7. *Шаньгин В. Ф.* Информационная безопасность компьютерных систем и сетей. М.: ИД «ФОРУМ» — ИНФРА-М, 2008.
8. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: ТРИУМФ, 2002.
9. Распределенные вычисления. URL: http://distributed.ru.
10. *Menezes A., Van Oorschot P., Vanstone S.* Handbook of Applied Cryptography. CRC Press, 1996.
11. *Бабаш А. В., Шанкин Г. П.* Криптография. М.: СОЛОН-ПРЕСС, 2007. — 512 с.
12. *Чмора А. Л.* Современная прикладная криптография. М.: Гелиос АРВ, 2002. — 256 с.
13. Словарь криптографических терминов / Под ред. Б. А. Погорелова и В. Н. Сачкова. М.: МЦНМО, 2006. — 94 с.
14. *Гергель В. П.* Теория и практика параллельных вычислений. М.: БИНОМ, 2007. — 423 с.
15. *Kshemkalyani A.* Distributed Computing: Principles, Algorithms, and Systems. Cambridge University Press, 2008.
16. *Barbosa V.* An Introduction to Distributed Algorithms. The MIT Press, 1996.
17. *Sipser M.* Introduction to the Theory of Computation. 2005.

*А. А. Варфоломеев*

## О КЛАССИФИКАЦИИ СХЕМ ПЕРЕШИФРОВАНИЯ ПО ДОВЕРЕННОСТИ

Понятие перешифрования по доверенности (Proxy Re-Encryption — PRE) было предложено Блэйзом, Блумером и Страусом (Blaze, Bleumer, Strauss) на конференции «Еврокрипт» в 1998 г. Схемы перешифрования по доверенности (далее — прокси-перешифрование, PRE-схемы) служат для преобразования доверенным лицом шифрованного текста, предназначенного одному пользователю системы связи, в шифрованный текст для другого пользователя без возможности ознакомиться с открытым текстом.

Схемы прокси-перешифрования вызывают большой интерес в связи с их применениями в системах обеспечения безопасности информации. Указанные схемы используются в следующих областях:

- электронный документооборот,
- распределенные файловые системы (distributed file systems),
- фильтрация зашифрованного спама (outsourced filtering of encrypted spam),
- передача зашифрованных сообщений электронной почты (encrypted e-mail forwarding) и др.

К настоящему моменту предложено и проанализировано достаточно много таких схем. Это делает необходимым сбор информации по всем таким схемам, их упорядочивание и классификацию для практической реализации. Как известно, классификация — это процесс группировки объектов исследования в соответствии с их общими признаками. Примером первой классификации является классификация по возможности направления перешифрования: однонаправленные и двунаправленные PRE-схемы. В двунаправленных схемах доверенное лицо может преобразовывать шифртекст от одного пользователя к другому и наоборот. В некоторых приложениях требуется обеспечить только однонаправленное перешифрование от одного пользователя к другому, исключающее возможность перешифрования в обратную сторону, в других приложениях это не важно.

Предлагаемая в данной работе классификация базируется на наборе требований к функциональным возможностям схемы. На основе многочисленных найденных и проанализированных работ по PRE-схемам предлагается фасетная классификация в виде набора параметров A, B, C, D, E…, означающих наличие в схеме того или иного признака:

A-тип: по требованиям к возможности направлений преобразований шифртекста (*bidirectional* PRE, *unidirectional* PRE);

B-тип: по требованиям к возможности многократного преобразования шифртекста для цепочки пользователей (*multi-hop* PRE, *single-hop* PRE);

C-тип: по требованиям к необходимости использования билинейных отображений (bilinear maps, without bilinear maps);

D-тип: по требованиям к используемому предположению о трудно решаемой задаче (decisional Diffie-Hellman, etc);

E-тип: по требованиям к модели безопасности (standard model, random oracle model) и другие.

В скобках указаны в качестве примера возможные значения параметра классификации.

Термины из работ по схемам прокси-перешифрования могли бы пополнить список терминов следующей редакции Словаря криптографических терминов [4].

## СПИСОК ЛИТЕРАТУРЫ:

1. *Blaze M., Bleumer G., Strauss M.* Divertible protocols and atomic proxy cryptography // EUROCRYPT. Lecture Notes in Computer Science. Vol. 1403. Berlin: Springer-Verlag, 1998. P. 127–144.
2. *Libert B., Vergnaud D.* Unidirectional chosen-ciphertext secure proxy re-encryption // Public Key Cryptography. Lecture Notes in Computer Science. Vol. 4939. Berlin: Springer-Verlag, 2008. P. 360–379.
3. *Matsuda* T., *Nishimaki R., Tanaka K.* CCA Proxy Re-Encryption without Bilinear Maps in the Standard Model // PKC 2010. Lecture Notes in Computer Science. 2010.Vol. 6056/2010. P. 261–278.
4. Словарь криптографических терминов / Под ред. Б. А. Погорелова и В. Н. Сачкова. М.: МЦНМО, 2006. – 94 с.

*Е. И. Гончаров*

## ПРОБЛЕМА БЕЗОПАСНОСТИ БАЗ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ С ТРЕХЗВЕННОЙ АРХИТЕКТУРОЙ

В последнее время для построения информационных систем, в том числе благодаря бурному развитию Интернета, все чаще используют трехзвенную архитектуру. Она удобна как для публичных сервисов (информационные порталы, платежные сервисы и т. д.), так и для применения в закрытых ИС. В связи с распространением данной архитектуры проблемы ее безопасности становятся еще острее.

Трехзвенная архитектура состоит из:

1. базы данных (БД), в которой хранятся обрабатываемые данные и которая недоступна для пользователей системы напрямую,

2. сервера приложений — некоторого ПО, обрабатывающего запросы пользователей и взаимодействующего с базой данных,

3. клиентского приложения — некоторого ПО для взаимодействия с сервером приложений.

Безопасность подобных систем, как правило, обеспечивается следующим образом:

1. ограничение сетевого доступа к БД и анализ запросов с помощью межсетевых экранов и систем обнаружения вторжений таким образом, что только сервер приложений имеет прямой доступ к БД;

2. анализ запросов к серверу приложений посредством систем обнаружений вторжений;

3. разграничение доступа сервера приложений к базе данных путем использования учетных записей с минимальными правами;

4. ограничение на уровне СУБД прямого доступа к таблицам с помощью хранимых процедур и других технологий [1].

Таким образом, исходя из стандартных методов защиты первым рубежом защиты от несанкционированного доступа к БД является сервер приложений, вторым — СУБД. Однако