные отображения.

2. Использование следствий функционирования шифрсистемы. Например, использовать не сам известный шифртекст, а значение некоторой функции от него.

3. Использование в качестве моделей «слабых» шифрующих автоматов, близких по расстоянию Хэмминга к табличному заданию оригинала. Слабого автомата в том смысле, что нахождение решения исходной задачи для него не слишком трудоемко и это решение с приемлемой вероятностью является и решением для оригинала.

4. Использование в качестве модели «слабых» шифрующих автоматов, выходные последовательности которых близки в метрике Хемминга к выходным последовательностям оригинала.

В докладе конкретизируются данные идеи построения приближенных моделей автомата в терминах теории автоматов. Некоторые из основных результатов представлены в работах списка литературы.

СПИСОК ЛИТЕРАТУРЫ:

1. *Бабаш А. В.* Автоматные отображения слов, размножающие искажения в метриках Хемминга и Левенштейна не более, чем в K раз // Дискретная математика. 2002. Том 14. Вып. 3.

2. *Бабаш А. В.* Решение автоматных уравнений с искажениями в функции переходов автомата // Проблемы передачи информации. М., 2002. Том 38. Вып. 3.
3. *Бабаш А. В.* Isoperiods of output sequences of automata // Probabilistic Methods in Discrete Mathematics. VCP. Utrecht, 2002.
4. *Бабаш А. В.* Приближенные модели конечных автоматов // Обозрение прикладной и промышленной математики. 2005. Том. 12. № 2. С. 209–248.
5. *Бабаш А. В.* О восстановлении информации о входном слове перестановочного автомата Медведева по начальным и заключительным состояниям // Проблемы передачи информации. М., 2007. Том 43. Вып. 2. С. 74–84.

Е. К. Баранова
Российский государственный социальный университет (Москва)

АНАЛИЗ И УПРАВЛЕНИЕ РИСКАМИ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рассматриваются два подхода к обоснованию проекта подсистемы обеспечения информационной безопасности (ИБ). *Первый подход* основан на проверке соответствия уровня защищенности информационной системы (ИС) требованиям одного из стандартов в области информационной безопасности. *Второй подход* к построению системы обеспечения ИБ связан с оценкой и управлением рисками, изначально он исходит из принципа «разумной достаточности», примененного к сфере обеспечения ИБ.

На основе идентификации риска по трем параметрам:

— *угроза*, возможной реализацией которой вызван данный риск,

— *ресурс*, в отношении которого может быть реализована данная угроза,

— *уязвимость*, через которую может быть реализована данная угроза в отношении данного ресурса,

оценивается ожидаемый ущерб и сравнивается с затратами на меры и средства защиты, после чего принимается решение в отношении данного риска, который может быть *снижен*, *устранен*, *перенесен* или *принят*.

Рассматривается графовая модель системы безопасности с полным перекрытием, описываемая соотношением:

$S=\{O,Y,M,V,B\}$,

где O — набор защищаемых объектов; Y — набор угроз; M — набор средств обеспечения безопасности; V — набор уязвимых мест; B — набор барьеров, упорядоченных троек $bi=(yi, oj, mk)$, представляющих собой точки, в которых требуется осуществлять защиту в системе.

В модели определяется каждый объект, требующий защиты, оцениваются средства обеспечения безопасности с точки зрения их эффективности и их вклад в обеспечение безопасности всей ИС.

Отмечается, что рассмотренная модель безопасности с полным перекрытием применима в основном как инструментарий при разработке определенных политик безопасности либо в случае построения комплексной системы защиты информации для малого предприятия.