Таким образом, для проработки концепции будущей системы интерактивной визуализации было разработано приложение-прототип, которое моделирует мультипланарную систему на одном статоре, которое включает в себя интерактивную составляющую — пользовательский интерфейс, позволяющий задать траекторию движения для каждого позиционера в трехмерном пространстве и обрабатывающий коллизии позиционеров между собой.

Литература

1. *Samuel R. Buss.* 3D Computer Graphics: A Mathematical Introduction with OpenGL. Cambridge University Press, 2003.

СРЕДСТВА И АЛГОРИТМЫ КОМПЬЮТЕРНО-ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ ГРАФИЧЕСКИХ ИЗОБРАЖЕНИЙ

А.Д. Зайков, А.М. Кадан

В докладе представлен опыт работы с современным специализированным программным обеспечением для проведения компьютерно-технических экспертиз (КТЭ) при решении задач поиска и закрепления доказательств в сфере мультимедийного контента и графической информации.

Рассмотрены задачи КТЭ, включающие изучение следующих вопросов: о наличии на исследуемых объектах информации, относящейся к делу (в том числе, в неявном, удалённом, скрытом или зашифрованном виде); о возможности (пригодности) использования исследуемых объектов для определённых целей; о действиях, совершённых с использованием объектов; об идентификации найденных документов, мультимедийной информации, программ.

Выполнен сравнительный анализ возможностей и применения современных специализированных программных систем эксперта, поддерживающих всю технологическую цепочку проведения КТЭ: EnCase, AsccessData Forensic Toolkit, Defacto AccessData, Password Recovery Toolkit, Adroit Photo Forensics, Amped Authenticate. Инструментами Image Error Level Analysis выполнена экспертная оценка графической информации. В результате работы выявлено и доказано наличие «дорисованных» областей на анализируемой базе изображений, а также отмечены документы с редактированием злоумышленником и вставленными новыми областями в ряд доказательных фотографий. Программное обеспечение позволило эффективно определить даже самые мелкие неоригинальные детали в графической информации, которые практически невозможно увидеть невооруженным глазом.

Определен класс задач, которые требуют разработки специальных алгоритмов, не реализованных существующими программными средствами и пути их решения.

МУЛЬТИАРБИТРАЛЬНАЯ ФИЗИЧЕСКИ НЕКЛОНИРУЕМАЯ ФУНКЦИЯ ДЛЯ ПЛИС

В.П. Клыбик, А.А. Иванюк

ФНФ (от англ. PUF — Physically Unclonable Function) эффективны для неклонируемой идентификации и аутентификации цифровых устройств на ПЛИС — программируемых логических интегральных схемах. Цифровые ФНФ основаны на отклонениях в задержках распространения сигналов по путям, обусловленных незначительными девиациями в физической структуре при изготовлении ПЛИС. Для измерения отклонений в задержках распространения сигналов применяется множество типов ФНФ, в частности ФНФ типа арбитр (АФНФ).

Проблемами реализации АФНФ на ПЛИС являются обеспечение симметричности путей распространения сигнала и стабильности ответов, обусловленные заведомой асимметрией конфигурируемых ресурсов ПЛИС. Для решения описанных проблем используются следующие подходы: пространственная локализация критичных доменов в одном структурном блоке ПЛИС; введение в схемы путей сигналов элементов конфигурируемой задержки; использование состояния метастабильности арбитра в качестве

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