СЕКЦИЯ 3. ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

SCADA SYSTEMS SECURITY

Al-Kamil Iehab Abduljabbar Kamil, N. Nasonova

Supervisory Control and Data Acquisition (SCADA) system is aimed at automatic controlling or monitoring the data and is composed of number of remote terminal units (RTUs) for collecting field data, hosts and nodes. SCADA systems cover large geographic areas and often require the use of wireless communications, supporting TCP/IP, UDP or other IP-based communications protocols as well as strictly industrial protocols. SCADA systems are exposed to the same cyberspace threats as any business system because they share the common vulnerabilities with the traditional Information Technology systems. Among the requirements to the SCADA systems security the following are suggested:

– critical components protection from cyber attacks, failures and strong safety policies and procedures development;

– knowledge management and training competencies for the personnel, based on policy, standards, design and attack patterns, threat models, code samples, reference architecture, and secure development framework;

– SCADA systems development, considering system security development starting from early stages and during the whole software development cycle, implementing the secure software development principles; this also concerns the security issues implementation in the devices;

– vulnerability analysis based on proactive, discovery, and adaptation solutions;

– the basic mechanisms to ensure network security for SCADA systems include authentication, confidentiality, integrity, availability, and nonrepudiation.

USE OF INTELLECTUAL AGENTS FOR INFORMATION SECURITY OF CORPORATE INFORMATION SYSTEMS

U.A. Visniakou, M.G. Mosduany Shiras

The methods of information protection include: management, regulation, motivation, compulsion, concealment of information. Information security tools include: formal (technical, software), informal (organizational, legal, moral and ethical) methods. Levels of information protection can be: the hardware and software, procedural, administrative. legislative. The protection system components are: physical security, safety personal, legal security, safety equipment, security software, security is telecommunication environment. Organizational protection measures determine the order: reference system of protection from unauthorized access; restrict access to premises; assignment of access; control and accounting of events; software maintenance; control of protection system.

Intellectual systems of information protection (ISIP) are devoted the attack detection systems. As a predictive tool ISIP use neural network (NN), the system of fuzzy logic and expert systems (ES). The scheme of attack detection includes detecting abuses and anomalies. In ISPI the knowledge base of ES contains the descriptions of the classification rules according relevant user profiles and the scenarios of attack on the information system (IS). Disadvantages of ISIP on ES: system is not adaptive, its not detect always unknown attacks.

The use of hybrid neuro-expert systems or neuro-fuzzy systems let to reflect in the system structure the fuzzy predicate rules which are automatically adjusted during neuron net (NN) training. The adaptive fuzzy NN let to solve individual tasks to identify threats comparing the behavior of users with existing template system and automatically configure new rules when changing field of threats. A new trend in ISPI is the use of intellectual agents (IA) working in a distributed IS and programmed for search as the invasion and anomalies. The following areas of IA use in information protection are identified: research on attack detection systems (ADS); automation of search in IP (organizations, technologies, services, etc.); intellectualization of decision in DP.

The use of multi-agent systems for IP is following. It is necessary to investigate widespread attacks on the information system and the process of implementation of the attacks; investigate the existing systems of attack detection and attack detection methods; design a multi-agent structure and composition of the ADS. Its develop the structure of agent in attack detection system; work out the model for knowledge representation of agents about the state of information system; develop the method of joint analysis by agents of the

information system state. The multi-agent architecture ADS involves many interacting intelligent agents. The standard IS components, sources of information to be analyzed for attack detection are proposed. The structure of agents, which includes modules: management, receiving and processing data, analysis, training, response, generate messages, making a decision. The function of modules are describes. Methods of work with a multi-agent ADS includes steps: placement agents by blocks of IS, data collection, the formation of training set, attack detection, and reporting it to the administrator.

ВРЕМЕННАЯ ПСЕВДОСЛУЧАЙНАЯ ПЕРЕСТРОЙКА ЦИФРОВЫХ ОПТИЧЕСКИХ ИМПУЛЬСНЫХ СИГНАЛОВ И ПЕРСПЕКТИВЫ ЕЕ ИСПОЛЬЗОВАНИЯ

Ю.Н. Аксенов

В работе предлагается способ передачи информации в оптических системах связи — временная псевдослучайная перестройка цифровых двоичных с активной паузой оптических импульсных сигналов ультрафиолетового, видимого и инфракрасного диапазонов (МИНСКИЙ КОД). Новый способ передачи информации позволит решать актуальные проблемы в связи: повысить помехозащищенность, обеспечить защиту информации от несанкционированного доступа, избавиться от вредного излучения радиоволн и границ проводной связи и др.

В современном мире передача информации осуществляется при помощи радиосигналов, проводной и оптоволоконной связи. Радиосигналы влияют на здоровье человека и электронные устройства. Современные системы атмосферной оптической связи FSO не могут использоваться в качестве интерфейсов подвижных устройств и в открытых водных пространствах, используемое в них излучение лазера опасно для человека. Квантовые оптические системы работают на малых расстояниях. Оптические фемтосотовые сети связи OLAN с корреляционным приемом сигналов и с использованием белых светодиодов позволят избавиться от этих проблем.

Широко применяемые в оптических системах связи аналоговый и цифровой виды модуляции сигналов имеют ряд недостатков. Так аналоговая модуляция подвержена нелинейным искажениям и помехам, а оптическая цифровая модуляция (более сложная) использует сигналы с пассивной паузой.

Предлагаемый вид модуляции оптических сигналов основан на импульсной модуляции (Pulse-position modulation, PPM).

В одноканальной системе связи информационный импульс, длительностью $\tau_0 << T$ (в пс), смещается относительно импульса «маркера», например, с периодом T = 300 нс на время $-\tau$ при символе «0» и на время $+\tau$ при символе «1».

При множественном доступе в системе сотовой оптической связи или в многоканальной системе оптической связи вводится кодирование путем временной псевдослучайной перестройки цифровых оптических импульсных сигналов. Информационные импульсы «1» и «0» абонента k, смещаются дискретно во временном интервале T на текущий временной сдвиг $\tau_k = T \pm \tau - \Gamma_k(t)\,\tau_o$, где $\Gamma_k(t)$ — персональный коэффициент временно́го сдвига импульса k-го абонента целочисленной псевдослучайной последовательности.

Достоинства предложенного вида модуляции: повышается помехоустойчивость, скрытность, безопасность связи; увеличивается объем, скорость передаваемой информации и пропускная способность каналов. При использовании предложенной модуляции появляются некоторые перспективы применения FSO в населенных пунктах, на промышленных объектах, в замкнутом пространстве (стадионе, самолете, доме и т. д.), в космосе и в открытом море.

СОЦИОЛОГИЯ ИНТЕРНЕТ: МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ИНФОРМАЦИОННОГО ПРОТИВОСТОЯНИЯ

А.У. Актаева, Н.Г. Галиева, Г.Б. Байман

В XXI веке современный этап развития общества характеризуется высокой степенью его информатизации и возрастающей ролью ИКТ, которые активно влияют на состояние политической, экономической, оборонной и других составляющих безопасности государства и их граждан. Для разрешения различных социальных и межгосударственных конфликтов все чаще используется информационная сфера, что порождает такое явление как «Информационная война, информационное противостояние, дезинформация, информационные конфликты» характеризующееся, с одной стороны, воздействием на информационную сферу противника, а с другой — принятием ряда мер по выявлению и защите своих элементов информационной инфраструктуры от деструктивного и управляющего воздействия.