Новизна предложенного подхода заключается в модификации существующей модели: разбиение ошибок на группы и введение весовых коэффициентов. В результате эффективность такого рода расчетов будет заметно выше, так как значимость каждой ошибки будет учтена и ошибки, не имеющие принципиального значения, будут отделены с точки зрения влияния на количественные характеристики надежности от тех, которые являются критическими.

СПИСОК ЛИТЕРАТУРЫ:

1. *Саттон М., Грин А., Амини П.* Fuzzing. Исследование уязвимостей методом грубой силы. М.: Символ-Плюс, 2009. — 560 с.
2. *Чуканов В. О.* Надежность программного обеспечения и аппаратных средств систем передачи данных атомных электростанций: Учебное пособие. М.: МИФИ, 2008. — 180 с.
3. *Майерс Г.* Надежность программного обеспечения. М.: Мир, 1980. — 350 с.

В. С. Матвеева, А. В. Мамаев

КРИМИНАЛИСТИЧЕСКИЙ ПОДХОД К АНАЛИЗУ ВРЕМЕННЫХ АТРИБУТОВ ФАЙЛОВ В ОПЕРАЦИОННОЙ СИСТЕМЕ СЕМЕЙСТВА MICROSOFT WINDOWS И ФАЙЛОВОЙ СИСТЕМЕ NTFS

Подмену временных атрибутов файлов можно сделать как вручную, переводя системные часы или внося изменения в служебные структуры файловой системы, так и с помощью специальных программ, которых существует достаточное количество. Но интересно то, что эти же функциональные возможности также прописывают у ряда вредоносных программ с целью ввести в заблуждение пользователя и отнести файл скорее к системному, чем к подозрительному. Таким образом, при просмотре свойств файла в ОС будут отображаться подмененные сведения. Но не все так просто с точки зрения компьютерной криминалистики. Для распознания факта подмены используются особенности файловой системы NTFS под управлением ОС семейства Microsoft Windows.

В файловой системе NTFS временные атрибуты файлов содержатся в файловой записи для каждого файла в главной файловой таблице (далее — MFT). И как ни странно, у файла их ровно 8, а не 3, как мы привыкли. За временные атрибуты отвечают две структуры: $STANDARD_INFORMATION и $FILE_NAME, каждая из которых содержит дату и время создания файла, последнего изменения файла, последнего доступа к файлу, а также дату и время последнего изменения сведений в файловой записи.

При подмене временных атрибутов файлов изменяют сведения в структуре $STANDARD_INFORMATION, так как именно она отображается пользователю в ОС. При этом структура $FILE_NAME остается неизменной и используется криминалистами для распознания факта подмены и восстановления оригинальных атрибутов файла. Однако это не так-то просто, так как существует большое количество особенностей, на основании которых изменяются временные атрибуты файла в зависимости от ОС и производимых действий. Поэтому проведена серия тестов для разных ОС семейства Microsoft Windows по выявлению условий изменения атрибутов в обеих

структурах. На основании тестов разработан метод выявления оригинальных атрибутов файла и предложен механизм автоматизации этого метода для обработки большого количества файлов.

Полученные результаты используются в сфере компьютерной криминалистики при восстановлении хронологии событий при инцидентах в сфере информационных технологий.

СПИСОК ЛИТЕРАТУРЫ:

1. *Lee R.* Windows 7 MFT Entry Timestamp Properties [Электронный ресурс]: международные публикации по компьютерной криминалистике. SANS Forensics Community, 2010. URL: http://computer-forensics.sans.org/blog/2010/04/12/windows-7-mft-entry-timestamp-properties. (дата обращения: 29.12.2012 г.).
2. *Carrier B.* File System Forensic Analysis. Addison Wesley Professional (издательство), 2005. 400 – 502 p.

А. А. А. Наджи, Н. А. Кинаш, А. А. Тихомиров, А. И. Труфанов

УГРОЗЫ БЕЗОПАСНОСТИ ПРОЕКТАМ ДИСТАНЦИОННОГО ОБРАЗОВАНИЯ В СТРАНАХ С ВЫСОКИМ ИНДЕКСОМ НЕДЕЕСПОСОБНОСТИ

Введение

Сложность реализации дистанционных форм образования в конкретной стране определяется множеством факторов, связанных с уровнем ее развития — социального, экономического, технического и т. д. Одним из общепринятых показателей низкого уровня развития является «рейтинг недееспособности» государств [1]. Например, по данным рейтинга недееспособности государств мира за 2012 г., Йеменская Республика (Йемен) занимает 8-е место. Правительство Йемена, учитывая значимость дистанционного образования (ДО), сформулировало национальную политику по его внедрению. Данная политика нуждается в активном воплощении, что требует ясного понимания и решения сопутствующих проблем информационной безопасности (ИБ) как одного из ключевых факторов успеха. Можно предполагать, что проблемы ИБ ДО в Йемене характерны для большинства стран с высоким индексом недееспособности.

Метод исследования

Первоочередными задачами при становлении новой области ИБ ДО являются:

- анализ рисков;
- разработка методов обеспечения ИБ в ДО с учетом новизны самого ДО.

Также необходимо обратить внимание на возможность использования самой системы ДО как потенциального канала распространения иной — не академической — конструктивной или деструктивной информации.

Основные результаты

Если такие факторы, как мошенничество со стороны организаций, предлагающих услуги ДО; мошенничество со стороны студентов, преподавателей, персонала технической поддержки; угрозы