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