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.