эффективности решения вышеуказанных задач определим значение предотвращенного ущерба [2]. При расчете данного показателя учитывается важность цели, которая в настоящий момент задается оператором вручную. Однако, не вызывает сомнения тот факт, что важность цели неразрывно связана с ее классом и задачей выполняемой в налете. Таким образом автоматическое определение классов воздушных объектов позволит достоверно определить важность цели, а, следовательно, и величину предотвращенного ущерба при решении задач распределения усилий и целераспределения. Результаты решения научной и практических задач диссертационной работы позволят выявить недостатки существующих методов распознавания целей, выработать последовательность и этапы решения задачи распознавания целей. Это позволит решать задачи распределения усилий и целераспределения более эффективно.

Литература

1. Скорик А.Б., Воронин В.В., Зверев А.А., Галицкий О.Ф. // Сб. науч. тр. Харьковского университета Воздушных Сил. 2010. № 3. С. 8–14.

2. Кругликов С.В. // Доклады БГУИР. 2013. № 5. С. 93–99.

СВОЙСТВА СИНДРОМОВ ОШИБОК ПРИМИТИВНЫХ БЧХ-КОДОВ

В.А. Липницкий, Н.В. Спичекова

В современных цифровых телекоммуникационных системах (ТКС), за исключением волоконно-оптических, для обнаружения и исправления ошибок, возникающих при передаче информации по каналу связи, используются помехоустойчивые коды. На практике широкое применение получили БЧХ-коды.

На сегодняшний день самый массовый вид ТКС — системы мобильной связи — обеспечивают исправление двойных ошибок на блок передаваемой информации. Практические потребности увеличения скоростей информационных потоков требуют исправления ошибок кратности, большей двух.

Процедура декодирования БЧХ-кода начинается с вычислени синдрома. Неравенство синдрома нулю является единственным свидетельством наличия ошибки в принятом блоке-сообщении. В примитичном БЧХ-коде C_9 длиной $n = 2^m - 1$ и конструктивным расстоянием 9 синдромы всех ошибок весом w, $1 \le w \le 4$, попарно различны. Данный факт является основой синдромных методов коррекции ошибок. Первым шагом в применении синдромных методов на практике является определение веса возникшей ошибки.

Авторами были исследованы свойства синдромов ошибок весом 1–4 в примитивных БЧХ-кодах C_9, сформулирована методика определения кратности ошибки по ее синдрому, установлена связь между предлагаемой методикой и методом определителей Блейхута нахождения веса ошибки БЧХ-кода на основании ее синдрома.

КЛАССИФИКАЦИЯ DDOS-АТАК В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

В.В. Маликов, И.И. Лившиц

В настоящее время DDoS-атаки получили широкое распространение среди киберпреступников как один из эффективных и экономически доступных инструментов, позволяющих удаленно нарушить режим устойчивого функционирования сетевого сервиса/ресурса за счет эксплуатации уязвимостей, направленных на исчерпание пропускной способности каналов связи и/или вычислительной емкости атакуемого объекта.

Авторами на основе данных из открытых источников проведен анализ методов/технологий проведения DDoS-атак и предложена классификация таких атак с привязкой к уровням модели OSI. Дополнительно предложена классификация DDoS-атак по уровню сложности их технической реализации, учитывающая количественные параметры: векторов атаки, хостов атаки, скорости атаки, времени атаки, использования метода усиления (амплификатора).

По результатам проведенного анализа методов/технологий, используемых для проведения DDoS-атак, можно сделать следующие выводы:

1. Как правило, в качестве основного ресурса для проведения DDoS-атак злоумышленниками используются ранее атакованные и зараженные вредоносным кодом устройства/системы легитимных пользователей, которые потом объединяются в управляемые бот-сети. При этом показатели

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.