## Литература

1. Report on the Development of the Advanced Encryption Standard (AES): http://csrc.nist.gov/archive/aes/.

2. New European Schemes for Signatures, Integrity, and Encryption: http://cryptonessie.org/.

3. Pascal Junod, Serge Vaudenay. FOX: a New Family of Block Ciphers. http://crypto.junod.info/sac04a.pdf

4. Federal Information Processing Standards Publication 197 (FIPS PUB 197). Specification for the Advanced Encryption Standard (AES) // Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory. November 26, 2001. http://csrc.nist.gov/publications/fips/fips197/fips – 197.pdf

Евсеев С.П., Дорохов А.В.

## Обзор механизмов обеспечения безопасности и достоверности данных в информационных системах

*(ХНЭУ, Харьков, Украина)*

Проблема защиты информационных систем от несанкционированного доступа в современных условиях приобрела особую остроту.

Стремительное развитие коммуникационных и вычислительных технологий позволяет строить сложные информационные системы с распределенной архитектурой, объединяющие большое количество сегментов, расположенных на значительном удалении друг от друга.

Все это вызывает увеличение числа узлов сетей и количества различных линий связи между ними, что, в свою очередь, повышает риск несанкционированного подключения к информационной системе и доступа к конфиденциальной информации [1–3].

Увеличение объемов обрабатываемых и передаваемых данных в компьютерных системах и сетях, прежде всего в банковских системах, в системах управления крупными финансовыми и промышленными организациями, предприятиями энергетического сектора, транспорта, в системах управления и связи военного назначения требует новых подходов в организации протоколов и механизмов обеспечения безопасности передаваемых данных.

Естественное требование к безопасности и достоверности обрабатываемой и передаваемой информации в таких системах стоит очень остро, поскольку отказ системы или выход за установленные ограничения указанных параметров может привести к значительным финансовым и материальным потерям, снижению обороноспособности, ущербу экологии, жизни, здоровью людей.



Проведенный анализ показывает [1–6], что за последнее время общий объем обрабатываемой и передаваемой информации в компьютерных системах и сетях возрос многократно (на два-три порядка каждые пять-десять лет) и общие тенденции свидетельствуют, что такая динамика сохраниться.

Современные криптографические средства защиты информации в таких условиях должны обеспечивать своевременную обработку огромных объемов данных (десятки-сотни Мбит/с) и удовлетворять жестким требованиям по достоверности и безопасности информации.

Механизмы обеспечения безопасности информации в информационных системах в большинстве основаны на криптографических методах, общая классификация которых приведена на рис. 1.

Это методы симметричной и несимметричной криптографии, развитию которых посвящены многочисленные работы [1–11].

Перспективным направлением в развитии криптографических средств защиты информации доказуемой стойкости являются крипто-кодовые механизмы, построение которых основано на сведении задачи взлома ключевых данных к решению теоретико-числовой задачи декодирования случайного кода [7–11]. В некоторых источниках они получили название теоретико-кодовых схем (ТКС) [9–10].

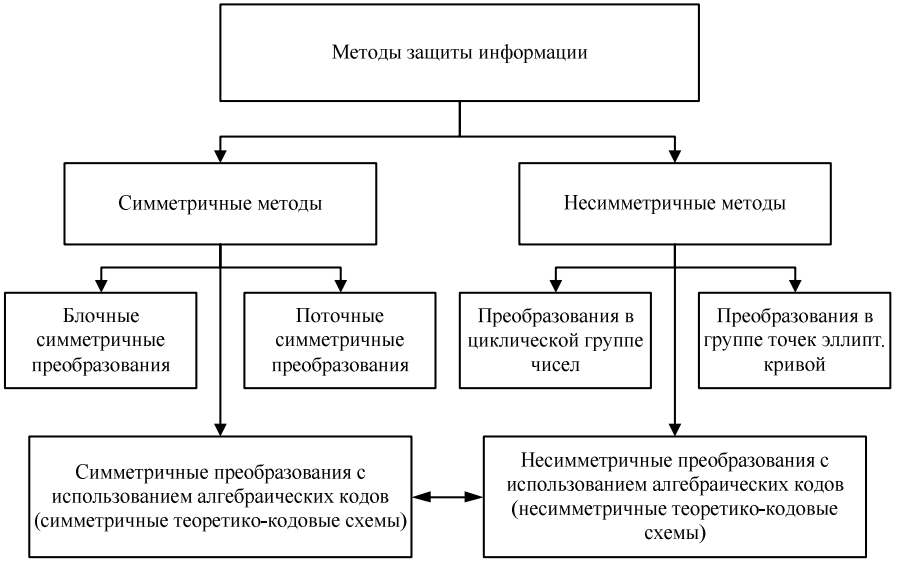


Рис. 1. Классификация криптографических методов защиты информации

Как показывает проведенный анализ, их применение позволяет реализовать быстрое криптографическое преобразование с обеспечением доказуемой стойкости.

Сложность их реализации сопоставима с симметричными криптоалгоритмами (блочно-симметричными шифрами БСШ)). Кроме того, их практическое использование позволяет применить инфраструктуру открытых ключей и строить интегрированные механизмы криптографического преобразования данных и канального кодирования для комплексного обеспечения безопасности и достоверности передачи данных.

В табл. 1 приведены результаты сравнительных исследований эффективности криптографических методов защиты информации при фиксированном уровне стойкости:

- среднем (сложность криптоанализа наилучшим известным алгоритмом не менее $2^{128}$ операций);
- высоком (сложность криптоанализа наилучшим известным алгоритмом не менее $2^{256}$ операций);
- сверхвысоком (сложность криптоанализа наилучшим известным алгоритмом не менее $2^{512}$ операций) [14].

Таблица 1

Сравнительная эффективность криптографических методов защиты информации при фиксированном уровне стойкости

| Методы криптографического преобразования | Модель безопасности | Длина ключевых данных, бит | Скорость крипт. преобр., бит/с | Дополн. функции |
|---|---|---|---|---|
| Блочные симметричные шифры | Практическая безопасность | 128, 256, 512 | $10^6 – 10^9$ | Нет |
| Поточные симметричные шифры | Практическая безопасность | 128, 256, 512 | $10^7 – 10^{10}$ | Нет |
| Несимметричные RSA-подобные криптоалгоритмы | Доказуемая безопасность | 3248 (128), 15424 (256) | $10^2 – 10^3$ | Нет |
| Несимметричные криптоалгоритмы на эллиптических кривых | Доказуемая безопасность | 283 (128), 571 (256) | $10^3 – 10^4$ | Нет |
| Несимметричные криптоалгоритмы с использованием кодовых конструкций | Доказуемая безопасность | $0{,}5\cdot10^6$ (128), $2\cdot10^6$ (256) | $10^6 – 10^8$ | Контроль ошибок, повышение достоверности |

Таким образом, как следует из приведенных результатов сравнительного анализа, несимметричные криптоалгоритмы с использованием теоретико-кодовых схем позволяют реализовать криптографическую защиту информации по технологии открытых ключей и обеспечить при этом скорость крипто-кодового преобразования информации со скоростью шифрования блочно-симметричных шифров.



Кроме того, в работах [10–12, 14] показано, что практическое использование теоретико-кодовых средств защиты информации позволяет на основе интеграции механизмов канального кодирования и шифрования комплексно обеспечить безопасность и достоверность передаваемых данных.

Следовательно, применение теоретико-кодовых схем, с одной стороны, экономически выгоднее применения целого комплекса различных механизмов шифрования и канального кодирования, решающих отдельно взятые задачи, а с другой – наблюдается существенное снижение суммарных вычислительных затрат, приходящихся на единицу обрабатываемой и передаваемой информации, т.е. за счет снижения времени обработки повышается оперативность передачи данных.

В свою очередь, общая классификация известных методов построения теоретико-кодовых схем приведена на рис. 2.

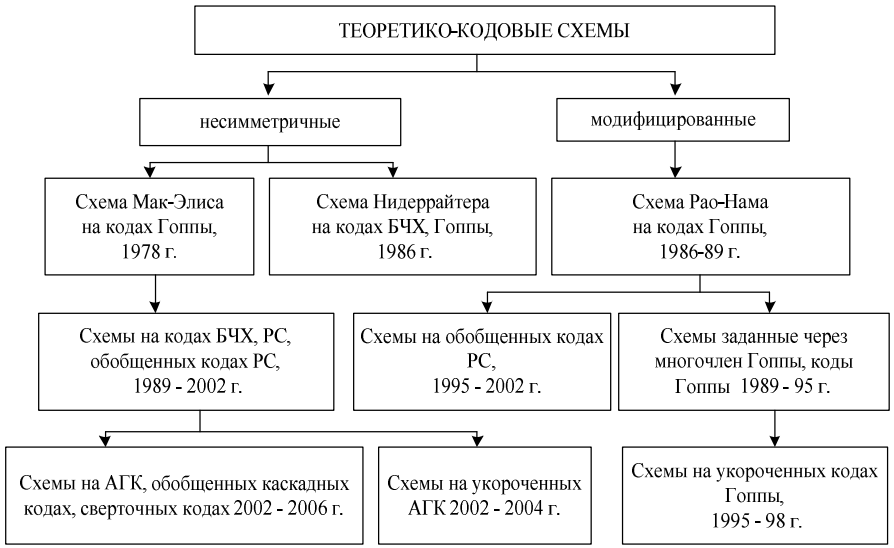


Рис. 2. Общая классификация теоретико-кодовых схем

Проведенный анализ и сравнительные исследования показали, что известные несимметричные крипто-кодовые средства защиты информации строятся по двум схемам: с маскированием порождающей матрицы кода (схема Мак-Элиса) и с маскированием проверочной матрицы кода (схема Нидеррайтера) [7, 8, 13].

В качестве исходных объектов могут выступать алгебраические блоковые коды с быстрым (полиномиальной сложности) алгоритмом декодирования, такие, например, как коды Гоппы, Рида-Соломона (РС), Боуза-Чоудхури-Хоквигнема (БЧХ) [7–11].

Таким образом, наиболее эффективными по стойкости к алгоритмам криптоанализа оказываются крипто-кодовые средства защиты информации (ТКС) с недвоичными линейными блоковыми кодами, возникающими на алгебраических кривых – алгеброгеометрическими кодами (АГК) [10–11].

С одной стороны, подобные конструкции устойчивы к атакам, предложенным Сидельниковым [9], с другой стороны, они обеспечивают высокие показатели достоверности и оперативности передачи данных [10–12].

**Литература**

1. Захист інформації в комп'ютерних системах від несанкціонованого доступу / За ред. С.Г. Лаптєва. – Киев, 2001. – 321 с.

2. Мамаев Е. Технологии защиты информации в Интернете. – СПб.: ИД Питер, 2001. – 848 с.

3. Харин Ю.С. Берник В.И., Матвеев Г.В., Агиевич С.В. Математические и компьютерные основы криптологии. – Минск: Новое знание, 2003. – 382 с.

4. Мао В. Современная криптография. Теория и практика. – М.: Вильямс, 2005. – 768 с.

5. Шнайер Б. Прикладная криптография. –М.: ТРИУМФ, 2003. – 816 с.

6. Молдавян Н.А., Молдавян А.А., Еремееев М.А. Криптография: от примитивов к синтезу алгоритмов. – СПб.: БХВ, 2004. – 448 с.

7. McEliece R.J. A Public-Key Criptosystem Based on Algebraic Theory // DGN Progres Report 42-44, Jet Propulsi on Lab. Pasadena, CA. January – February, 1978. – P. 114-116.

8. Niederreiter H. Knapsack-Type Cryptosystems and Algebraic Coding Theory // Probl. Control and Inform. Theory. – 1986. – V. 15. – P. 19-34.

9. Сидельников В.М. Криптография и теория кодирования // Материалы конференции «Московский университет и развитие криптографии в России», МГУ. – 2002. – 22 с.

10. Стасев Ю.В., Кузнецов А.А. Несимметричные теоретико-кодовые схемы с использованием алгеброгеометрических кодов // Кибернетика и системный анализ: Международный научно-теоретический журнал. – Киев: НАНУ. – 2005. – № 3. – С. 47-57.

11. Кузнецов А.А. Несимметричные криптосистемы доказуемой стойкости на алгебраических блоковых кодах // Радіоелектронні і комп'ютерні системи. Науково-технічний журнал – Х.: ХАИ, 2007. – № 8(27). – С. 130-144.

12. Науменко Н.І., Стасев Ю.В., Кузнецов О.О. Теоретичні основи та методи побудови алгебраїчних блокових кодів. – Х.: ХУ ПС, 2005. – 267 с.

13. Кузнецов А.А., Евсеев С.П. Разработка теоретико-кодовых схем с использованием эллиптических кодов // Системи обробки інформації / ХВУ. – Х., 2004. – Вип. 5. – С. 127-132.

14. Дудикевич В.Б. Дослідження несиметричних криптосистем на алгебраїчних блокових кодах для каналів з автоматичним перезапитом / В.Б. Дудикевич, Б.П. Томашевський // Науково-технічний журнал «Захист інформації». – 2008. – № 1. – С. 37-44.