исследованиями в этой области. Интерес представляют поисковые технологии, методы и технологии ведения аналитической разведки, методики анализа и синтеза найденной фактографической информации (текст, рисунки, видео), технологии мониторинга Интернета и социальных сетей. Всесторонне исследуется специализированное ПО, часто называемое процессорами сбора и анализа данных, позволяющее извлекать, верифицировать и анализировать оперативную информацию из сети Интернет (в контексте поставленной задачи/цели). Особый интерес представляют системы, позволяющие получить доступ к информационно-аналитическим системам, в свою очередь занимающимся сбором и анализом информации («робот роботов»). Систематизируется и развивается современный инструментарий для работы с ресурсами как видимого, так и невидимого Интернета.

О ВЫБОРЕ ПРЕДСТАВИТЕЛЕЙ ОРБИТ ПРИ КЛАССИФИКАЦИИ ТОЧЕЧНЫХ ОБРАЗОВ

В.А. Липницкий, Н.В. Спичекова

Обобщением ряда конкретных задач, возникающих при распознавании образов в медицине, биологии, радиолокации и других областях человеческой деятельности, является задача описания образов, возникающих на экране, состоящем из n^2 пикселей, при «вспыхивании» n точек. Данная задача эквивалентна задаче описания классов эквивалентностей (орбит), на которые разбивается множество P_n квадратных (0,1)-матриц порядка n с n единицами под действием квадрата симметрической группы S_n, переставляющей строки (столбцы) матриц из P_n.

При создании библиотеки орбит множества P_n для фиксированного n возникает проблема выбора характерного представителя каждой орбиты. С учетом физической природы исходной задачи естественным представляется использование геометрического подхода, суть которого заключается в выборе в качестве представителя орбиты матрицы, которой соответствует однозначно идентифицируемый геометрический образ. На практике использование данного подхода сопряжено со значительными трудностями, обусловленными сложностью визуального анализа большого количества образов. Так, уже при n=8 среди 558 орбит множества P_n имеется несколько орбит мощности 67 737 600.

Имеется ряд весомых аргументов в пользу того, что в качестве канонического представителя фиксированной орбиты множества P_n можно использовать ту матрицу, для которой одномерный вектор, построенный из строк этой матрицы, лексикографически старше такого же вектора, построенного для любой другой матрицы этой же орбиты.

АКТУАЛЬНЫЕ ВОПРОСЫ ОЦЕНКИ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

В.В. Маликов, И.И. Лившиц, С.А. Чурюканов

Для обеспечения безопасности информации требуется периодически оценивать состояние защищенности информации, при котором обеспечивается ее конфиденциальность, доступность и целостность. Указанная проблема имеет несколько возможных вариантов для эффективного решения, из которых наиболее современным, универсальным и практически применимым считаются системы менеджмента информационной безопасности (СМИБ) и выполнение оценки защищенности посредством оценки результативности.

Авторами предложен методический подход к оценке защищенности информации в телекоммуникационных системах (ТКС) на основе анализа их доступности. Реализация данного подхода основывается на применении СМИБ, комплекс требований к которой затрагивает обеспечение всей «триады безопасности», в том числе – доступности. Измерение параметров результативности СМИБ предполагает применение метрик информационной безопасности (ИБ), которые позволяют, в том числе, учесть фактические данные доступности в конкретной ТКС при периодической оценке (например, при выполнении аудитов ИБ).

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