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.