Лабораторная работа №4,5

Разработка защищённых приложений

Количество часов практических занятий – 8
Количество часов самостоятельной работы – 12

Цель работы:
Познакомиться с концепцией ролевого управления доступом и способами защиты программного обеспечения от существующих угроз.
Научиться разрабатывать приложения, которые используют ролевое управление доступом для разграничения полномочий пользователей. Получить навыки защиты разработанной программы от несанкционированного копирования и других угроз, которым может подвергаться программное обеспечение.

ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Список литературы
1. Нортроп, Т. Разработка защищённых приложений на Visual Basic .NET и Visual C# .NET : учебный курс Microsoft / Т. Нортроп. – М. : Издательство "Русская редакция", 2007. – 688 с.
2. Скляров, Д.В. Искусство защиты и взлома информации / Д.В. Скляров. – СПб. : БХВ- Петербург, 2004. – 288 с. 3. Ховард, М. Защищённый код : пер. с англ. / М. Ховард, Д. Лебланк. – 2-е изд., испр. – М. : Издательско-торговый дом "Русская редакция", 2004. – 704 с.

ЗАДАНИЕ:

Реализовать программы, выполняющие указанные в задании действия.
Задание I.
Реализовать приложение с графическим интерфейсом, удовлетворяющее следующим требованиям:
1) Приложение проводит аутентификацию пользователя.
2) Каждый пользователь программы должен относиться к какой-нибудь группе пользователей (роли), членам которой доступны различные функциональные возможности программы.
3) Программа должна принимать от пользователя некоторые данные и, возможно, после некоторой обработки, отображать их.
4) При этом должна осуществляться защита от как минимум 4-х типов возможных атак на приложение:
   4.1) Атака «переполнение буфера».
   4.2) Атака «SQL-инъекции».
   4.3) Атака, эксплуатирующая ошибки канонизации.

4.4) Атака «XSS» (межсайтовое кодирование).
4.5) Принцип минимизации привилегий.
4.6) DoS-атака (отказ в обслуживании).

При разработке защиты нужно предположить, что приложение работает с базой данных, в которой сохраняет введённые пользователем данные.

Задание II.

Протестировать правильность работы систем защиты разработанных приложений посредством реализации тестовых атак выбранных 4-х типов.

Задание III.

Реализовать приложение-инсталлятор, позволяющее установить на компьютер пользователя приложение, реализованное в предыдущем пункте задания.

Требования к приложению:

1) Приложение-инсталлятор совместно с устанавливаемым приложением должно обеспечивать защиту программного продукта от несанкционированного тиражирования.
2) Приложение-инсталлятор должно иметь защиту от возможных атак на него.