источника уникальности. Для обеспечения стабильности ответов ФНФ используется мажоритарный выбор из серии последовательных результатов на одном запросе, для уникальности — серия на разных запросах.

Предлагается мультиарбитральная ФНФ, содержащая схему арбитра на каждом звене конфигурируемых путей, которая теоретически обладает большей достоверностью и уникальностью, по сравнению с классической реализацией АФНФ на ПЛИС. Открытой остается проблема формирования множеств входных запросов для генерации уникальных, стабильных ответов.

Литература

1. *Plaga R., Merli D.* // Proc. CS2 15 Proceedings of the Second Workshop on Cryptography and Security in Computing Systems, Amsterdam, 2015, ACM Digital Library.

РАСЧЕТ ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИНФОРМАЦИИ В СЕТЯХ PON

В.И. Кириллов, Е.А. Коврига

При проведении расчетов считаем известными на основе экспертных оценок [1]: стоимость организации защитных мер (контроля соблюдения прав доступа d_1, у.е.; оснащения линий PON техническими средствами d_2, у.е.; оснащения сети измерительными средствами d_3, у.е.; криптографической защиты d_4, у.е.); потенциальную величину ущерба при выполнении каждой возможной угрозы (нарушение конфиденциальности u_1, у.е.; доступности u_2, у.е.; достоверности u_3, у.е.); вероятность перехода злоумышленника к следующему этапу сценария атаки либо к осуществлению самой угрозы при несоблюдении прав доступа p_1; отсутствии технических средств защиты p_2; измерительных средств защиты p_3; криптографических средств защиты p_4.

Определим вероятную стоимость величины ущерба u, ед. из следующего выражения: $u = u_1 p_1 p_2 p_3 + u_2 p_1 p_2 p_3 + u_3 p_1 p_2 p_4$, где первое, второе и третье слагаемые есть не что иное, как вероятные стоимости величины ущерба из-за успешного нарушения конфиденциальности, доступности и достоверности соответственно [2]. Тогда вероятная стоимость защитных средств d, ед.: $d = (d_1 + d_2 + d_3) \cdot (1 - p_1 \cdot p_2 \cdot p_3) + (d_1 + d_2 + d_3) \cdot (1 - p_1 \cdot p_2 \cdot p_3) + (d_1 + d_2 + d_4) \cdot (1 - p_1 \cdot p_2 \cdot p_4)$ [2].

О целесообразности системы защиты можно говорить, если вероятная стоимость величины ущерба превышает вероятную стоимость защитных средств ($u > d$) [1].

Литература

1. *Кириллов В.И., Коврига Е.А.* // Информационные технологии и системы: Материалы. Межд. науч. конф. БГУИР, Минск 23 окт. 2013. С. 46–47.

2. *Кириллов В.И., Коврига Е.А.* // Веснік сувязі, 2014. № 2. С. 38–43.

ИНТЕРНЕТ-РАЗВЕДКА: ВОЗМОЖНОСТИ, МЕТОДИКИ, ИНСТРУМЕНТЫ

Е.Н. Ливак

Аналитическая Интернет-разведка (конкурентная разведка в Интернет, бизнес-разведка средствами Интернет) сегодня — это не только прерогатива правоохранительных органов и спецслужб, но также и направление деятельности современных подразделений безопасности коммерческих компаний и государственных организаций, и прибыльный бизнес компаний, специализирующихся на информационном анализе.

Бизнес-разведка на основе анализа ресурсов Интернет становится все более востребованной и в Беларуси. Технологии своевременного выявления угроз и недобросовестных сотрудников, методы слежения за конкурентами позволяют обеспечить корпоративную безопасность, принимать верные управленческие решения и не упускать возможности, противостоять корпоративным войнам в Интернет.

Сотрудники и студенты кафедры системного программирования и компьютерной безопасности Гродненского государственного университета имени Янки Купалы занимаются

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).