для отвода тепла и охлаждения, в частности, в ноутбуках. Принцип работы ТТ аналогичен принципу работы термосифона (ТС). Однако ТТ имеет капиллярную структуру, в отличие от ТС. И поэтому работа по охлаждению объекта может происходить в любых положениях ТТ, так как конденсат возвращается в зону поглощения тепла под действием капиллярных сил. К тому же, ТТ имеют ряд преимуществ, таких как: автономность и надежность, столь важные для защиты информации, а также эффективность, бесшумность и компактность. Для увеличения площади контакта ТТ с сервером конструктивно лучше использовать ТТ с квадратным либо прямоугольным сечениями. Все выше перечисленное приводит к концепции расположения сервера на поверхности ТТ. Для проведения исследований изготовлены: экспериментальный ТС и два конструктивно отличающихся друг от друга рабочих радиатора. На основании экспериментальных данных рассчитаны: эффективный коэффициент теплопроводности и термическое сопротивление ТС, что подтверждает правильность выбора ТТ в качестве нового охладительного элемента для оборудования в ЦОД.

ВВЕДЕНИЕ ДИСКРЕТНЫХ ХАОТИЧЕСКИХ ОТОБРАЖЕНИЙ ПРИ ФОРМИРОВАНИИ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ

А.В. Сидоренко, И.В. Шакинко

На современном этапе развития информационных технологий большинство веб-приложений и интернет-ресурсов обеспечивают передачу изображений. Возникает необходимость в решении задач связанных с защитой цифровых изображений из-за невозможности обеспечения требуемых уровней безопасности передаваемой информации в телекоммуникационных каналах [1]. Для этих целей традиционно используется подход, получивший название цифровые водяные знаки (ЦВЗ). Это специальные метки, встроенные в изображение (или другие цифровые данные) для обеспечения контроля его применения [2].

В данной работе приводятся результаты анализа разработанного алгоритма формирования, встраивания и извлечения ЦВЗ. ЦВЗ формируются при использовании следующих хаотических отображений: логистического, тент-отображения и отображения Бернулли.

Установлено, что ЦВЗ, формируемые на основе различных хаотических отображений, при встраивание в изображение практически не меняют его статистические характеристики.

Результаты тестирования предлагаемого алгоритма свидетельствуют о том, что данный алгоритм является стойким к атакам копирования. При использовании алгоритма допустимы потери фрагмента изображений, а также наличие шумов в канале передачи. При этом в последнем случае возможны изменения более 10 % элементов изображения.

Варьируя пороговым значением уровня шума, изменяя размеры блоков изображения становится возможным различать искажения и модификацию областей изображения, произведенных злоумышленником.

Литература

1. Robust Image Watermarking Theories and Techniques: A Review / H. Tao [et al.] // Journal of Applied Research and Technology. 2014. Vol. 12. P. 122–138.

2. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. М.: Солон-Пресс, 2002 . С. 5.

ОБЗОР МЕТОДОВ ДЛЯ ПОИСКА УЯЗВИМОСТЕЙ В ПРОГРАММНОМ ОБЕСПЕЧЕНИИ

В.О. Сидорович, А.Е. Варюшина

Провал или успех наших повседневных дел в той или иной степени определяется корректностью функционирования программного обеспечения (ПО), что ставит современное общество в зависимость от уязвимостей в ПО[1].

Уязвимости ПО – критические ошибки, не выявленные в ходе тестирования и не декларированные спецификацией разработчика или заложенные преднамеренно, предоставляющие злоумышленникам исключительные возможности по разглашению

информации, ее модификации, блокированию использования и безостаточному уничтожению без возможности восстановления.

Возможность изменения основных свойств защищенности (доступность, целостность, конфиденциальность) информационных ресурсов и дестабилизации процессов функционирования информационно-вычислительных систем различного назначения посредством применения злоумышленниками несанкционированных воздействий деструктивного характера (атак) на уязвимости ПО предопределяют острую потребность в своевременном обнаружении уязвимостей на этапах разработки и проектирования ПО, проверки соответствия их заявленной политики безопасности и реализации механизмов защиты [2].

При статическом анализе можно обнаружить уязвимости кода даже до того, как код будет готов для запуска. С другой стороны, динамический анализ происходит на работающем программном обеспечении и обнаруживает уязвимости по мере их возникновения, обычно используя сложные инструментальные средства. Кто-то может возразить, что одна форма анализа предваряет другую, но разработчики могут комбинировать оба способа для ускорения процессов разработки и тестирования, а также для повышения качества выдаваемого продукта [3].

Литература

1. Истинная цена программных ошибок [Электронный ресурс]. URL: https://www.osp.ru/os/2009/03/8158133/ (дата обращения: 30.04.2018).

2. Технологии статического и динамического анализа уязвимостей программного обеспечения [Электронный ресурс]. URL: http://cyberrus.com/wp-content/uploads/2014/11/vkb_04_04.pdf (дата обращения: 30.04.2018).

3. Использование статического и динамического анализа для повышения качества продукции и эффективности разработки [Электронный ресурс]. URL: http://www.swd.ru/print.php3?pid=828/ (дата обращения: 30.04.2018).

ЭЛЕКТРОННЫЕ СВОЙСТВА ФОСФОРЕНА, ЛЕГИРОВАННОГО АЗОТОМ

В.А. Скачкова, М.С. Баранова, Д.Ч. Гвоздовский

Последнее десятилетие, важное место в микро- и наноэлектронике занимают двумерные материалы, такие как графен, силицен, германен, гексагональный BN, дихалькогениды переходных металлов и др., благодаря их выдающимся свойствам. Монослой черного фосфора (фосфорен), представляет собой перспективный 2D-материал, который, в отличие от графена, является прямозонным полупроводником с запрещенной зоной, равной ~ 0,3–2 эВ, в зависимости от количества слоев в структуре [1]. Из-за своей «сморщенной» структуры фосфорен обладает сильной анизотропией электронных и оптических свойств [2, 3], и высокой подвижностью носителей заряда. Для исследования электронных свойств монослоя фосфорена, легированного азотом, который замещает один атом фосфора в суперячейке, состоящей из 4×4 элементарных ячейки фосфорена, использовалась теория функционала электронной плотности, реализованная в программе VASP (Vienna An initio Simulation Package)[4]. Энергия связи рассчитывалась путем вычитания из полной энергии легированного фосфорена полной энергии фосфорена с вакансией и полной энергии отдельного атома азота, и составила –6,72 эВ. Такая большая энергия связи говорит о том, что данный процесс легирования энергетически выгоден. Легирование атомом азота не ведет к возникновению магнитного момента. Таким образом, исследование электронных свойств фосфорена, легированного азота показало сильные связи легирующего атома, что говорит о высокой вероятности присутствия этой частицы в образцах фосфорена.

Литература

1. Nat. Nanotechnol. / Y. Du [et al.]. 2015. Vol. 9. P. 372–377.
2. ACS Nano / H. Liu [et al.]. 2014. Vol. **8.** P. 4033–4041.
3. Nat.Commun / F. Xia [et al.]. 2014. 5, 4458.
4. Kresse G. VASP the guide: tutorial. Austria, University of Vienna, 2003. P. 94–104.