M кодовых слов $\boldsymbol{X}$ над полем Галуа в сравнении с линейными кодами, что важно для защиты информации. Рассматривается подход защиты кодированной информации в предположении, что преднамеренно генерируемые ошибки $\boldsymbol{E}$ в принятом сигнале и шумы n в канале с подслушиванием должны существенно увеличить значение вероятности ошибки декодирования кодового слова в условиях ограничения времени на анализ и обработку перехватываемого сигнала. В этом случае на входе декодера канала с подслушиванием формируется вектор наблюдения $\boldsymbol{Y}$ в виде трехкомпонентного аддитивного процесса: векторов слов кода $\boldsymbol{X}$, векторов ошибок $\boldsymbol{E}$ и векторов шума n канала. Так как значения вероятностей $P(x)$ входа и $P(y)$ выхода основного канала априори известны и практически равны, то в соответствии с теоремой Байеса, зная переходные вероятности $P(\boldsymbol{Y} \mid \boldsymbol{X})$ канала, легко можно найти вероятность $P(X \mid Y)$ правильного декодирования информации по основному каналу. Наилучшая процедура декодирования вектора наблюдения $\boldsymbol{Y}$ по каналу подслушивателя состоит в нахождении такого значения номера кодового слова, при котором значение вероятности $P(\boldsymbol{Y} \mid \boldsymbol{X})$ достигает максимума [1]. Поскольку в канале подслушивателя функция $\max P(\boldsymbol{Y} \mid X)$ зависит от большого числа M, от структуры векторов внедряемых ошибок $\boldsymbol{E}$ и векторов шума n, байесовская процедура нахождения вектора $\boldsymbol{X}$ ближайшего по расстоянию d к принятому вектору Y становится затратной с точки зрения необходимости значительных вычислительных, временных и технических ресурсов для успешного перехвата кодированной информации.

Литература

1. Митюхин А.И., Якубенко П.Н. Корреляционные спектры и кодовые расстояния мажоритарных последовательностей // Докл. БГУИР. 2015. № 4 (90). С. 5–9.

ИСПОЛЬЗОВАНИЕ МЕЖСЕТЕВОГО ЭКРАНА НОВОГО ПОКОЛЕНИЯ В КОРПОРАТИВНЫХ СЕТЯХ

А.Д. Михейчик, О.А. Хацкевич

На сегодняшний день практически все организации осуществляют информационную безопасность своей корпоративной сети, используя различные средства. К таким средствам можно отнести: антивирусные ПО, межсетевые экраны, DLP-системы, системы обнаружения и предотвращения вторжений. Проблема заключается в том, что если использовать комплексное решение по обеспечению информационной безопасности сети, то могут возникнуть случаи, когда одно средство по безопасности будем считать другое средство угрозой для сети. Данная проблема может возникнуть, если в качестве комплексного решения использовались средства по информационной безопасности различных производителей. Для решения проблемы предлагается использовать набирающие популярность в последнее время межсетевые экраны нового поколения (МЭНП).

Межсетевые экраны нового поколения (англ. Next-Generation Firewall) – это совокупность средств, в которые входят: межсетевой экран, система обнаружения и предотвращения вторжений, DPI-технология, DLP-система. Некоторые МЭНП, например Fortigate 3810A, могут поддерживать антивирусное ПО, а также обнаружения DoS-атак. Отличие от обычного межсетевого экрана заключается в том, что МЭНП включает в себя больше уровней модели OSI, улучшая фильтрацию сетевого трафика, зависящую от содержимого пакета.

ОПЫТ ПРИМЕНЕНИЯ МЕТОДИКИ ОПРЕДЕЛЕНИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Е.В. Моженкова, А.И. Парамонов

Корпоративная информационная система (КИС) должна обеспечивать не только ведение учета и формирование отчетов по национальным и международным стандартам, а также предупреждать попытки несанкционированного доступа к информации. Для определения угроз безопасности персональных данных (ПДн) при их обработке в информационных системах (ИС) в Российской Федерации разработана «Методика

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