определения угроз безопасности информации в информационных системах» [1]. Документ устанавливает единый подход к определению угроз безопасности информации и разработке моделей угроз безопасности информации в ИС.

В докладе обсуждается опыт применения методики для КИС предприятия на этапе сопровождения. Для КИС характерны следующие исходные данные: имеет подключение к сетям общего доступа; является многопользовательской ИС; является системой с разграничением прав доступа; предназначена для обработки конфиденциальной информации, в том числе ПДн категории «Иные» сотрудников и пользователей системы.

Согласно критериям оценки, уровень защищенности оценивается как «средний», в связи с тем, что более 70% характеристик соответствуют уровню не ниже «средний» определенными характеристиками КИС. Данному уровню исходной защищенности ставится в соответствие числовой коэффициент Y1=5. Таким образом, в отношении ПДн, обрабатываемых в КИС, актуальными являются следующие угрозы безопасности: действия вредоносных программ; утрата ключей и атрибутов доступа; доступ к информации, копирование, модификация, уничтожение лицами, не допущенными к ее обработке; разглашение информации, копирование, модификация, уничтожение сотрудниками, допущенными к ее обработке. По результатам анализа определен состав и содержание организационных и технических мер по обеспечению безопасности ПДн.

Литература

1 Методика определения угроз безопасности информации в информационных системах [Электронный ресурс]. – URL: https://fstec.ru/component/attachments/download/812 (дата обращения: 17.05.2018).

ГЕНЕРАЦИЯ СЛУЧАЙНЫХ ЧИСЕЛ НА ОСНОВЕ НЕЙРОННОЙ АКТИВНОСТИ МОЗГА

А.О. Молчан

Случайные числа в современном мире имеют огромное значение и являются его неотъемлемой частью. Они получили широкое применение в IT сфере, криптографии и других сферах жизни. Почти всем системам компьютерной безопасности, в которых применяется криптография, необходимы случайные числа – для ключей, уникальных чисел в протоколах и т.п. – и безопасность таких систем часто зависит от произвольности случайных чисел. Если генератор случайных чисел ненадежен, вся система выходит из строя.

В общем случае все генераторы случайных чисел можно разделить на генераторы псевдослучайных чисел, как правило, реализованы программами, и генераторы случайных чисел, реализуемые в большинстве своем как аппаратно-программные решения. Аппаратный генератор случайных чисел – устройство, которое генерирует последовательность случайных чисел на основе измеряемых, хаотически изменяющихся параметров протекающего физического процесса. Например, генерация на основе теплового шума в резисторе.

Цель исследования: выявить возможность использования нейронной активности мозга в качестве источника случайной величины для аппаратно-программного генератора случайных чисел. В качестве источника случайной величины предполагается использование электроэнцефалограммы головного мозга человека.

В ходе математического анализа электроэнцефалограмм будет определена возможность использования активности головного мозга человека в качестве источника случайной величины для генератора случайных чисел. Данные исследования могут открыть новое направление развития генераторов случайных чисел и использоваться в системах шифрования данных.

ПРОБЛЕМЫ БЕЗОПАСНОСТИ В ПРОГРАММНО-ОПРЕДЕЛЯЕМЫХ СЕТЯХ

Б.А. Монич

Программно-конфигурируемые сети представляют собой сети, в которых разделены уровни управления сетью и коммутации потоков данных. Данная архитектура сети предоставляет возможность программного управления пересылкой данных, которое логически

и физически отделено от коммутаторов и маршрутизаторов. Все функции управления сетью выполняются приложениями на отдельном физическом сервере-контроллере. В архитектуре программно-определяемых сетях можно выделить три уровня: инфраструктурный уровень, представляющий набор сетевых устройств (коммутаторов, маршрутизаторов, каналов передачи данных); уровень управления, включающий в себя сетевую операционную систему, которая обеспечивает приложениям сетевые сервисы и программный интерфейс для управления сетевыми устройствами и сетью; уровень сетевых приложений для более гибкого и эффективного управления сетью, позволяет выполнять различные изменения и настройки сети без прерывания сервисов и видимых изменений со стороны пользователей сети. Основными требованиями к безопасности в программно-определяемых сетях являются требования к обеспечению защиты управляющего контроллера. В первую очередь контроллер требуется защитить физическим образом и ограничить к нему доступ рабочего персонала. Работа по настройке и изменениям конфигурации сети должна проводиться в выделенной защищенной виртуальной сети. Для обеспечения отказоустойчивости, программно-определяемой сети, существует необходимость предусмотреть физическое резервирование управляющего контроллера, который должен вступать в работу, в случае взлома или отказа основного контроллера. В типичном сегменте программно-определяемой сети между контроллером и коммутатором используется безопасное соединение SSL (Secure Sockets Layer), данные методы шифрования могут быть достаточными для передачи информации внутри ЦОД, но вряд ли подойдут для внешних сетей, поскольку возникают проблемы, связанные с управлением ключами, возрастанием расходов и задержки шифрования.

Литература

1. Heller R. Sherwood, McKeown N. The controller placement problem // Proceedings of the first workshop on Hot topics in software defined networks, ser. HotSDN'12. ACM, 2012.

2. Smeliansky R.L., Gamaynov D. The model of network applications behavior. Moscow: Proggraming and Computer software, 2007.

3. Основы программно-конфигурируемых сетей / Н.Ф. Бахарева [и др.]. Самара: ПГУТИ, 2015. 111 с.

ПОЛЯРИЗАЦИОННАЯ МОДУЛЯЦИЯ В СВЧ МОДУЛЕ МИЛЛИМЕТРОВОГО ДИАПАЗОНА ДЛИН ВОЛН

В.В. Муравьёв, С.А. Кореневский, Н.М. Наумович, А.А. Стануль, П.И. Карпович

В настоящее время для обеспечения защиты передаваемой информации в системах телекоммуникаций все более широкое применение находит миллиметровый диапазон длин волн. В этом диапазоне частот имеется возможность обеспечения большой полосы частот излучаемого сигнала и узкой диаграммы направленности при малых габаритах антенных устройств, что повышает скрытность работы системы связи. Ширина диаграммы направленности определяется диаметром антенного устройства. Для повышения защищенности передаваемой информации СВЧ модуль может работать с фазовой и поляризационной модуляцией. Современная элементная база позволяет разрабатывать модули, обеспечивающие мощность выходного сигнала 2 Вт, в диапазоне частот 36–37 ГГц [1]. Дальнейшее увеличение мощности выходного сигнала передающего устройства может быть обеспечено путем суммирование мощностей двух усилителей. Применение сумматоров на мостовых схемах приводит к уменьшению к.п.д. выходного сигнала. Для повышения суммарного к.п.д. передающего устройства, суммирование мощностей осуществляется в полосковом облучателе антенного устройства. Поляризации сигналов, возбуждаемых каждым из усилителей ортогональны, что позволяет обеспечить хорошее согласования выходных сопротивлений усилителей и полоскового излучателя. Это позволяет обеспечивать поляризационную модуляцию путем изменения разности фаз выходных сигналов усилителей

Литература

1. СВЧ модуль полудуплексной системы связи миллиметрового диапазона длин волн / В.В. Муравьёв [и др.]. // Технические средства защиты информации : тезисы докладов XV Белорусско-российской науч.-техн. конф. Минск, 6 июня 2017 г. С. 94.