как расширения простого поля характеристики 2 является нечётным числом, то квадратное уравнение требуется решать в квадратичном расширении исходного поля. В [3] предлагается метод, позволяющий осуществлять переход от квадратичного расширения к его подполю. Однако данный метод приводится без доказательства и, к сожалению, работает не во всех случаях. Существует и иной, более чёткий, способ перехода от расширения к подполю. Он основан на согласовании примитивных элементов мультипликативной группы поля и его расширения. Важным моментом является то, что данный способ может без изменений быть применён не только к квадратичным расширениям конечных полей, но и к произвольным циклическим группам и их подгруппам. В основе рассматриваемого подхода лежит тот факт, что для любого целого x, взаимно простого с целым m, и для любого целого n существует целое t такое, что t взаимно просто с mn и при этом t сравнимо с x по модулю m. Доказательство данного факта выводится из китайской теоремы об остатках.

Литература

1. *Липницкий В.А., Конопелько В.К.* Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. Минск, 2007. 239 с.
2. *McEliece R.J.* A public-key cryptosystem based on algebraic coding theory // Technical Report DSN 42-44, JPL, Pasadena, 1978.
3. *Муттер В.М.* Основы помехоустойчивой телепередачи информации. Л., 1990. 288 с.
4. *Богрецов В.А., Липницкий В.А.* Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных: материалы международного научно-технического семинара. Минск, 2012. С. 57–64.

АНАЛИЗ УЛУЧШЕННОГО АЛГОРИТМА ФОРМИРОВАНИЯ ОБЩЕГО КЛЮЧА С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

Н.В. БРИЧ

Создание канала защищенной передачи информации является одной из актуальных задач в различных сферах в настоящее время. Обобщенно защищенная передача может быть описана следующим образом: отправитель зашифровывает сообщение ключом так, что злоумышленник не может прочитать либо внести изменения в передаваемое сообщение. одним подходом в формировании общего секретного ключа является использование искусственных нейронных сетей (ИНС). ИНС — математические модели, программные и аппаратные реализации, построенные по принципу организации и функционирования биологических нейронных сетей. Одним из главных преимуществ нейронных сетей является возможность обучения и синхронизации. Синхронизированные ИНС — ИНС, весовые коэффициенты (ВК) которых одинаковы. Время, необходимое для синхронизации ИНС, много меньше времени, затрачиваемого на обучение ИНС. На основании этого свойства И. Кантер и В. Кинцель предлагают идею использования ИНС для решения проблемы распределения общего секретного ключа. На практике доказано, что изначально алгоритм обладает некоторыми уязвимостями, на основании которых применяется несколько типов атак — с использованием одной ИНС (методом грубой силы, геометрическая) и с использованием нескольких ИНС. Предлагается алгоритм, при использовании которого уменьшается время, необходимое для вхождения ИНС в синхронизм (соответственно, увеличивается криптостойкость протокола). ИНС в процессе синхронизации стремятся подавить вклад тех весовых коэффициентов (ВК),значения которых ошибочны — т.е. работа канала связи для этих весов неэффективна. Соответственно, корректируя ВК для персептрона с наименьшим значением весового коэффициента, мы с большой вероятностью производим шаг к сближению ВК обеих ИНС.При использовании ИНС для формирования общего ключа необходимо вдумчиво

Библиотека БГУИР

подходить к выбору начального вектора весовых коэффициентов, учитывая особенности реализации протокола. Количество ВК должно быть достаточным для формирования секретного ключа. Однако криптостойкость зависит от времени вхождения ИНС в синхронизм. Как вариант, можно формировать секретный ключ как результат конкатенации нескольких более коротких ключей, полученных в результате вхождения ИНС в синхронизм.

DEVELOPMENT OF INFORMATION SECURITY OF CORPORATE INFORMATION SYSTEMS ON THE BASE OF INTELLECTUAL TECHNOLOGIES

ZAHRA GHNABARI, V.A. VISHNYAKOV

The analysis of two directions of intellectual technologies in information security (IS) of corporate information systems (CIS) are given: intellectual supports of decision-making in IS of corporate systems and use it in cloud computing. As tendencies of development are considered improvement of methods, models, architecture, hardware-software decisions IT in IS for corporate systems.

For the development the theory and practice of information security (IS) for corporate information systems (CIS) exists such situation: on the one hand, increased attention to security of information objects, increased requirements for IS, on the other hand, increasing the damage caused by the owners of information resources [1]. The way out of this situation is the introduction in all phases of security the intellectual technology (IT), growing in importance in systems of IS. The main tasks that must address the intellectual system IS (ISIS): security detection the unknown attacks; auto-decision support solutions (DSS) on the redeployment of resources means IS CIS.

In work [2] separate offers on an intellectual problem of DSS are made: it is offered to consider threats as a set of channels of unauthorized access, information leakage and destructive influences; the technique of a numerical assessment of level of information security on a set of these channels is developed; the method of synthesis of rational sets of the means of protection consisting of compatible hardware-software products on criterion function is offered; algorithmic providing a subsystem of DSS on operational management of information security is developed; the architecture of creation of intellectual system of IS is offered.

Results on a problem of intellectual DSS in IS are received in work [1]:

1. The model of counteraction to threats of violation of the information security, based on use of the rational option of reaction of a method of decision-making adapted for a choice, is that the decision on a choice of option of reaction is made depending on probability of attack which is estimated with use of the mechanism of an indistinct logical conclusion, on the basis of data on safety events from various detectors.

2. Method of formation of a rational complex of means of protection being that on the basis of three-level model of protection are developed: morphological matrixes for each of levels; system of hierarchical criteria of quality of means of protection on the basis of their technical characteristics; options of hardware are generated; the rational option of a set for each level of protection on the criterion function maximizing the relation of a total indicator "security of information" to a total indicator of "expenses" gets out.

3. The structure of system of information security joins the rational sets which total cost doesn't exceed the resources allocated for protection that allows to receive a complex of the means of protection certified on the set class of security, meeting requirements to admissible expenses for its realization.

IS in the environment of cloud computing consists on [3]: the mathematical model of software representation is synthesized; the way and algorithm of the formal description of a classifying sign software and approach to an assessment of similarity of various copies of the

Библиотека БГУИР