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

со стороны конкурентов; угрозы со стороны контролирующих органов; низкая подготовленность заинтересованных в получении ДО; низкая квалификация предлагающих услуги ДО; возникновение различных негативных явлений в физическом, нравственном и духовном здоровье обучаемого в системе ДО, являются известными и присущими любой системе ДО, то анализ рисков ДО в Йемене указывает на широкий спектр специфических угроз ИБ и на их сложную взаимосвязь. Следуя традиционной классификации, выделены следующие источники угроз (ИУ):

антропогенные ИУ:

- низкий уровень грамотности (Йеменская Республика занимает 154-е место в индексе образования, публикуемом ООН [2], причем этот показатель в последние годы только снижается),
- терроризм, экстремизм, гражданская война (продолжается гражданская война против племени Аль-Хути, функционирует штаб Аль-Каиды на юге страны);

техногенные ИУ:

- проблема электроснабжения (в Йеменской Республике только 52 % населения имеют доступ к электричеству [3]; зафиксированы многочисленные случаи повреждения линий электропередачи злоумышленниками),
- низкий уровень развития ИКТ (по данным нового рейтинга развития Интернета в странах мира, включающего пока 61 страну (2012 г.), Йемен занимает последнее место [4]; только 12 % населения используют Интернет),
- высокая стоимость интернет-услуг (при полном отсутствии кабельных сетей два часа веб-серфинга через телефонную сеть стоят 1200 риалов (около $ 5,6); для граждан Йемена со средним доходом это означает трату половины зарплаты только на Интернет);

природные ИУ:

- проблемы с водоснабжением (проблема дефицита воды в Йемене является источником 80 % конфликтов внутри страны; вооруженные конфликты возникают между йеменскими племенами за скважины, подрывая социальную стабильность в стране. Это, в свою очередь, опосредованно осложняет перспективу развития ДО),
- наркопотребление (в Йемене выращивается растение кат, которое жуют до 90 % мужского населения и 25 % женщин [5]. Большая часть зарплаты граждан Йемена уходит на покупку листьев ката, остальная часть средств — на поддержание семьи, оставляя образовательные услуги невостребованными. При этом значительное время йеменцы проводят за употреблением ката, который дает ощущение эйфории, сменяющееся спокойствием, и полностью отбивает стремление к учебе).

Наряду с вниманием к функциональным уязвимостям системы ДО, с которыми взаимодействует комплекс угроз, не менее, а даже более важным представляется анализ топологической компоненты. Если функциональные уязвимости напрямую связаны с недостаточным финансированием защитных мероприятий, то структурные обусловлены организационными просчетами и ошибками проектирования. Моделирование композитной сети с социальной и технологической составляющими рассматривалось в качестве перспективного инструмента при построении топологически устойчивой системы ДО в Йемене, позволяющей учесть множество специфических, взаимовлияющих друг на друга угроз.

Выводы

Сформулирован набор наиболее значимых угроз, которые необходимо учитывать при построении устойчивой системы дистанционного образования в бедных странах арабского Востока.

Предложено использование сетевых моделей для анализа информационной безопасности систем дистанционного образования с акцентом на их структурные уязвимости.

СПИСОК ЛИТЕРАТУРЫ:

1. http://gtmarket.ru/news/2012/06/19/4439 (дата обращения: 13.12.2012).
2. http://hdrstats.undp.org/en/indicators/103706.html (дата обращения: 13.12.2012).
3. http://espanol.doingbusiness.org/~/media/fpdkm/doing%20business/documents/profiles/country/YEM.pdf (дата обращения: 13.12.2012).
4. http://thewebindex.org/data/index/ (дата обращения: 13.12.2012).
5. http://ru.wikipedia.org/wiki/Кат (дата обращения: 13.12.2012).

А. П. Никитин

МОДЕЛЬ СИСТЕМЫ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ ПЕРСОНАЛЬНОГО КОМПЬЮТЕРА ПО ЕГО «КЛАВИАТУРНОМУ ПОЧЕРКУ»

Целью работы является построение теоретической модели системы идентификации пользователей, основанной на применении динамических биометрических параметров.

Данной теме посвящено значительное количество работ, однако ряд их носит сугубо теоретический характер, задачей других является аутентификация пользователя. Также в некоторых работах отмечаются ошибки как первого, так и второго рода, затрудняющие практическое использование предложенных схем. Причиной этого является рост объемов текстов и/или длительности обучения.

Необходимость системы идентификации пользователя возникает в целом ряде случаев, например, когда стоит задача идентификации «анонимных» пользователей в сети Интернет. Вторым применением данной системы может быть мониторинг пользователей в процессе их работы за компьютером с целью предотвращения НСД в систему через АРМ, на которых уже выполнена аутентификация пользователей другими методами.

Наиболее перспективным методом решения данной задачи представляется использование «клавиатурного» почерка, т. е. характерных особенностей работы пользователя с клавиатурой, которые позволяют однозначно идентифицировать пользователя.

Система идентификации, предложенная в данной работе, имеет клиент-серверную архитектуру и состоит из двух компонентов — клиентской части, предназначенной для сбора статистики по клавиатурному «почерку», и серверной части, предназначенной для выполнения следующих функций:

- построение на основе собранных статистических данных образов «почерка»,
- хранение образов,
- сопоставление полученного образа с имеющимися в базе,
- принятие решения об идентификации пользователя на основании сравнения полученного образа его «почерка» с уже имеющимися в базе данных.

Клиентская часть комплекса реализуется с использованием приложений уровня ядра, перехватывающих сообщения драйвера клавиатуры.

Серверная часть производит первичную обработку полученных от клиента данных. Затем происходит построение образа пользователя. Далее полученный образ последовательно сопоставляется со всеми имеющимися в базе образами.