Итоговые оценки расчета метрик ИБ позволяют оценить общий уровень результативности СМИБ и, соответственно, оценить текущий уровень защищенности информации — в текущей «конфигурации» СМИБ («scope»). Эти оценки должны послужить целям, во-первых, предоставления высшему менеджменту, как лицам, принимающим решения, достаточных доказательств о выборе оптимального состава средств (мер) обеспечения ИБ, и, во-вторых, предложить специалистам, обеспечивающим безопасность ТКС, численные метрики оценки результативности как отдельных реализованных средств (мер) ИБ, так и совокупно – всей СМИБ.

ИССЛЕДОВАНИЕ СТРУКТУРЫ APT-АТАК НА КРЕДИТНО-ФИНАНСОВЫЕ УЧРЕЖДЕНИЯ

В.В. Маликов, А.Д. Кушнеров, М.П. Филенков

Главными целями реализации APT-атак (Advanced Persistent Threat — целевые продолжительные атаки повышенной сложности) на кредитно-финансовые учреждения (КФУ) со стороны злоумышленников являются получение персональных финансовых данных и денежных средств.

Наибольший ущерб КФУ в 2014 г. нанесла группировка Carbanak, реализовавшая специфическую APT-атаку. Основной целью APT-атаки было проникновение в сеть КФУ и поиск критически важной системы информатизации, с помощью которой из организации можно вывести денежные средства.

Алгоритм реализации APT-атаки Carbanak (основан на коде Carberp):

1) фишинговая рассылка (вредоносное вложение: CPL-файл, документ Word);

2) установка кода Carbanak на ПЭВМ сотрудника КФУ;

3) сетевой взлом ПЭВМ администратора КФУ и других ПЭВМ;

4) gроведение финансовой разведки (видеозапись действий оператора, перехват клавиатурного кода и др.);

5) преступный вывод денежных средств:

6) удаленная команда банкоматам на выдачу наличных денежных средств подставным лицам («дропам»);

– перевод денежных средств на счета киберпреступников через сеть SWIFT;

– изменения баз данных с информацией о счетах, позволяющие создать фальшивые счета с высоким балансом, с последующим выводом денежных средств.

ЗАЩИТА ДАННЫХ В СИСТЕМАХ МОНИТОРИНГА ОЧАГОВ ХИМИЧЕСКОГО ПОРАЖЕНИЯ

Е.В. Новиков, Д.А. Мельниченко

Мониторинг состояния очагов поражения, возникающих в чрезвычайных ситуациях с выбросом ядовитых веществ, наиболее эффективно может осуществляться с применением распределенных автоматизированных систем сбора данных. Такие распределенные системы сбора данных, обеспечивающие быстрое развертывание в очаге поражении, строятся на базе технологий беспроводной связи.

Одним из наиболее перспективных является стандарт беспроводной связи ZigBee, ориентированный на построение локальных систем управления и сбора данных. ZigBee за счет ретрансляции обеспечивает достаточно большую зону покрытия с сохранением низкого энергопотребления (Расстояния между узлами сети до сотен метров на открытом пространстве).

Одним из важнейших факторов, которые следует учитывать при построении сети мониторинга, является защита данных, так как развертываемые сети остаются физически доступными для внешних воздействий.

Спецификации поддерживают шифрование данных при помощи симметричных ключей на сетевом уровне, а также механизм дополнительного шифрования на уровне

приложения. Основа безопасности сетей мониторинга — центр управления безопасностью, который на этапе конфигурирования сети управляет подключением устройств, а также обеспечивает обновление в процессе сбора данных ключей сети.

В сетях ZigBee предусмотрено три типа ключей для управления безопасностью. Первоначальный главный ключ должен быть получен через безопасную среду (передачей или предварительной установкой), так как безопасность всей сети зависит от него. Он не используется для шифрования и применяется как разделяемый двумя устройствами секретный код при выполнении устройствами процедуры генерации ключа канала связи. Сетевые ключи обеспечивают безопасность сетевого уровня, и такой ключ имеет каждое устройство в сети ZigBee. По беспроводным каналам сетевые ключи должны пересылаться только в зашифрованном виде. Ключи каналов связи обеспечивают безопасную одноадресную передачу сообщений между двумя устройствами на уровне приложений.

НЕЛИНЕЙНЫЕ МНОЖЕСТВА КОДОВЫХ СЛОВ

А.И. Митюхин, Р.П. Гришель

В специальных системах одним из основных требованием является структурная защита информации от несанкционированного доступа к ней. Определенная степень структурной защиты обеспечивается при использовании сравнительно большого, меняющегося со временем, ортогональных и биортогональных последовательностей с кодовым расстоянием $d=n/2$, где n — длина кода.[1]. В работе рассматривается нелинейная кодовая конструкция. Она позволяет создать усеченное нелинейное множество последовательностей вида $a=(a_1, a_2, \ldots, a_{2l})$, а $\in 1, -1$, l —нечетные числа с $d'>d$. Все множество образуется диадными перестановками образующей последовательности, получаемой мажоритарным суммированием ортогональных функций Радемахера с кратным периодом. Приводятся результаты численного исследования корреляционных спектров последовательностей. Выяснено, что математическое ожидание и дисперсия корреляционных выбросов зависит от длины последовательностей. Исследовалась усеченная нелинейная кодовая конструкция кода длиной $n=32$ с минимальным расстоянием Хэмминга $d=12$ на множестве с явно выраженными спектральными компонентами. Корректирующая способность кода $t=5$. На основе анализа спектральной и структурной регулярности корреляционных спектров мажоритарных последовательностей удалось сформировать конструкции из 120 множеств нелинейных последовательностей, состоящих из четырех слов с расстоянием $d=20$.

Литература

1. *Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А.* Теория кодов, исправляющих ошибки: пер. с англ. М., 1979.

ЗАЩИТА КОРПОРАТИВНЫХ СЕТЕЙ СВЯЗИ ОТ ВНЕШНИХ АТАК

Н.А. Павлов

Одной из самых актуальных задач в сфере услуг предоставления информации является борьба с DDoS-атаками.

Для повышения качества фильтрации трафика в корпоративной сети компании от нежелательной нагрузки был разработан модуль обработки внешних запросов и внедрена система автоматического обнаружения DDoS атак в телекоммуникационной корпоративной сети и усовершенствованы алгоритмы фильтрации.

Данный модуль представляет собой защиту от DDoS атак методом HTTP флуда посредством внедрения специализированного программного кода в тело сайта, которое будет отвечать на первоначальные атаки. Данный модуль работает как быстрый фильтр между ботами и бэкэндом во время L7 DDoS атаки и позволяет отсеивать мусорные запросы, при высоких нагрузках будет передавать защиту как эстафетную палочку на следующий уровень защиты.