будет уязвим, вся система продолжит функционировать в нормальном режиме. Контроль доступа должен быть основан на идентификации. В этом случае необходимо присваивать каждому субъекту уникальный образ, имя и число. В обязанности службы безопасности входит проверка соответствия всем требованиям. Приведенные выше организационные методы являются лишь базовыми для обеспечения защиты информации на предприятии. Данный список может дополняться в зависимости от конфиденциальности информации, которая используется при работе предприятия, объема выполняемых работ и опыта работы сотрудников предприятия в сфере защиты информации. Эффективность каждого блока полностью зависит от руководства предприятия, которое должно обеспечить предприятие финансовыми и человеческими ресурсами. Финансовые вложения позволяют обеспечить предприятие необходимыми техническими и криптографическими средствами защиты информации.

Литература

1. Бабенко Л.К., Ищукова Е.А. Современные алгоритмы блочного шифрования и методы их анализа. М.: Гелиос АРВ, 2006. 376 с.

2. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. Кн. 1. М.: Энергоатомиздат, 1994. 400 с.

ПРОГРАММНОЕ СРЕДСТВО ПРЕДПРОСМОТРА НАСТРОЕК ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ MICROSOFT DYNAMICS AX

В.Н. Нестеренко

В работе представлено расширение для модуля «Безопасность» ERP-системы Microsoft Dynamics AX [1], позволяющее осуществлять предпросмотр отдельных частей интерфейса системы с учетом привилегий конкретного пользователя.

Разработанное программное средство предназначено для оптимизации процесса обеспечения безопасности путем определения прав доступа пользователей ERP-системы. С его помощью разработчики и менеджеры безопасности могут увидеть, как будет выглядеть та или иная форма для указанного пользователя Microsoft Dynamics AX в соответствии с предоставленными ему привилегиями. Программное средство позволяет учитывать общие настройки доступа пользователей, особенности отображения форм, связанные с привилегиями точки входа, а также воздействия «Record-level security». Для случаев, когда вызов формы осуществляется из родительской формы, предусмотрена возможность настройки и передачи необходимых входных данных в вызываемую форму, в том числе привилегии формы-родителя, что позволяет в полной мере эмулировать такого рода ситуации. Расширение представлено графическим интерфейсом, выполненным в соответствии с правилами, принятыми для Microsoft Dynamics AX. В ходе работы были реализованы алгоритмы обхода элементов форм, определения действующих прав доступа к элементам форм на основе ролей пользователя и установленной привилегии точки входа, фильтрации данных по правилам «Record-level security» с учетом текущих ролей пользователя и других особенностей этой технологии. Для этого использовались встроенный фреймворк для обработки узлов дерева объектов Microsoft Dynamics AX, стандартные методы и классы модуля «Безопасность», а также утилиты для работы с «Record-level security». В результате удалось получить эффективное средство для контроля проделываемой работы по установке привилегий пользователей.

Литература

1. The Microsoft Dynamics AX Team. Inside Microsoft Dynamics AX 2012 R3. Redmond: Microsoft Press, 2014. 371 p.

МЕТОДИКА ТЕСТИРОВАНИЯ АНТИВИРУСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Омуару Алвелл Эллингтон, Е.С. Белоусова

С быстрым развитием технологий меняется и характер вирусных угроз для данных. Технологии, которые должны обеспечить защиту от этих угроз, должны адаптироваться.

Разработчики антивирусных программ утверждают, что они обеспечивают эффективное реагирование на компьютерные вирусные инциденты. Однако в настоящее время мало указаний относительно наилучшего способа оценки эффективности таких требований. Поэтому особенно актуальным является разработка тестов антивирусных программных продуктов, которые измеряют эффективность функциональных возможностей антивируса. Используя этот подход, была разработана методика тестирования выполнения требований к функциональности антивирусных программ. В настоящее время существует 4 метода тестирования антивирусных программ: статическое тестирование, динамическое тестирование; тестирование скорости реакции, ретроспектива. Тесты продолжают развиваться по мере развития отрасли, продукты становятся более сложными, требуются более сложные тесты. важно расширить методологию тестирования в областях, которые наиболее важны для защиты пользователей, используя индикаторы, которые важны как для пользователей, так и для разработчиков.

Методика тестирования антивирусных продуктов заключалась в диагностики сканирующих механизмов, защиты от вредоносных веб-приложений, фишинга, дополнительных сканеров. Для тестирования были выбраны следующие программные продукты: Kaspersky, Avira, Avast, Eset NOD32. На основе проведенных тестов можно заметить, что не один из тестируемых продуктов не обнаружил 100 % зараженных файлов, при этом все продукты осуществляли попытку лечения некоторых файлов, а не просто удалять обнаруженные ими угрозы. Антивирусный продукт Kaspersky обнаружил 97,65 % зараженных файлов, при этом из них более 60 % было удалено. Антивирусный продукт Eset NOD32 обнаружил 77,88 % зараженных файлов, восстановлено было около 55 % файлов.

ЗАЩИТА АВТОРСКИХ ПРАВ ИЗОБРАЖЕНИЯ С ИСПОЛЬЗОВАНИЕМ ЦВЗ

Н.В. Орлов

1. *Проблема.* Вопрос защиты авторских прав на цифровые изображения актуален в наше время, т.к. графические материалы, разработанные автором, могут быть легко скопированы или распространены. Простота кражи чужих графических изображений привело к тому, что каждый день увеличивается их хищение. Исходя из этого, проблема защиты авторских прав на графические изображения актуальна в наше время, и техническим решением данной проблемы является программный продукт, предотвращающий копирование, искажение или распространение авторских материалов.

2. *Метод решения.* Для защиты графических материалов широко используется применение цифровых водяных знаков. Таким образом, для защиты графических материалов от копирования и распространения используется программное обеспечение, основанное на графической защите с применением ЦВЗ на основе криптографического метода Куттер-Джордона-Боссена.[1]

В данном методе ЦВЗ внедряются с помощью изменения цветовых компонентов пикселя. Отдельно взятые биты ЦВЗ неоднократно внедряются в изображение с помощью изменения показателей синего канала в пикселе. Внедрение информации производится по одному биту в один пиксель контейнера. С помощью секретного ключа задаются координаты пикселей, в которые будет произведено встраивание. При внедрении цветовые показатели красного и зеленого цветов остаются неизменными, а цветовые показатели синего – будут изменяться по следующей формуле: $Bx,y^* = \begin{cases} Bx,y + \lambda Yx,y, \text{ при } Mi = 1 \\ Bx,y - \lambda Yx,y, \text{ при } Mi = 0 \end{cases}$, где $\lambda = 0{,}1$; $Yx,y = 0{,}3*Rx,y+0{,}59*Gx,y+0{,}11*Bx,y$. Обозначения: Bx,y – показатель яркости синего цвета с координатами (x, y); Bx,y^* – показатель изменения яркости синего цвета пикселя; Yx,y – показатель яркости пикселя; Mi – i-й бит встраиваемой информации; λ – коэффициент, задающий энергию встраиваемого бита данных [2].

3. *Эффективность.* ЦВЗ должен отвечать следующим свойствам: незримость для человеческого глаз, стойкость к искажению контейнера. Метод Куттера-Джордана-Боссена выполняет необходимые свойства. Достижение незримости для человеческого глаза осуществляется с помощью внедрения битов ЦВЗ именно в синий канал пикселя, так как к данному цвету, человеческий глаз обладает наименьшей чувствительностью.