



Рисунок 3 – Выявляемость дефектов на контрольных образцах при освещении устройством на основе светодиодов ARL2-3214UVC-180mcd (400 нм). а – образец по EN ISO 3452-2 [3], б – образец [4]

На основании проведенных исследований было разработано и изготовлено устройство для освещения зоны контроля при люминесцентной капиллярной дефектоскопии с использованием фиолетовых светодиодов со средней длиной волны 400 нм. Схема и фотография устройства приведены на рисунке 2.

С целью обеспечения высокой чувствительности контроля в данном устройстве были использованы 8 дугообразных плат, содержащих по 25 ориентированных на одну точку светодиодов ARL2-3214UVC-180mcd (400 нм), обеспечивающих для каждой платы на пятне диаметром 35-45 мм яркость до 4000 Кд/м².

Устройство состоит из основания 1, на котором по центру установлена цилиндрическая втулка 2 с отверстием для визуального наблюдения зоны контроля изделия 3. Слева и справа от втулки 2 на основании 1 закреплены держатели 4, на каждом из которых установлены по четыре платы 5 со светодиодами. Основание 1 устанавливается в зоне контроля на регулируемых опорах 6. Для защиты зоны контроля от видимого света используется чехол 7 из светонепроницаемой ткани. Аккумуляторный блок питания обеспечивает возможность автономного использования устройства в полевых условиях.

УДК 004.056.53

ОЦЕНКА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Бондарев В.В.

*Московский государственный технический университет имени Н.Э. Баумана
Москва, Российская Федерация*

При проектировании и построении комплексной системы защиты информации одной из самых сложных проблем является выбор конкретного средства защиты информации из возможных, представленных на рынке. Другими словами, нам приходится проводить сравнитель-

ный анализ, оценку и выбор средства защиты, руководствуясь какими-то критериями, требованиями и прочее. Чаще всего этот выбор основывается на основе профессионального опыта, интуиции, цене, наличии сертификата и т. д., то есть чисто умозрительно, без привлечения

Через смотровое окно втулки 2 возможно проводить фотосъемку индикаторных следов дефектов. На рисунке 3 представлены результаты капиллярного люминесцентного контроля образцов с дефектами раскрытием 0,5-10 мкм [3, 4], полученные с использованием данного устройства. Из рисунка видно, что подсветка зоны контроля при помощи описываемого устройства обеспечивает надежную выявляемость дефектов с шириной раскрытия менее 1 мкм.

Выводы

Впервые показана возможность эффективного применения светодиодов со средней длиной волны 400 нм в качестве источников освещения при выявлении дефектов в люминесцентном капиллярном контроле.

Разработан переносной осветитель для люминесцентной дефектоскопии на основе светодиодов с длиной волны 400 нм. Устройство имеет значительно более низкую стоимость по сравнению с аналогами и обладает большей безопасностью в работе. Устройство может эффективно использоваться при проведении люминесцентного капиллярного контроля в полевых условиях для выявления поверхностных дефектов с раскрытием от 1 мкм.

Литература

1. Migoun N., Delenkovsky N., Gnusin A. Electrochemical Machining for Penetrant Testing in Field Conditions // 18th World Conference on Nondestructive Testing. 16-20 April 2012, Durban, South Africa.
2. Н.П. Мигун, А.Б. Гнусин, И.В. Волович. Компьютеризированная система определяет качество дефектоскопических материалов // Промышленная безопасность. – 2004. – № 1. – С. 34–36.
3. EN ISO 3452-2. Non-destructive testing – Penetrant testing – Part 2: Testing of penetrant materials.
4. Мигун Н.П., Деленковский Н.В. Гнусин А.Б. Новые средства определения чувствительности дефектоскопических материалов для капиллярного контроля // Метрология и приборостроение. – 2007. – № 2. – С. 16–18.

методов и способов формализации. Автор ни разу не сталкивался с математическим аппаратом, который можно было бы положить в основу данного выбора и тем самым добиться хоть какой-то объективности. Данная работа и представляет попытку оценить средства защиты, опираясь на формальные приёмы и методы. Надо сказать, что основные положения статьи были разработаны в моей кандидатской диссертации, где не без успеха удалось ранжировать средства космического нападения эвентуального противника по степени опасности и, тем самым, разработать облик системы предупреждения о космическом нападении.

Вначале необходимо вспомнить или ввести ряд необходимых понятий.

Оценка. Под оценкой будем понимать установление степени соответствия объекта, в данном случае средства защиты информации, нормам, требованиям, эталонам.

Отображением объекта/средства защиты информации в средстве оценки является **мера объекта** – единство качественной и количественной определенности объекта: $M = (\text{качество, количество})$.

Качество – совокупность свойств, отличающая данный объект от другого объекта.

Количество – выражение однородности объектов.

Оценка систем сводится к измерению – оценке соответствия меры системы некоторым эталонам, критериям. В отдельных случаях может производиться сравнительная оценка объектов, в данном случае – средств защиты информации.

Обычно свойства выражают или количественно, или качественно: каждое свойство описывают количественно с помощью некоторой переменной – показателя свойства, значение которого характеризует уровень качества относительно этого свойства.

Уровень качества объекта характеризуется совокупностью показателей свойств, необходимых для соответствия объекта его назначению.

Эта совокупность называется **показателем качества** объекта.

Требуемые качества задаются условиями, которым должны удовлетворять возможные значения показателя качества.

Эти условия называются **критериями оценивания**, а проверка их выполнения – **оцениванием** качества объекта.

А сейчас все введенные понятия попытаемся облечь в виде математического аппарата, может быть, к сожалению, и не совсем совершенного.

Описание средства защиты информации в виде меры

Представим меру в виде

$$M = \begin{bmatrix} C_1, C_2, C_3 \dots, & C_n \\ v_{c_1} v_{c_2} v_{c_3} & v_{c_n} \end{bmatrix}, \quad (1)$$

где C_i – свойства объекта; v_{c_i} – величина (количество) свойства.

Например, описывая межсетевой экран, можно предложить следующие группы свойств и количеств этих свойств:

- физические параметры (WAN, LAN, DMZ, консоль, размер...);
- производительность (производительность межсетевого экрана, кол-во пользователей, параллельные сессии, 3DES, политики, работа по расписанию...);
- работа в режиме межсетевого экрана (NAT, PAT, прозрачный режим, режим маршрутизации, статическая, динамическая, Virtual IP, NAT на основе политик, фильтрация пакетов в туннелях VPN.....) и т. д.

Требуемая мера (стандарт, критерий):

$$M_K = \begin{bmatrix} C_1, C_2, \dots, & C_n \\ v_{c_1}^K v_{c_2}^K & v_{c_n}^K \end{bmatrix}. \quad (2)$$

Мера предмета деятельности:

$$M_{\Pi} = \begin{bmatrix} C_1, C_2, \dots, & C_n \\ v_{c_1}^{\Pi} v_{c_2}^{\Pi} & v_{c_n}^{\Pi} \end{bmatrix}. \quad (3)$$

Близость мер определяется одним из возможных показателей:

$$K_N = \frac{N_{M_K \cap M_{\Pi}}}{N_{M_K \cup M_{\Pi}}}; \quad (4)$$

$$K_N = \frac{\sum_{N_{M_{\Pi}}} \left[\frac{v_{c_i} \min}{v_{c_i} \max} \right]}{N_{M_{\max}}}, \quad (5)$$

где $N_{M_K}, N_{M_{\Pi}}$ – мощности M_K, M_{Π} ; $N_{M_{\Pi}}$ – мощность пересечения множеств C^{Π}, C^K ; $N_{M_{\max}}$ – мощность объединения множеств C^{Π}, C^K .

Качество объекта характеризуется декартовым произведением свойств, а величина этого качества – произведением величин этих свойств.

$$M_K = \begin{bmatrix} C_1, C_2, \dots, & C_n \\ \prod_i & v_{c_i} \end{bmatrix} \quad (6)$$

Методика оценки близости мер

1. Объединяем мощности множеств C в $M_0, M_3: N_{C^0}, N_{C^3}$.

2. Представляем $M_0 \cap M_3$ в виде:

$$M = \begin{bmatrix} C_m, & C_{m+1}, \dots, & C_n \\ v_{c_m}^0 & v_{c_{m+1}}^0 & v_{c_n}^0 \\ v_{c_m}^3 & v_{c_{m+1}}^3 & v_{c_n}^3 \end{bmatrix} \quad (7)$$

3. В каждой паре определяем min- и max-величины.

4. Подставляем значения $v_{c_i} \min, v_{c_i} \max, \max(N_{C^3}, N_{C^0})$ в K_N .

Пример.

$$M_0 = \begin{bmatrix} C_1, & C_2, & C_3, & C_4, & C_5, \\ 2 & 3 & 4 & 1 & 5 \end{bmatrix}. \quad N_{M_0} = 5.$$

$$M_3 = \begin{bmatrix} C_1 & C_3 & C_4 \\ 1 & 3 & 2 \end{bmatrix}. \quad N_{M_3} = 3.$$

$$K_N = \frac{1}{5} \left(\frac{1}{2} + \frac{3}{4} + \frac{1}{2} \right) = \frac{7}{20}. \quad N_{M_n} = 3.$$

Необходимо упомянуть о слабых местах данного подхода. Во-первых, мы исходим из того, что свойства оцениваемого объекта независимы, что на практике встречается крайне редко. Во-вторых, открытым остаётся вопрос, сколько нужно учитывать этих свойств для получения максимально объективной оценки. И, наконец, по умолчанию считается, что рассматриваемые и учитываемые свойства обладают одинаковым весом для оценки, что также встречается нечасто. Однако эти недостатки не носят принципиального характера и могут быть устранены в процессе дальнейших исследований.

Выводы

Сделана попытка добиться максимальной объективности при сравнении различных средств защиты информации. Предлагаемая методика была апробирована автором на практике. Были рассмотрены шесть наиболее широко применяемых (согласно статистике портала Securitylab.ru) сканеров уязвимостей: Nessus (версия 3.2.1); MaxPatrol (версия 8.0.1178); Internet Scanner (версия 7.2.58); Retina Network Security Scanner (версия 5.10.2.1389); Shadow Security Scanner (SSS) (версия 7.141.262); NetClarity Auditor (версия 6.1).

Рассматривались следующие свойства и количества этих свойств: цена сканера; универ-

сальность применения сканера (число поддерживаемых протоколов и векторов доставки – методов доставки данных к серверу); количество поддерживаемых векторов атаки (количество и тип активных плагинов); точность обнаружения CSS; точность обнаружения SQL-инъекций; точность обхода структуры веб-приложения и обнаружения локальных файлов; удаленное использование файлов, XSS; фишинг через RFI; WIVET-сравнение; адаптивность сканера (количество дополнительных возможностей сканера для преодоления защитных барьеров); сравнение особенностей аутентификации (количество и тип поддерживаемых способов авторизации и аутентификации); количество дополнительных возможностей сканирования и встроенных механизмов; общее впечатление о работе основной функции сканирования; наличие лицензий и сертификатов и т. д.

В результате применения методики первое место занял сканер MaxPatrol, на втором месте – сканер Nessus. Эти результаты были подтверждены экспериментальными исследованиями.

Литература

1. Колесников и др. Эргономическое обеспечение деятельности космонавтов, М.: Машиностроение, 1985.

2. Бондарев В.В. Возможный подход к оценке средств защиты информации// Информационно-методический журнал INSIDE. Защита информации. – № 3 – 2017, С. 76–78.

УДК 621.382

ОДНОЭЛЕМЕНТНЫЕ МНОГОФУНКЦИОНАЛЬНЫЕ ФОТОПРИЕМНЫЕ СТРУКТУРЫ СИСТЕМ ОПТИЧЕСКОЙ ДИАГНОСТИКИ

Воробей Р.И., Гусев О.К., Свистун А.И., Тявловский А.К., Тявловский К.Л., Шадурская Л.И.

Белорусский национальный технический университет, Минск, Республика Беларусь

Современные измерительные преобразователи систем оптической диагностики должны автоматически оценивать параметры оптического сигнала и переключаться между различными диапазонами энергетической и спектральной характеристиками чувствительности. Это требует применения нескольких фотоприемников, сложных оптических схем и сложных алгоритмов обработки измерительных сигналов. Относительная сложность физических процессов при перезарядке нескольких энергетических уровней многозарядной глубокой примеси позволяет реализовать многофункциональность фотозлектрического преобразователя (ФЭП) при простой конструкции чувствительного элемента. Фотоэлектрические одноэлементные преобразователи [1] характеризуются расширенными функциональными характеристиками и увеличенными диапазонами энергетической (на несколько десятков децибел)

и спектральной характеристик чувствительности (со сдвигом на 2–4 мкм в диапазоне спектральной чувствительности 1–10 мкм), с возможностью переключения между поддиапазонами энергетической и спектральной характеристик чувствительности под действием как измерительного сигнала, так и дополнительных управляющих воздействий. В качестве основного материала резистивной или барьерной структуры фотоприемника могут использоваться германий, кремний, полупроводниковые соединения типа A^3B^5 , и другие материалы, в том числе совместимые с «не кремниевыми» технологиями и структурами на сапфировых подложках. Характеристиками: функциональностью и параметрами ФЭП можно управлять выбором структуры и материала основного полупроводника, технологией изготовления, режимами питания и смещения, дополнительным оптическим излучением [1–3].