мощности проводимых DDoS-атак постоянно возрастают (до 500 Гбит/с в 2015 г.), а стоимость организации таких атак постоянно падает (1 час — $5, неделя — $260, месяц — $900).

2. Проведение DDoS-атак возможно на всех семи уровнях модели OSI. Наибольший интерес для злоумышленников представляют удаленные DDoS-атаки на сетевом (3), транспортном (4) и прикладном уровнях (7).

3. Особенную опасность представляют DDoS-атаки с использованием метода усиления (амплификатора).

ИССЛЕДОВАНИЕ СЕТЕВЫХ СЕРВИСОВ/РЕСУРСОВ КРЕДИТНО-ФИНАНСОВЫХ ОРГАНИЗАЦИЙ НА ПРЕДМЕТ ПРОВЕДЕНИЯ DOS / DDOS-АТАК

В.В. Маликов, М.А. Бабич, Г.В. Обрядин

Главной предпосылкой для успешного проведения DoS-атак являются ошибки программного кода в реализации соответствующих сетевых сервисов/ресурсов, которые позволяют выполнить недопустимую инструкцию или исключительную ситуацию, которая может привести к аварийному завершению процесса/службы.

Авторами исследован уровень информационной безопасности сервисов/ресурсов в сети интернет на примере кредитно-финансовых организаций (КФО) Республики Беларусь. Для проведения исследования были выбраны 20 белорусских КФО из реестра Национального банка Республики Беларусь, имеющие специальные разрешения (лицензии) на осуществление банковской деятельности.

По результатам проведенного исследования, можно сделать следующие выводы:

1. В настоящее время существуют предпосылки для проведения DoS / DDoS-атак на сервисы / ресурсы КФО в сети интернет за счет наличия множества ошибок в программном коде, а также критических уязвимостей в алгоритмах реализации программного обеспечения (ПО).

2. Тестирование программного кода (тест ПО «CSE HTML Validator Professional») сервисов/ресурсов КФО показало, что все 100% КФО имеют ошибки в коде, а в коде одной из КФО имеются 2 грубые ошибки. Данная ситуация существенно увеличивает риск проведения DoS / DDoS-атак.

3. Особую опасность представляют уязвимости в реализации алгоритмов / протоколов шифрования (например: CVE-2016-0800), так как указанное ПО обеспечивает в том числе удаленное проведение финансовых операций:

– результаты проведенного тестирования (тест ПО «DROWN-attack») сервисов/ресурсов КФО на предмет реализации уязвимости CVE-2016-0800 показали, что в 20% КФО возможно проведение DROWN-атаки;

– тестовая эксплуатация уязвимости CVE-2016-0800 (DROWN) на уязвимом поддомене одной из КФО с использованием ресурсов ПО «Censys» позволила выделить секретный ключ, используемый для шифрования информации.

СОКРЫТИЕ ИНФОРМАЦИИ В СЕТИ С ЦЕЛЬЮ ЗАЩИТЫ

А.Л. Мастыкин

В настоящее время возможности предоставляемые пространством не индексированной части интернета («темного интернета» или «darknet») по сокрытию информации серьезно недооценены. Ими просто пренебрегают. Тяжело даже предположить соотношение «видимой» (легко доступной) его части и «невидимой» (той, которая требует для доступа к себе специального подхода). Проблему представляет не столько наличие динамики в строении этих составляющих, сколько размытость границ между ними. По большей части «темный интернет» представляет собой «свалку» того, что когда-то являлось ресурсом открытого интернета или никогда не использовалось вовсе, того что популярные поисковые системы, по какой-либо причине, оставили без внимания. Ежедневно в «сеть» загружаются и выкачивается огромное количество информации. К концу 2016 года трафик достигнет зеттабайта, а к 2019 двух зеттабайт в год [1]. Ежегодный прирост общего объема информации составляет 24% [2]. И это говорит о том, что количество информации в отмирающих ресурсах также колоссально. Хаотичность условий нахождения в сети «забытых» ресурсов дает возможность скрытого размещения нужной информации, предназначенной для узкого круга лиц. Эта информация может быть анонимно, как размещена, так и принята.

На текущий момент широко используется шифрование данных, которое имеет предназначение обессмыслить полезную информацию для всех кроме тех, кому она предназначена, либо затруднить дешифрование третьими лицами, на срок пока та актуальна. В случае намеренного сокрытия полезной информации в лавине «мусора» ее поиск может составить весьма впечатляющий период времени (если вообще увенчается успехом). Комплексное применение вышеупомянутого варианта сокрытия информации в «даркнете» и метода шифрования существенно снизит эффективность поисковых и дешифровальных систем оппонирующих организаций, из-за необходимости неоправданного увеличения имеющихся вычислительных мощностей.

Литература

1. The Zettabyte Era — Trends and Analysis.// Cisco.com [Электронный ресурс]. — 2015. — Режим доступа: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/VNI_Hyperconnectivity_WP.html. — Дата доступа:11.05.2016.

2. Data volume of global consumer IP traffic from 2014 to 2019.// Statista.com [Электронный ресурс]. – 2016. – Режим доступа: http://www.statista.com/statistics/267202/ data-volume-of-global-consumer-ip-traffic/. – Дата доступа:11.05.2016.

ВЕКТОРНОЕ КВАНТОВАНИЕ СИГНАЛОВ НА ОСНОВЕ МНОГОМЕРНЫХ РЕШЕТОК

А.И. Митюхин, Д.В. Шакинов

В специальных системах с защитой информации одним из основных требованием является эффективное использование канального ресурса. Для реализации данного требования широко используются методы энтропийного, универсального и спектрального кодирования (сжатия). Известно, что для целей сжатия можно применять и методы векторного квантования, как способа кодирования непрерывного источника [1].

В работе исследуется конструкция векторного квантователя на основе точек решетки в виде слов блокового помехоустойчивого кода C над полем GF(2) длиной r. В этом случае входная последовательность отсчетов $x = (x_1, \dots x_n)$ сигнала (изображения), как точка решетки, будет соответствовать n-мерному вектору в преобразуемых пространствах $R^n \rightarrow Z^n$, а кодовые слова кода выступают в качестве аппроксимирующих точек входа. Рассматривались решетки, представленные аддитивной подгруппой L = <M; + 0>, где M = 16 — объем кода (кодовая книга квантователя), 4 — размерность кода. Построение решетки основывалось на операции разложения группы порядка 2^4 на смежные классы по подгруппе L. Элементы всех объединенных смежных классов соответствуют квантуемым отсчетам x. В качестве лидеров смежных классов записывались кодовые слова с принадлежит множеству C.

Процесс квантования сводится к нахождению точки решетки — номера кодового слова c, ближайшего к $x = (x_1, \dots x_n)$ и координат $l = (l_1, \dots l_n)$ аппроксимирующего вектора $y = (y_1, \dots y_n)$ входа квантователя. При этом выполняется: 1) скалярное квантование компонент последовательности отсчетов $x = (x_1, \dots x_n)$; 2) находится минимальное евклидовое расстояния между точками x и y. Показано, что на эффективность кодирования и значение минимальной ошибки при обратном преобразовании декодером канала влияют структурные особенности применяемых кодов.

Литература

1. *Конвей Дж., Слоэн Н.* Упаковки шаров, решетки и группы: В 2-х т. Пер. с англ. М., 1990.

О ПОСТРОЕНИИ МОДЕЛИ СЕТЕЦЕНТРИЧЕСКОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Е. Б. Михайловский

В современных условиях развития информационно-коммуникационных систем, когда вся информация образует общее информационное поле, возрастают требования к системам централизованного хранения и к сетям передачи данных. При иерархической модели построения систем информационные поля существовали на каждом уровне, и доступ к ним был ограничен персоналом соответствующего уровня.

Сетецентрическая информационно-управляющая система [1] представляет собой распределенную систему в виде множества независимых агентов, соединенных каналами связи, рассматриваемую пользователями в виде единой объединенной системы. Совокупность ее свойств