возможности когнитивной компьютерной графики

Задача когнитивного анализа многомерных данных формулируется как поиск наиболее подходящей содержательной интерпретации, которую может обеспечить их визуальное представление в пространстве обобщенных признаков (факторов риска).

Предложена методика структурирования экспериментальных данных, включающая многомерный анализ, выявление когнитивных паттернов и их содержательную интерпретацию в терминах опасных событий и рисков.

1. *Зенкин А. А*. Когнитивная компьютерная графика. М.: Наука, 1991. – 192 с.
2. *Зиновьев А. Ю.* Визуализация многомерных данных. Красноярск: ИПЦ КГТУ, 2000. – 168 с.
3. *Боровиков В.* STATISTIKA. Искусство анализа данных на компьютере: Для профессионалов. – СПб.: Питер, 2003. – 688 с.
4. *Сердюцкая Л.Ф., Каменева И.П.* Системный анализ и математическое моделирование медико-экологических последствий аварии на ЧАЭС и других техногенных воздействий. – К.: «Медэкол», 2000. – 173 с.
5. *Шмелев А.Г.* Введение в экспериментальную психосемантику: теоретико-методологические основания и психодиагностические возможности. М.: Изд-во МГУ, 1983. – 158 с.
6. *Большаков А.М., Крутько В.Н., Пуцилло Е.В.* Оценка и управление рисками влияния окружающей среды на здоровье населения. – М.: Эдиториал УРСС, 1999. – 256 с.
7. *Каменева І. П.* Просторово-семантичні моделі репрезентації знань в геоекологічних дослідженнях // Геоінформатика. – 2005. – № 4. – С. 64 – 69.

Поступила 8.02.2010р.

УДК 004.056:004.274

Ю.М. Коростиль, А.Н. Давиденко, С.Я. Гильгурт, М.М. Панченко

АНАЛИЗ УГРОЗ И ОПАСНОСТЕЙ В КОМПЬЮТЕРНЫХ СИСТЕМАХ НА ПРЕДМЕТ ЗАЩИТЫ ЦИФРОВЫМИ РЕКОНФИГУРИРУЕМЫМИ УСТРОЙСТВАМИ

The utilization of the programmable logic for the computer security problems is investigated. A classification of threats and vulnerabilities in computer systems taking into account the potential of FPGA-based digital equipment when using for solving security tasks is proposed.

Реконфигурируемые вычисления, основанные на применении программируемых логических интегральных схем (ПЛИС), которые позволяют совместить быстродействие специализированных аппаратных решений с

гибкостью универсальных процессоров, в настоящее время находят все более широкое распространение, в том числе, в области информационной безопасности [1, 2].

Для того, чтобы задействовать высокий потенциал и последние достижения программируемой логики для решения задач защиты информации наиболее результативно, необходимо провести глубокий и максимально полный анализ проблем, существующих в данной области. В частности, необходимо исследовать угрозы и опасности, существующие в автоматизированных системах (АС) различного уровня, имея в виду возможности применения цифровых устройств на базе ПЛИС.

В работе [3] была предпринята попытка подойти к проблеме со стороны анализа уже существующих методов и средств обеспечения компьютерной безопасности и проанализировать, какие из них могут быть реализованы на реконфигурируемых вычислителях. Однако, для получения более полных и строгих в научном смысле выводов, данные вопросы требуют серьезного исследования, основанного на более формализованных подходах.

Настоящая статья является первой в ряде публикаций, посвященных исследованию проблем информационной безопасности, конечным практическим результатом которого является создание класса недорогих и эффективных, пригодных для массового применения средств защиты на базе программируемой логики.

Для получения максимально полных сведений в исследуемой области, в первую очередь необходим глубокий, системный и разносторонний анализ угроз и опасностей, существующих в информационных системах. Кроме того, наблюдаемая в настоящее время тенденция возрастания проблем в области информационной безопасности, делает актуальной задачу предсказания новых, потенциально возможных в будущем рисков и угроз.

Анализ последних достижений и публикаций по данной теме [4 – 8] показывает, что, несмотря на наличие большого количества разнообразных перечней, классификаций угроз и опасностей, невозможно выбрать достаточно полную, детальную и непротиворечивую разработку, подходящую для решения сформулированной выше задачи. С другой стороны, многочисленные работы по применению реконфигурируемых устройств ориентированы, в подавляющем большинстве случаев, на решение конкретных задач, либо классов задач в области защиты информации. Полноценных исследований, посвященных целенаправленному и максимально полному анализу возможностей программируемой логики в данной области, на сегодняшний день проводится недостаточно.

Целью настоящей статьи является подробный анализ известных источников и формирование на его основе максимально полной классификации существующих и потенциально возможных угроз и опасностей в компьютеризированных системах, имея в виду применение в качестве средств защиты цифровых реконфигурируемых устройств на базе ПЛИС.

В данной работе и последующих публикациях авторов по данной теме

будет использоваться следующая терминология:

Угроза – возможная опасность (потенциальная или реально существующая) совершения какого-либо деяния (действия или бездействия), направленного против объекта защиты (информационных ресурсов), наносящего ущерб.

Уязвимость – присущие объекту информатизации причины, приводящие к нарушению безопасности информации на конкретном объекте и обусловленные недостатками процесса функционирования объекта информатизации, свойствами архитектуры автоматизированной системы, протоколами обмена и интерфейсами, применяемыми программным обеспечением и аппаратной платформой, условиями эксплуатации.

Атака – реализация угрозы источником угрозы через имеющиеся уязвимости.

Принципы построения искомой классификации угроз обусловливает конечная цель данной работы – максимально полное исследование возможностей создания на базе реконфигурируемых устройств средств информационной безопасности, в том числе для задач, для решения которых ранее данные подходы не применялись. Поэтому необходимо:

- обеспечить как можно более полный учет всех возможных источников угроз;
- идентифицировать и сопоставить с источниками угроз все возможные уязвимости объектов защиты;
- всем идентифицированным источникам и уязвимостям сопоставить угрозы информационной безопасности.

В рассмотренной ниже классификации угроз и уязвимостей информационных систем при перечислении одноуровневых пунктов порядок следования выбирался по принципу от простого к сложному.

На высшем уровне иерархии все угрозы информационной безопасности *по характеру* можно разделить на (рис. 1):

1. Технические;
2. Организационные.

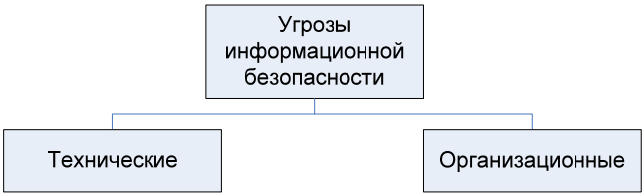

Рис.1. Верхний уровень иерархии угроз информационной безопасности

Следует заметить, что организационные угрозы в большей степени зависят от человеческого фактора, в связи с чем вопросы противодействия в

этом случае сложнее организовать техническими средствами, к которым относятся и реконфигурируемые устройства. Тем не менее, высокий потенциал программируемой логики позволяет существенно повысить интеллектуальные возможности создаваемых на их основе систем компьютерной безопасности. По этой причине в предлагаемую классификацию включены оба вида угроз.

Технические угрозы информационной безопасности *по виду* воздействия делятся на (рис. 2):

1.1. Физические;
1.2. Логические (программные).

Физические угрозы менее многочисленные и более простые в плане противодействия техническими средствами по сравнению с логическими. В зависимости *от источника* они подразделяются на:

1.1.1. Отказ оборудования и систем жизнеобеспечения;
1.1.2. Действия нарушителя;
1.1.3. Форс-мажорные обстоятельства.

Каждая из вышеупомянутых групп *по целенаправленности* воздействия подразделяется на:

1.1.1.1., 1.1.2.1., 1.1.3.1. Угрозы ресурсам;
1.1.1.2., 1.1.2.2., 1.1.3.2. Угрозы каналам связи.

Группа логических (программных) угроз представляет наибольший интерес в плане организации защиты, так как требует оценки действия субъекта и прогнозирования его поведения для принятия адекватных мер.

Логические (программные) угрозы в зависимости *от источника* подразделяются на:

1.2.1. Локальные (исходящие от внутренних нарушителей);
1.2.2. Удаленные (исходящие от внешних нарушителей).

Деление нарушителей на внутренних и внешних обусловлено тем, что для одной и той же угрозы требуются разные методы парирования в зависимости от их источника.

Внутренними нарушителями обычно являются квалифицированные специалисты, знакомые со спецификой решаемых задач, структурой, основными функциями и принципами работы средств защиты информации, имеющие возможность использования штатного оборудования и технических средств. К ним относятся:

- представители службы защиты информации;
- основной персонал (пользователи, программисты, разработчики);
- технический персонал (жизнеобеспечение, эксплуатация);
- вспомогательный персонал (уборщики, охрана).

Локальные угрозы *по целенаправленности* воздействия могут инициировать:

1.2.1.1. Угрозы ресурсам.

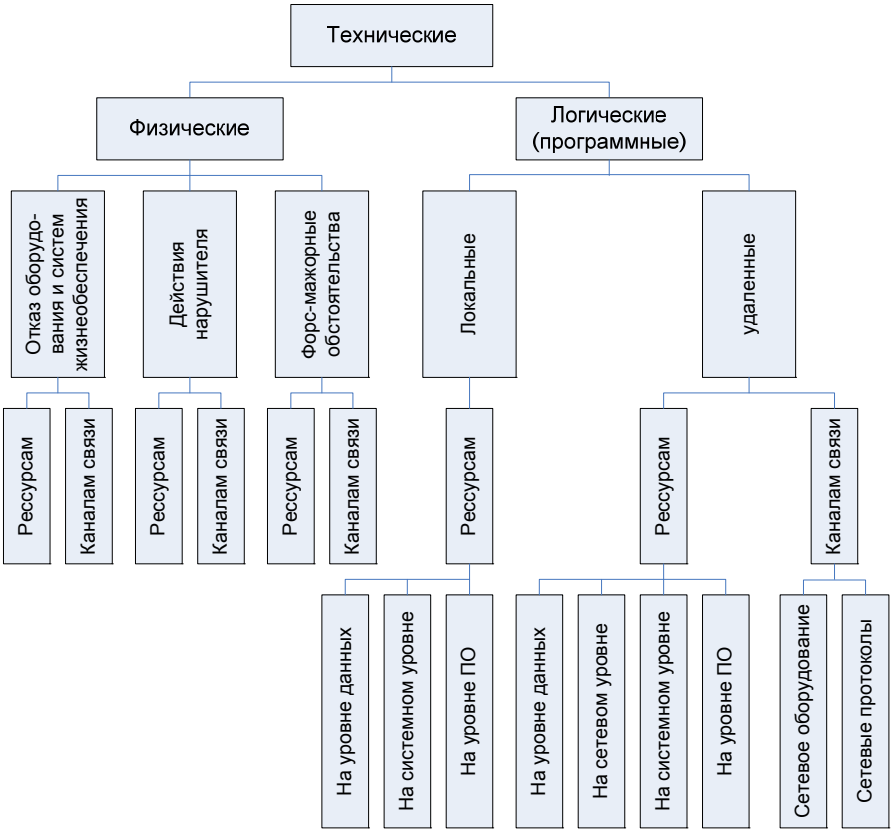

Рис.2. Технические угрозы информационной безопасности

Программные угрозы ресурсам от локального нарушителя *по воздействию* подразделяются на угрозы:

1.2.1.1.1. На уровне данных;
1.2.1.1.2. На системном уровне;
1.2.1.1.3. На уровне программного обеспечения.

Внешних нарушителей отличает большее разнообразие в квалификации и степени владения информационными технологиями. В общем случае их возможности более ограничены по сравнению с внутренними. С другой

стороны, сфера их воздействия несколько шире.

Угрозы от удаленных нарушителей *по целенаправленности* воздействия могут представлять собой:

1.2.2.1. Угрозы ресурсам.
1.2.2.2. Угрозы каналам связи.

Программные угрозы ресурсам от удаленного нарушителя *по воздействию* подразделяются на угрозы:

1.2.2.1.1. На уровне данных;
1.2.2.1.2. На сетевом уровне;
1.2.2.1.3. На системном уровне;
1.2.2.1.4. На уровне программного обеспечения.

Программные угрозы каналам связи от удаленного нарушителя *по воздействию* подразделяются на угрозы:

1.2.2.2.1. Сетевое оборудование;
1.2.2.2.2. Сетевые протоколы.

Организационные угрозы *по направленности воздействия* бывают (рис. 3):

2.1. Действиями персонала;
2.2. Воздействием на персонал.

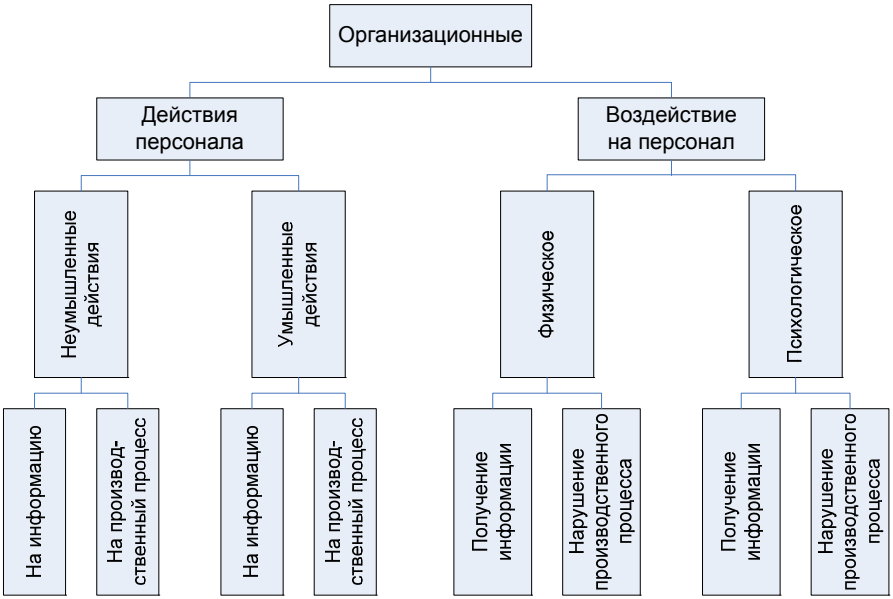

Рис.3. Организационные угрозы информационной безопасности

Причиной угроз, исходящих от персонала, в зависимости от *осознанности* могут быть:

2.1.1. Неумышленные действия.
2.1.2. Умышленные действия;

Угрозы, вызванные как неумышленными, так и умышленными действиями персонала, могут быть направлены:

2.1.1.1., 2.1.2.1. На информацию;
2.1.1.2., 2.1.2.2. На производственный процесс.

Воздействие на персонал *по типу* разделяют на:

2.2.1. Физическое;
2.2.2. Психологическое.

Как физическое, так и психологическое воздействие на персонал может оказываться с целью:

2.2.1.1., 2.2.2.1. Получения информации;
2.2.1.2., 2.2.2.2. Нарушения производственного процесса.

Выводы по результатам настоящего исследования могут быть сформулированы следующим образом.

Реконфигурируемые цифровые устройства на базе современных микросхем ПЛИС позволяют создавать недорогие эффективные средства защиты информации в компьютеризированных системах различного уровня.

Проведенный в данной работе анализ существующих угроз и опасностей, а также предложенная на его основе классификация позволят наиболее полно задействовать возможности программируемой логики для решения задач информационной безопасности.

Высокая гибкость реконфигурируемых устройств позволяет создавать интеллектуальные системы противодействия не только известным, но и потенциально возможным угрозам.

1. Реконфигурируемые вычислительные системы: Основы и приложения. / *А.В. Палагин, В.Н. Опанасенко.* – К.: «Просвіта», 2006. – 280 с.
2. *Гильгурт С.Я.* Обзор современных реконфигурируемых унифицированных вычислителей // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ НАН України. – Вип. 49. – Київ: 2008. – С. 17–24.
3. *Гильгурт С.Я., Гиранова А.К.* О применении реконфигурируемых вычислителей для решения задач защиты информации // Зб. наук. праць ІПМЕ НАН України. – Київ, 2008. – Вип. 46. – С. 93–99.
4. *Amoroso E.G.* Fundamentals of Computer Security Technology. – NJ: Prentice Hall PTR, 1994. – 404 p.
5. *Лукацкий А.В.* Обнаружение атак. – СПб.: БХВ-Петербург, 2001. – 624 с.
6. *Коул Э.* Руководство по защите от хакеров: Пер с англ. – М.: Издательский дом "Вильямс", 2002. – 640 с.

7. Методи захисту банківської інформації: Навчальний посібник. / В.К. Задірака, О.С. Олексюк, М.О. Недашковський. – К.: Вища шк., 1999. – 261 с.
8. *Куканова Н.Ю.* Описание классификации угроз DSECCT // Научно-технический вестник СПбГУ ИТМО. – СПб., 2006. – Вып. 29. – С. 175–178

Поступила 1.02.2010р.

УДК 65.012.123.001.26:575(045)

Т.І. Олешко, Н.В.Ратушна

ОПТИМІЗАЦІЯ БАГАТОПАРАМЕТРИЧНИХ ФУНКЦІЙ ЗА ДОПОМОГОЮ ГЕНЕТИЧНИХ АЛГОРИТМІВ

Генетичні алгоритми є важливою складовою еволюційних методів. У світі спостерігається бум розвитку генетичних алгоритмів. Відбулись десятки міжнародних конференцій, опублікована величезна кількість літератури по генетичних алгоритмах, і інтерес до цієї тематики постійно зростає.

Генетичні алгоритми – це процедури пошуку, засновані на механізмі природного відбору і наслідування. Вони відрізняються від інших оптимізуючих і пошукових процедур такими ознаками [1]:

- обробляють не значення параметрів самої задачі, а їх закодовану форму;
- здійснюють пошук рішень, враховуючи не одиничну точку, а їх деяку популяцію;
- використовують тільки цільову функцію, а не іншу додаткову інформацію;
- використовують ймовірність, а не детерміновані правила вибору;
- у процесі еволюції кожна нова популяція залежить тільки від попередньої.

Генетичні алгоритми застосовуються до вирішення багатьох наукових і технічних проблем. Проте, можливо найпопулярніше застосування генетичних алгоритмів – оптимізація багатопараметричних функцій. Багато задач можуть бути сформульовані як пошук оптимального значення, де значення – складна функція, що залежить від певних вхідних параметрів. У деяких випадках потрібно знайти ті значення параметрів, при яких досягається найкраще значення функції. В інших випадках глобальний екстремум не потрібний – рішенням може вважатися будь-яке значення, краще за певну задану величину. У цьому випадку генетичні алгоритми – часто найкращий метод для пошуку "прийнятних" значень. Особливість генетичного алгоритму полягає в його здатності маніпулювати одночасно багатьма параметрами.

Тому не дивно, що вчені звернулися до теорії еволюції в пошуках

