Санкт-Петербургский Государственный Политехнический университет

Институт информационных технологий и управления

Факультет технической кибернетики

Кафедра измерительных информационных технологий

Проект допущен к защите   
Зав. кафедрой

\_\_\_\_\_\_\_\_\_\_\_\_\_Г.Ф. Малыхина

«\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_ 2014 г.

**ДИПЛОМНЫЙ ПРОЕКТ**

Тема: **Внедрение элементов защиты в .NET приложения  
без необходимости модификации исходного кода**

Направление: 090900 — Информационная безопасность

Специальность: 090104 — Комплексная защита объектов информатизации

Выполнил:

студент гр. 53505/2 С.А. Гладышев

Руководитель:

доцент, к.т.н. В.Ю. Сальников

Консультанты:

по экономической части

доцент, к.э.н. И.Б. Корокин

по вопросам охраны труда

доецнт, к.ф.-м.н. Г.В. Струйков

Санкт-Петербург   
2014

**Оглавление**

[Введение 6](#_Toc388132801)

[Техническое задание 9](#_Toc388132802)

[1. Обзор технологий защиты 12](#_Toc388132810)

[1.1. Стеганография и водяные знаки 12](#_Toc388132811)

[1.2. Обфускация 14](#_Toc388132812)

[1.3. Упаковка 16](#_Toc388132813)

[1.4. Системы лицензирования 17](#_Toc388132814)

[1.5. Защита от модификаций 17](#_Toc388132815)

[1.6. Сокрытие данных 18](#_Toc388132816)

[1.7. Комплексный подход 19](#_Toc388132817)

[1.8. Обзор имеющихся решений 19](#_Toc388132818)

[2. Теоретическая разработка 22](#_Toc388132819)

[3. Реализация 29](#_Toc388132823)

[4. Тестирование 30](#_Toc388132824)

[5. Организация рабочего места 31](#_Toc388132825)

[6. Экономическое обоснование 36](#_Toc388132832)

[Список литературы 40](#_Toc388132835)

# Перечень терминов и условных обозначений

**CLR** (Common Language Runtime) **–** общеязыковая исполняющая среда. Исполняющая среда, интерпретирующая код на языке IL в байт-код, в который компилируются программы, написанные, в частности, на .NET-совместимых языках программирования.

**DLL** (Dynamic Link Library) **–** динамически подключаемая библиотека. Динамическая библиотека, позволяющая многократное использование различными программными приложениями.

**Easter Egg** («пасхально яйцо») **–** разновидность секрета, оставляемого в программном обеспечении создателями, особенность которого состоит в том, что его содержание, как правило, не вписывается в общую концепцию.

**IL** (CIL, MSIL, Common Language Runtime) **–** промежуточный язык, разработанный фирмой Microsoft для платформы .NET Framework.

**ILASM/ILDASM** (IL assembler/IL disassembler) – служебные программы, ассемблер и дизассемблер, поставляемые совместно с VisualStudio.

**JIT-компиляция** (Just-in-time) – динамическая компиляция, технология увеличения производительности программных систем, использующих байт-код, путём компиляции его в машинный код непосредственно во время работы программы.

**MSBuild** – платформа сборки проекта, разработанная Microsoft и позволяющая автоматизировать сборку и назначить дополнительные задачи.

**WinApi-приложение** (Windows application programming interfaces) – приложения, использующие набор базовых функций интерфейсов программирования приложений операционных систем семейств Microsoft Windows.

**ПО** – программное обеспечение.

**Сборка** (англ. assembly) – двоичный файл, содержащий управляемый код (метаданные и инструкции языка IL), получаемый на выходе компилятора.

**Хеш-сумма** – результат обработки неких данных хеш-функцией (функция, преобразующая по определенному алгоритму данные произвольной длины в строку фиксированной длины).

# Введение

В наши дни информационные технологии являются основной движущей силой прогресса и захватывают все большие области современной жизни. Информационные технологии – это совокупность программно-технических средств вычислительной техники и способов их применения для обработки информации в различных областях. В связи с таким широким их распространением, серьезно встает вопрос защиты обрабатываемых и хранимых данных. Ведь если раньше, вы были уверены в том, что никто не получит доступ к вашим документам, лежащим в сейфе, без ключа или пароля. Теперь же большая часть информации хранится в электронном виде и необходимы уже другие способы защиты.

Этот принцип действует и для разрабатываемых программ. Если раньше, программы были по большей части низкоуровневыми и хранились в виде машинных кодов конкретной архитектуры, то с течением времени появляется все больше различных высокоуровневых инструментов для облегчения разработки, развиваются и усложняются сами языки программирования.

Чтобы снять с разработчика обязанности прямой работы с памятью, контроля типов, а также сделать программу более гибкой для различных платформ и языков, приложения выполняются специальной исполняющей средой (виртуальной машиной). Примеры таких виртуальных машин: JVM (виртуальная машина Java), CLR (общеязыковая исполняющая среда), Dalvik Virtual Machine (часть мобильной платформы Android). Эти средства значительно упрощают разработку, но они разработаны так, что требуют трансляции приложения в промежуточный байт-код (промежуточный язык, язык высокоуровневого ассемблера), который затем в момент выполнения компилируется в машинный ход JIT-компиляторами (компиляция «на лету»). Вследствие чего, приложения хранятся на диске в виде инструкций промежуточного языка, который легко декомпилируется обратно в исходные коды с помощью различных инструментов, таких как .NET Reflector, FernFlower (декомпилятор Java) и другие.

Соответственно существуют простые способы обхода лицензирования, получения исходных кодов и модификации под свои нужды незащищенных приложений написанных на языках .Net (и других подобных языков программирования, таких как Java). При этом для них не существует абсолютной защиты, как и не существует такой защиты для низкоуровневых приложений (например Win-32, написанных на С++), отсюда исходит основной принцип защиты программных продуктов:

*Защита приложения лишь увеличивает время его взлома и в идеале, защита должна окупить себя, т.е. время, затраченное на защиту приложения должно быть сопоставимо со временем, затраченным на взлом этой защиты.*

Существуют несколько основных технологий или методик защиты .Net приложений. Их можно разделить на две части: те, которые работают с кодом программы и те, которые работают с памятью.

Для сокрытия кода используются различные обфускаторы и упаковщики. Обфускаторы используют для защиты запутывание кода (англ. control flow), переименование методов и классов, шифрование ресурсов, добавление невалидных конструкций и др. Упаковщики модифицируют сборку, и на выходе получается WinApi-приложение, содержащие в себе код сборки и модуль распаковки. Упаковщики и обфускаторы могут применяться одновременно.

В дополнение к защите кода может применяться защита данных, хранящихся в памяти во время выполнения программы. Здесь возможно множества решений, которые зависят от конкретного приложения и его архитектуры.

Так же существует еще один метод защиты – модификация кода во время выполнения приложения. С помощью перехвата вызовов функций (англ. hooking) можно изменять поведение программы, что дает возможность более сложной защиты приложений.

Данная работа направлена на рассмотрение существующих решений, выявления преимуществ и недостатков и разработку нового решения, основанного одновременно на нескольких методах и технологиях, как защиты, так и упрощения ее внедрения в готовый проект.

# Техническое задание

## Введение

Данный программный продукт предназначен для защиты данных, используемых в приложениях, написанных с использованием .NET Framework. Программа модифицирует целевое приложение и тем самым защищает данные, находящиеся в памяти во время его работы.

## Основания для разработки

Разработка решения ведется на основании обзора и анализа существующих решений в сфере защиты программного обеспечения в рамках текущего дипломного проекта.

## Назначение разработки

Программа представляет собой отдельное приложение, позволяющее модифицировать .NET сборки путем внедрения кода, обеспечивающего определенную защиту. Внесенные изменения должны предоставлять эффективную защиту данных приложения, хранящихся в памяти и по возможности препятствовать их модификации.

## Требования к программному продукту

Требования к функциональным характеристикам.

Программа должна уметь работать с запускаемыми exe файлами и библиотеками функций DLL. Цель модификации – внедрение конструкций, отвечающих за выполнение логики по защите данных.

Логика защиты данных описана в отдельной DLL библиотеке, которая должна быть подключена к модифицируемому приложению и поставляться вместе с ним конечному пользователю.

Входными данными для приложения является валидная .NET сборка, транслированная в промежуточный язык IL. На выходе необходимо получить приложение с тем же функционалом и не нарушенной логикой работы.

Должна быть предусмотрена возможность модификации приложения в ходе сборки проекта с использованием платформы MSBuild.

Требования к надежности

При некорректном завершении работы приложения по каким-либо причинам, состояние модифицируемой сборки должно быть восстановлено до исходного.

Требования к составу и параметрам технических средств

Минимальные технические характеристики:

* Windows XP SP1 и выше;
* Microsoft Visual Studio 2005 и выше;
* .NET Framework 2.0 и выше.

Требования к информационной и программной совместимости

Модифицируемые сборки должны быть написаны на платформе .NET Framework версии 2.0 и выше на следующих языках программирования: C#, F#, Visual Basic.

Специальные требования

Специальных требований к характеристикам программы не предъявляется.

## Технико-экономические показатели

Разрабатываемый продукт является бесплатным для распространения.

Время, затраченное на разработку, составит 20 человеко-часов.

## Стадии и этапы разработки

Эскизный проект – 1 час

Разрабатывается структура программы, алгоритм модификации сборок и алгоритм защиты данных. Определяется система взаимодействия с модифицируемыми приложениями.

Тестовый проект – 6 часов

Создание рабочего решения, позволяющего защищать приложения с помощью простого алгоритма. Отсутствие проверок и восстановления после ошибок.

Технический проект – 4 часа

Написание эффективного алгоритма по защите данных, добавление обработки ошибок и восстановления после некорректного завершения работы.

Рабочий проект – 4 часа

Реализация автоматизации процесса, интеграция с процессом сборки модифицируемых решений. Подготовка контрольно-отладочного примера.

Тестирование – 5 часов

Тестирование работоспособности решения. Попытка противодействовать используемой защите.

## Порядок контроля и приемки

Контроль и приемка разработки осуществляются на основе проведенных испытаний контрольно-отладочных примеров. При этом проверяется выполнение всех функций программы.

# Обзор технологий защиты

В данной главе будут рассмотрены основные технологии защиты программного обеспечения, исполняемого в среде .Net и приведены популярные существующие решения для этих областей. По завершению этой главы будет проведен анализ преимуществ и недостатков рассмотренных средств защиты.

## Стеганография и водяные знаки

Стеганография – это метод защиты программного обеспечения (ПО) путем встраивания секретной информации в приложение (код или данные). Это делается для идентификации владельца ПО и позволяет избежать или детектировать создание нелицензионных копий приложений. Подобное внедрение водяных знаков (англ. watermarks) позволяет владельцам лицензионного ПО определить подлинность копии путем извлечения водяных знаков.

По методу встраивания водяные знаки можно разделить на две категории: статические (англ. static) и динамические (англ. dynamic). К статическим относятся: модификация данных (строк) и кода. Для детектирования таких водяных знаков не обязательно запускать приложение, но они очень легко снимаются. К динамическим относятся: «пасхальные яйца» (англ. dynamic Easter Egg watermarks) – изменения в незаметном или редко используемом месте программы, изменения алгоритма работы программы (англ. dynamic execution trace watermarks) или изменение динамических данных, доступных из вне (англ. dynamic data structure watermarks), например, глобальных переменных или областей памяти.

Чтобы понять эффективность тех или иных мер защиты, необходимо понимать потенциальные направления атак. Рассмотрим возможные виды атак на водяные знаки:

* Удаление водяных знаков (англ. subtractive attack). Заключается в нахождение измененного места и вырезания защиты.
* Искажение водяных знаков (англ. distortive attack). Цель такой атаки – исказить значение так, чтобы владелец не смог идентифицировать свое приложение.
* Добавление водяных знаков (англ. additive attack). Добавление новых водяных знаков затрудняет доказательство владельцем подлинности продукта.

Любая из указанных атак считается эффективной, если не нарушена работоспособность приложения и в случае добавления или искажения, механизм создания новых водяных знаков должен использовать алгоритм владельца.

Исходя из особенностей атак на водяные знаки мы можем определить стратегию защиты ПО с использованием данного метода:

* Водяные знаки должны быть скрыты от обнаружения;
* Водяные знаки должны обладать устойчивостью к модификации приложения (обфускации, деобфускации);
* Чем больше используется различных способов внедрения водяных знаков и их количество, тем эффективнее защита;
* Внедрение защиты не должно сказываться на производительности приложения;
* Водяные знаки следует генерировать с использованием закрытого алгоритма или ключей (ассиметричное шифрование), что позволит избавиться от проблемы добавления новых водяных знаков злоумышленником.

Как пример эффективного решения можно привести следующий алгоритм: в программе создается несколько статических массивов и, чтобы они не были «мертвыми», нам необходимо вовлечь их в какие-либо вычисления. Генерировать значения водяных знаков будем с помощью ассиметричного алгоритма шифрования (например, AES) и будем использовать хеширование для точной идентификации водяных знаков в памяти. Секретный ключ для генерации хранится у разработчика. Проверять приложения на подлинность будем путем анализа памяти и нахождения значений наших водяных знаков.

Подобные методы защиты могут быть реализованы как в отдельных продуктах, так и в комплекте с обфускатором.

## Обфускация

Обфусцированной (англ. obfuscated, запутанной) называется программа, которая на всех допустимых для исходной программы входных данных выдаёт тот же самый результат, что и оригинальная программа, но более трудна для анализа, понимания и модификации [3].

Соответственно, *обфускация* – это процесс применения к исходной программе запутывающих преобразований, затрудняющих дальнейший ее анализ. Обфускация может осуществляться на разных уровнях, соответствующих типам информации, на которые она нацелена, так, основываясь на таксономии запутывающих преобразований [4], можно выделить следующие уровни обфускации:

1. **Запутывание форматирования исходного текста** (англ. layout obfuscation).

Сюда относятся изменение имен методов и классов, объединение классов и пространств имен, удаление форматирования, комментариев, изменение метаданных. Данные преобразования могут применяться как к исходному тексту программы на языке высокого уровня, так и к скомпилированной сборке. Особо не влияют на сложность анализа.

1. **Запутывание данных** (англ. data obfuscation).

Изменения могут затрагивать размещение данных в памяти (имеется ввиду перенос переменных в глобальную область, объединение нескольких переменных в одну, изменение порядка в массиве), кодирование, агрегацию и перемешивания строк и ресурсов.

1. **Запутывание потока управления** (англ. control flow obfuscation).

В отличие от запутывания данных, данный метод способен достаточно сильно увеличить сложность программы. Можно выделить следующие способы преобразований:

* Преобразования агрегации. Вставка и переплетение функций, раскрутка циклов, клонирование кода;
* Преобразования вычислений. Вставка избыточного кода, и усложнение вычислительных преобразований;
* Использование непрозрачных предикатов. Непрозрачный предикат – предикат, значение которого известно в момент запутывания, но трудноустанавливаемо после [3], это такие выражение, которые не зависимо от значений аргументов, всегда истины, либо ложны.
* Табличная интерпретация. Добавление таблиц переходов (например, больших CASE структур), сильно увеличивающих ветвление кода. Добавление интерпретатора (виртуальной машины) – свойственно упаковщикам.

1. **Превентивные трансформации** (англ. preventive transformation).

Такие трансформации ориентированы на отладчики, декомпиляторы, деобфускаторы. Могут быть как врожденными (затрудняющие распутывание существующими методами) и целевыми (использующие известные проблемы конкретных решений).

На рынке существует множество различных обфускаторов, отличающихся своим набором возможностей для обфускации, рассмотренных выше, возможностями противодействия деобфускации, цена и зависимостью от версий сборок и платформы. В общем, обфускаторы можно разделить на две группы по используемым средствам воздействия на обфусцируемую сборку [6]:

* Stand-alone обфускаторы, использующие свои интерфейсы для доступа к метаданным и генерации обфусцированной сборки;
* Зависимые от сервисов .Net (ILASM/ILDASM). Функционал таких обфускаторов заведомо ограничен тем набором инструментов, которые предоставляют сервисы.

## Упаковка

*Упаковка* – способ модификации сборки, при котором на выходе получается WinApi-приложение, содержащее в себе упакованный (не обфусцированный) IL код и распаковочный модуль.

Такой способ вносит некоторые ограничения:

* Сборка остается рабочей только под операционной системой Windows;
* Из-за этого теряется преимущество JIT-компиляции среды CLR, дающее гибкость для х64 и х86 платформ (генерация различных инструкций, в зависимости от платформы);
* Упаковка немодифицированных сборок не дает серьезной защиты и легко обходится;
* Упаковщики могут перехватывать вызовы виртуальной машиной функций библиотеки mscoree.dll, что предоставляет дополнительную защиту от его снятия. Но на работу таких программ может влиять антивирус и они сильно зависимы от версии .Net Framework.

Упаковщики помимо своей основной функции обычно содержат множество средств дополнительной защиты, основными из которых являются:

* Отслеживание отладки. Позволяет запретить или детектировать выполнение приложения под отладчиком. В продвинутом варианте, оболочка (упаковщик) приложения может передать сигнал на нижний уровень, где, например, может произойти затирание отлаживаемого кода в памяти.
* Обнаружение виртуальной машины. Запрещает выполнение приложения под виртуальной машиной
* Защита памяти и проверка целостности данных. Отслеживание и выявление обращений к памяти и ее модификации.
* Защита импорта и создание DLL оберток. Позволяет либо скрыть информацию об используемых библиотеках, либо исключить их хранение на диске путем включение DLL в состав исполняемого файла.

## Системы лицензирования

Данный метод защиты используется для защиты лицензионного ПО от копирования. Основная суть заключается в выдачи вместе с продуктом уникального ключа, который однозначно идентифицирует данную копию продукта. Отслеживание подлинности продуктов может проводится с использованием сервера лицензирования и активации, это значительно повышает устойчивость к взлому. Сервер активации предполагает, что при установке приложения, оно должно быть активировано с помощью ключа активации, использование которого строго отслеживается, таким образом, избегается возможность повторной установки.

Часто такие системы входят в состав продуктов, называемых протекторами. *Протекторы* (англ. native processor wrapper) – приложения, совмещающие в себе упаковщик и обфускатор (обычно довольно слабый). Протекторы являются комплексным решением.

При генерации упакованной сборки, протектор внедряет в нее блок активации. Многие протекторы, имеющие систему лицензирования предлагают различные дополнительные сервисы:

* Сервер активации;
* Генератор ключей. Возможность генерировать ключи на сервере в автоматическом режиме;
* Деактивация ключей. Позволяет пользователю перенести программу на другой компьютер и активировать ее заново;
* Блокировка ключей. В приложение встраивается база скомпрометированных ключей активации;
* Привязка к аппаратному обеспечению.

## Защита от модификаций

Суть данного метода заключается в обнаружении нарушения целостности оригинального ПО. Может применяться совместно с обфускацией приложения и защищать его от попыток деобфусцирования.

Самый простой способ защиты от модификаций (англ. tamper-resistant**)**– это подсчет хеш-суммы всего приложения или его модулей (в случае использования упаковщика – хеш-суммы упакованного кода). Полученное значение сравнивается с оригинальным значением, рассчитанным для данной сборки. Минус статического расчета хеш-суммы в возможности модификации приложения уже после его запуска.

Так же существуют методы динамической самопроверки (англ. integrity veriﬁcation). В отличие от проверки статического образа приложения (файл на диске), программа сравнивает значения в памяти. Могут сравниваться значения переменных в памяти на выходе из функций, хеш-сумма последних выполненных инструкций или значений в стеке [8].

Более продвинутые метод заключается в шифровании исходного кода в памяти. Секции кода, незадействованные в текущих вычислениях могут быть зашифрованы в любое время и расшифрованы при необходимости их выполнения. Таким образом, исключается модификация кода без знания алгоритма шифрования. Данный способ можно усложнить еще больше, транслировав весь код в код виртуальной машины [9].

## Сокрытие данных

Рассмотренные ранее методы защиты помогают защитить код от кражи и модификации, позволяют отслеживать подлинность используемого ПО или противодействовать отладке, но они не помогают защитить данные приложения. Запущенное приложение в какой-то момент хранит все свои данные в оперативной памяти, откуда злоумышленник может их получить. От этого может спасти модификация данных, перед записыванием их в память. Возможных реализаций этого способа защиты существует множество, и они будут рассмотрены позже.

В ходе анализа не было найдено продуктов, предоставляющих подобную защиту, но она, несомненно, используется в готовых приложениях.

## Комплексный подход

Как уже было сказано ранее, нельзя полностью защитить приложение от взлома, можно лишь увеличить необходимые на это затраты. Сокрытие данных не придаст приложению дополнительной защиты без использования других методов, т.к. такую защиту легко снять, то же самое относится к системе лицензирования, защите от модификаций, да и любого рода проверкам.

Для эффективной защиты необходимо применять комплексный подход, который и реализован в готовых предлагаемых решениях, которые будут рассмотрены далее.

## Обзор имеющихся решений

В основном на рынке инструменты для защиты приложений представлены в виде двух групп: обфускаторы и протекторы.

На основании обзоров и анализов обфускаторов был выбран Spices.Net Obfuscator как один из лучших в данной группе, благодаря следующим возможностям:

* Неограниченная по функционалу версия для некоммерческих проектов;
* Интеграция в MSBuild и VisualStudio;
* Возможность защиты сборки от фальсификации (tamper-resistance);
* Противодействие декомпиляции;
* Запутывание данных (с противодействием подмене благодаря технологии tamper-resistance) и потока управления (технология CodeAnonymizer, запутывающая IL код без возможности восстановления);
* Оперативная поддержка на русском языке.

Из множества протекторов, работающих с .Net сборками можно выделить следующие [7]: Obsidium, Enigma Protector, Oreans Themida, .NET Reactor. Все они имеют примерно одинаковую цену ($150-200) и за исключением .NET Reactor’a схожие возможности. .NET Reactor больше ориентирован на .Net приложения и включает в себя довольно мощный обфускатор, что достаточно важно для .Net приложений с открытым исходным кодом. В нем так же предусмотрена достаточно гибкая система лицензирования.

В качестве протектора для сравнения был выбран Enigma Protector, благодаря более богатому набору функционала для защиты.

Лучшие отобранные решения будут сравниваться по описанным методам защиты приложений. Если данный метод реализован, напротив него ставится «+», если нет – «–», если информация не предоставлена – «?».

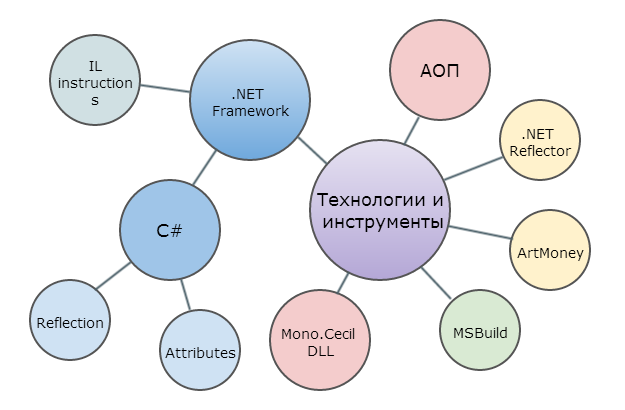
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Возможности | Spices.Net Obfuscator | .NET Reactor | Enigma Protector | Мое решение |
| Обфускация кода |  |  |  |  |
| Защита кода | + | + | + | +/– |
| Защита от дизасемблирования | + | + | – | – |
| Запутывание потока управления | + | + | – | – |
| Упаковка | – | + | + | – |
| Система лицензирования | – | + | + | – |
| **Tamper-resistant** | + | – | + | – |
| Watermarks | + | – | + | – |
| Сокрытие данных | – | – | – | + |
| Поддержка различных версий и языков .Net | + | + | ? | + |
| Цена | $400 | $180 | $150 | $0 |
|  | <http://www.9rays.net/TourStep.aspx?TourStepID=17> | <http://www.eziriz.com/dotnet_reactor.htm> | <http://enigmaprotector.com/ru/about.html> |  |

Исходя из проведенного обзора, можно сделать некоторые выводы и рекомендации. Enigma Protector предоставляет множество различных методов защиты, но можно предположить, что из-за достаточно простой обфускации, эту защиту достаточно легко снять. Spices.Net Obfuscator представляет собой очень мощный инструмент для обфускации приложений и если не нужна система лицензирования, это, пожалуй, лучший вариант. .NET Reactor – что-то среднее между двумя описанными решениями.

Но ни одно из этих решений не предоставляет инструмента для защиты данных, что так же является довольно важным элементом защиты. Этот метод защиты и будет представлен в моем решении, которое может быть использовано как часть комплексной подхода к защите приложения.

# Теоретическая разработка

В ходе разработки данного решения были использованы различные инструменты и технологии, представленные на следующем рисунке:



В данной главе рассмотрены основные моменты, примененных на практике технологий.

## Аспектно-ориентированное программирование

*Парадигма программирования* — это совокупность идей и понятий, определяющих стиль написания компьютерных программ. Это способ концептуализации, определяющий организацию вычислений и структурирование работы, выполняемой компьютером. Существуют несколько основных парадигм (моделей, концепций) программирования, вот основные из них:

* Императивное программирование:
  + Процедурное программирование;
  + Структурное программирование;
  + Объектно-ориентированное программирование (ООП);
  + Аспектно-ориентированное программирование.
* Декларативное программирование:
  + Функциональное программирование;
  + Логическое программирование;
* Метапрограммирование.

*Аспектно-ориентированное программирование* (АОП) представляет собой одну из концепций программирования, которая является дальнейшим развитием процедурного и объектно-ориентированного программирования (ООП) . Современные программы постоянно усложняются и параллельно с их усложнением, разрабатываются способы снижения сложности программного кода. Так в свое время появилось ООП и возможность выделять код с близким функционалом в отдельные классы. Но некоторую функциональность с помощью предложенных методов невозможно выделить в отдельные сущности. Это сквозная функциональность, это функциональность, необходимая в нескольких модулях системы или приложения. Соответственно ее реализация становится разбросанной по различным модулям, и сопровождение такого кода становится затруднительным, а количество потенциальных ошибок повышается. АОП предполагает наличие языковых средств, позволяющих выделять сквозную функциональность в отдельные модули. Примерами такой функциональности могут служить:

* логирование,
* обработка транзакций,
* обработка ошибок,
* авторизация и проверка прав,
* кэширование,
* элементы контрактного программирования.

С точки зрения АОП в процессе разработки достаточно сложной системы программист решает две ортогональные задачи:

* Разработка компонентов, то есть выявление классов и объектов, составляющих словарь предметной области;
* Разработка сервисов, поддерживающих взаимодействие компонентов, то есть построение структур, обеспечивающих взаимодействие объектов, при котором выполняются требования задачи.

У каждой парадигмы программирования есть свои особенности, но главным отличием является понятие основной единицы программы, например, для императивного – это инструкции, для функционального – функции, для ООП – объект, для логического – факт. В АОП такой единицей является *аспект*. Аспект (aspect) – это модуль или класс, в который вынесена основная сквозная функциональность. Аспектный модуль – это результат выявления и декомпозиции явлений, понятий и событий, применимых к группе компонентов. Но прежде чем рассматривать подробнее сущность аспектно-ориентированного подхода, необходимо дать определения и другим важнейшим средствам АОП:

* точка соединения (join point) – точка в выполняемой программе (вызов метода, создание объекта, обращение к переменной), где следует применить сквозную функциональность (совет);
* совет (advice) – дополнительная логика, код, который должен быть вызван из точки соединения. Совет может быть выполнен до, после или вместо точки соединения;
* срез (pointcut) – набор точек соединения. Срез определяет, подходит ли данная точка соединения к заданному совету;
* внедрение (introduction) – изменение структуры класса и/или изменение иерархии наследования для добавления функциональности аспекта в инородный код;
* цель (target) – объект, к которому будут применяться советы;
* переплетение, вшивание (weaving) – связывание объектов с соответствующими аспектами (возможно на этапе компиляции, загрузки или выполнения программы).

Таким образом, в аспектном модуле описываются срезы и советы, связанные с конкретными срезами.

Существуют несколько реализаций АОП, самыми известными из которых можно назвать AspectJ (Java) и PostSharp (C#). В них представлен набор конкретных срезов, т.е. мест, куда привязывается совет, например: вызов методов определенного класса, возвращающих значение определенного типа или определенное значение, принимающих определенные аргументы; все манипуляции с конкретным объектом; вызов статических методов определенного класса; выполнение точки соединения, цель которой помечена аннотацией или атрибутом.

Все эти принципы теряют свое основное преимущество без автоматической компоновки аспектных модулей с модулями программы (вшивания). Реализация автоматической компоновки во многом определяет возможности той или иной аспектно-ориентированной платформы. В настоящее время обсуждаются два подхода к интеграции аспектов:

* Статическая интеграция на этапе компиляции;
* Динамическая интеграция на этапе выполнения программы.

Основными преимуществами использования АОП являются:

* Инкапсуляция функциональности, которая не может быть представлена в отдельном модуле или функции, тем самым улучшается декомпозиция и упрощение структуры системы;
* Упрощение сопровождения программной системы и внесения в нее изменений;
* Простая возможность повторного использования кода.

Но так же аспектно-ориентированный подход пока что обладает рядом недостатков. Концепции АОП реализованы только на уровне языковых расширений, такая реализация представляется неполной и неэффективной. Различные реализации отличаются по своим возможностям и не стандартизованы.

В рамках моего проекта методология АОП была применена для внедрения функционала модификации данных (совет) для защищенного хранения в памяти в местах применения атрибутов (точка соединения) к свойствам защищаемого класса. Внедрение происходит после компиляции целевой программы путем модификации скомпилированной сборки с использованием сторонней библиотеки Mono.Cecil путем применения рефлексии (отражений) .NET Framework.

## Отражения

*Отражение* или *рефлексия* (англ. reflection) - это процесс, во время которого программа может отслеживать и модифицировать собственную структуру и поведение во время выполнения. В .NET Framework это становится возможным благодаря пространству имен System.Reflection. В этом пространстве имен имеется несколько типов, позволяющих писать код разбора таблиц метаданных. Точнее, типы из этого пространства имен предоставляют объектную модель для работы с метаданными сборки или модуля.

Метаданные – это блок двоичных данных, состоящий из набора таблиц. Метаданные хранятся в исполняемом файле непосредственно перед кодом и после PE32 и CLR заголовков. Существуют три категории таблиц: определений, ссылок и манифестов.

Основные таблицы определений включают в себя таблицы для: модуля (содержит одну запись, идентифицирующую текущий модуль), типов, методов, полей, свойств, параметров, событий (содержат по одной записи для каждой соответствующей сущности) и т.д. Для каждой сущности, определяемой в компилируемом исходном тексте, компилятор генерирует строку в одной из таблиц.

В ходе компиляции исходного текста компилятор также обнаруживает сущности, на которые имеются ссылки в исходном тексте текущего модуля. Все сведения о найденных сущностях регистрируются в нескольких таблицах ссылок, составляющих метаданные. В них же содержатся записи о других сборках, на которые ссылается модуль [12].

Типы пространства имен System.Reflection дают возможность запрашивать поля, методы, свойства и события типа путем разбора соответствующих таблиц метаданных. Можно узнать, какими атрибутами помечена та или иная сущность метаданных. Есть даже классы, позволяющие определить указанные сборки и методы и возвращающие в методе байтовый IL-поток.

В моем решении отражения используются для двух целей. Первая – это модификация целевой сборки отдельным приложением (внедрение аспекта), вторая – использование отражений в совете (внедряемом функционале). Внешнее приложение в частности модифицирует код определенных свойств (property) целевой сборки, а точнее методов доступа к этим свойствам – чтения (get) и записи (set). Внутри этих методов с помощью отражения получается текущий метод, затем он передается в класс, отвечающий за защиту данных, в нем из объекта типа MethodBase описывающего методы получается свойство, из метода которого был произведен вызов.

## Атрибуты

Атрибуты в CLR – это декларативные аннотации, наделяющие код дополнительными возможностями. Они выступают в роли определенных меток или ярлыков, привязанных к определенной сущности, такой как метод, класс, поле, свойство и т.д. Функционал атрибутов в среде .NET довольно обширный и его описание не является целью данной работы.

В CLR так же есть мощный механизм настраиваемых или пользовательских атрибутов (custom attributes). Настраиваемые атрибуты служат лишь средством передачи дополнительной информации, которая хранится в метаданных модуля. Само по себе определение атрибутов бесполезно и никак не влияет на работу программы [12].

В соответствии с методикой АОП атрибут можно назвать срезом, к которому может быть применен определенный совет. Применение атрибута в определенном месте кода программы – точка соединения.

В моей библиотеке для защиты данных определен класс SecureFieldAttribute, унаследованный от System.Attribute. Область применения этого атрибута распространяется только на свойства классов, это достигается путем применения к классу атрибута, другого атрибута AttributeUsage с параметром AttributeTargets.Property.

# Реализация

# Тестирование

# Организация рабочего места

Для работы с моим программным модулем необходима персональная электронная вычислительная машина (ПЭВМ). Существуют требования и нормы к работе за ПЭВМ . Для охраны здоровья и труда необходимо соблюдать все правила и требования, описанные в данной главе.

## Требования к помещениям для работы с ПЭВМ

* + 1. Помещения для эксплуатации ПЭВМ должны иметь естественное и искусственное освещение. Эксплуатация ПЭВМ в помещениях без естественного освещения допускается только при соответствующем обосновании и наличии положительного санитарно-эпидемиологического заключения, выданного в установленном порядке.

Естественное и искусственное освещение должно соответствовать требованиям СанПин 2.2.2/2.4.1340-03 . Окна в помещениях, где эксплуатируется вычислительная техника, преимущественно должны быть ориентированы на север и северо-восток.

Оконные проемы должны быть оборудованы регулируемыми устройствами типа: жалюзи, занавесей, внешних козырьков и др.

* + 1. Площадь на одно рабочее место пользователей ПЭВМ с ВДТ (видеодисплейные терминалы) на базе электроннолучевой трубки (ЭЛТ) должна составлять не менее 6 м2. Для ВДТ на базе плоских дискретных экранов (жидкокристаллические, плазменные) – 4,5 м2.

При использовании ПЭВМ с ВДТ на базе ЭЛТ (без вспомогательных устройств – принтер, сканер и др.), отвечающих требованиям международных стандартов безопасности компьютеров, с продолжительностью работы менее 4-х часов в день допускается минимальная площадь 4,5 м2 на одно рабочее место пользователя.

* + 1. Помещения, где размещаются рабочие места с ПЭВМ, должны быть оборудованы защитным заземлением (занулением) в соответствии с техническими требованиями по эксплуатации.
    2. Не следует размещать рабочие места с ПЭВМ вблизи силовых кабелей вводов, высоковольтных трансформаторов, технологического оборудования, создающего помехи в работе ПЭВМ.

## Требования к микроклимату, содержанию энтропинов и вредных химических веществ в воздухе

* + 1. В производственных помещениях, в которых работа с использованием ПЭВМ является вспомогательной, температура, относительная влажность и скорость движения воздуха на рабочих местах должны соответствовать действующим санитарным нормам микроклимата производственных помещений.
    2. В помещениях, оборудованных ПЭВМ, проводится ежедневная влажная уборка и систематическое проветривание после каждого часа работы на ПЭВМ.
    3. Содержание вредных химических веществ в производственных помещениях, в которых работа с использованием ПЭВМ является основной (диспетчерские, операторские, расчетные, кабины и посты управления, залы  вычислительной техники и др.), не должно превышать предельно допустимых концентраций загрязняющих веществ в атмосферном воздухе населенных мест в соответствии с действующими гигиеническими нормативами.

## Требования к уровням шума и вибрации

* + 1. В производственных помещениях при выполнении основных или вспомогательных работ с использованием ПЭВМ уровни шума на рабочих местах не должны превышать предельно допустимых значений, установленных для данных видов работ в соответствии с действующими санитарно-эпидемиологическими нормативами.
    2. При выполнении работ с использованием ПЭВМ в производственных помещениях уровень вибрации не должен превышать допустимых значений вибрации для рабочих мест в соответствии с действующими санитарно-эпидемиологическими нормативами

В помещениях всех типов образовательных и культурно-развлекательных учреждений, в которых эксплуатируются ПЭВМ, уровень вибрации не должен превышать допустимых значений для жилых и общественных зданий в соответствии с действующими санитарно-эпидемиологическими нормативами.

* + 1. Шумящее оборудование (печатающие устройства, серверы и т.п.), уровни шума которого превышают нормативные, должно размещаться вне помещений с ПЭВМ.

## Требования к освещению

* + 1. Рабочие столы следует размещать таким образом, чтобы ВДТ были ориентированы боковой стороной к световым проемам, чтобы естественный свет падал преимущественно слева.
    2. Искусственное освещение в помещениях для эксплуатации ПЭВМ должно осуществляться системой общего равномерного освещения. В производственных и административно-общественных помещениях, в случаях преимущественной работы с документами, следует применять системы комбинированного освещения (к общему освещению дополнительно устанавливаются светильники местного освещения, предназначенные для освещения зоны расположения документов).
    3. Освещенность на поверхности стола в зоне размещения рабочего документа должна быть 300 – 500 лк. Освещение не должно создавать бликов на поверхности экрана. Освещенность поверхности экрана не должна быть более 300 лк.
    4. Следует ограничивать прямую блесткость от источников освещения, при этом яркость светящихся поверхностей (окна, светильники и др.), находящихся в поле зрения, должна быть не более 200 кд/м2.
    5. Для освещения помещений с ПЭВМ следует применять светильники с зеркальными параболическими решетками, укомплектованными электронными пуско-регулирующими аппаратами (ЭПРА). Допускается использование многоламповых светильников с ЭПРА, состоящими из равного числа опережающих и отстающих ветвей.

Применение светильников без рассеивателей и экранирующих решеток не допускается. При отсутствии светильников с ЭПРА лампы многоламповых светильников или рядом расположенные светильники общего освещения следует включать на разные фазы трехфазной сети.

* + 1. Для обеспечения нормируемых значений освещенности в помещениях для использования ПЭВМ следует проводить чистку стекол оконных рам и светильников не реже двух раз в год и проводить своевременную замену перегоревших ламп.

## Требования к уровню электромагнитных полей

* + 1. Временные допустимые уровни ЭМП, создаваемых ПЭВМ на рабочих местах пользователей представлены в таблице 5.1.

Таблица 5.1

Временные допустимые уровни ЭМП, создаваемые ПЭВМ

|  |  |  |
| --- | --- | --- |
| Наименование параметров | | ВДУ ЭМП |
| Напряженность элеткрического поля | В диапозоне частот 5Гц - 2КГц | 25В/м |
| В диапозоне частот 2КГц - 400КГц | 2,5В/м |
| Плотность магнитного потока | В диапозоне частот 5Гц - 2КГц | 250нТл |
| В диапозоне частот 2КГц - 400КГц | 25нТл |
| Электростатический потенциал экрана видеомонитора | | 500В |

* + 1. Для дисплеев на ЭЛТ частота обновления изображения должна быть не менее 75 Гц при всех режимах разрешения экрана, гарантируемых нормативной документацией на конкретный тип дисплея и не менее 60 Гц для дисплеев на плоских дискретных экранах (жидкокристаллических, плазменных и т.п.).

## Требования к визуальным параметрам ВДТ

* + 1. Предельно допустимые значения визуальных параметров ВДТ, контролируемые на рабочих местах, представлены в таблице 5.2.

Таблица 5.2

Визуальные параметры ВДТ, контролируемые на рабочих местах

|  |  |
| --- | --- |
| Параметры | Допустимые значения |
| Яркость белого поля | Не менее 35кд/кв.м. |
| Неравномерность яркости рабочего поля | Не более +-20 |
| Контрастность (для монохромного режима) | Не менее 3:1 |
| Временная нестабильность изображения (мелькания) | Не должна фиксироваться |
| Пространственная нестабильность изображения (дрожание) | Не более 2х10 (-4L), где L - проектное расстояние наблюдения, мм. |

В данной главе были установлены правил безопасности по работе с моей библиотекой.

# Экономическое обоснование

За экономическую часть своего проекта я предлагаю расчет затрат, которые необходимы для разработки моего решения. В перечень затрат вошли как стоимость самой работы, так и стоимость начального материала и ресурсов.

## Определение трудоемкости выполнения разработки

Трудоёмкость характеризует затраты рабочего времени на производство определённой единицы продукции или на выполнение конкретной технологической операции.

Трудоемкость определяется методом экспертных оценок по сумме трудоемкости этапов работ, выраженных в днях. Ожидаемое время выполнения работ Тож определяется по формуле:

,

где Tmin - минимально возможное время выполнения заданной работы;

Тmах - максимально возможное время.

Основные этапы работ, которые необходимо выполнить для разработки устройства, приведены в таблице 6.1.

Таблица 6.1

Трудоемкость выполнения разработки

|  |  |  |  |
| --- | --- | --- | --- |
| Наименование этапов разработки | Tmin, дни | Тmах, дни | Тож, дни |
| Составление технического задания | 1 | 1 | 1 |
| Анализ существующих решений | 1 | 2 | 1.4 |
| Установка необходимого ПО | 2 | 3 | 2.4 |
| Разработка ПО | 15 | 20 | 17 |
| Тестирование | 3 | 5 | 3.8 |
| Написание технической документации | 10 | 15 | 12 |
| **Итого:** | **32** | **46** | **37.6** |

## Расчет затрат на разработку

Сметная стоимость затрат является основным документом, на основании которого осуществляется планирование и учет затрат на разработку устройства.

В состав сметной стоимости могут входить следующие статьи затрат:

1. Материалы, покупные изделия.
2. Специальное оборудование для проведения разработки.
3. Заработная плата разработчиков.
4. Отчисления на социальные нужды.
5. Затраты на электроэнергию для технологических целей.
6. Затраты на командировки
7. Контрагентские работы.
8. Прочие затраты.
9. Накладные расходы.

Сметная стоимость определяется методом сметного калькулирования. Метод сметного калькулирования основан на прямом определении затрат по определенным статьям.

Стоимость материалов, покупных изделий (См) оценивается по действующим рыночным ценам с учетом величины транспортно-заготовительных расходов по формуле:

,

где n – число позиций применяемых материалов;

Нмi – норма расхода материала, кг;

Цмi – цена материала, руб/кг;

Ктз – величина транспортно-заготовительных расходов.

* + 1. Затраты по статье «Материалы, покупные изделия» приведены в   
       табл. 6.2.

Таблица 6.2

Затраты по статье «Материалы, покупные изделия»

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Наименование материалов, покупных изделий и п/фабрикатов | Ед. изм. | Кол-во | Цена единицы (руб.) | Сумма (руб.) | Транспортно-заготовительные расходы | Итого матер. затрат (руб.) |
| Бумага для принтера | Пачка | 1 | 150 | 150 | 1,2 | 180 |
| Картридж для принтера | шт. | 1 | 1100 | 1100 | 1,05 | 1155 |
| **Итого:** |  | | | 1250 |  | **1335** |

Остальные использованные инструменты распространяются на основе свободной лицензии или в демо версии, которой хватает для нужд проекта.

* + 1. В качестве специального оборудования для проведения разработки использовался компьютер, балансовая стоимость которого равна **17000** рублей.
    2. Заработная плата разработчиков (Сз) рассчитывается по формуле.

,

где ЗП– заработная плата разработчика;

Кдоп – коэффициент дополнительной заработной платы;

Тож – ожидаемое время выполнения работ;

22 – количество рабочих дней в месяце.

Для текущего проекта: ЗП = 25000 руб., Кдоп = 0, Тож = 37,6 дней.

**Итого:** .

* + 1. Отчисления в социальные внебюджетные фонды определяются по формуле:

,

где *r* – суммарная величина отчислений в социальные внебюджетные фонды (26%).

* + 1. Затраты на электроэнергию, потребляемую ЭВМ, рассчитываются по следующей формуле:

,

где *W* - установленная мощность ЭВМ, кВт;

*Т* - время использования для проведения разработки, ч;

*Сk* - цена одного кВт/ч электроэнергии;

*KWi* - коэффициент использования мощности.

* + 1. Расходы на служебные командировки, а так же расходы на контрагентные работы в данной разработке не предусматриваются.
    2. Статья «Прочие затраты» в данной работе отсутствует.
    3. Накладные расходы (Сн) начисляются в процентах к основной заработной плате (90%). Величина накладных расходов:

На основании полученных данных по отдельным статьям затрат, составляем смету затрат на разработку в целом по форме, приведённой в таблице 6.3:

Таблица 6.3

Смета затрат на разработку

|  |  |  |
| --- | --- | --- |
| Статьи затрат | Условные обозначения | Затраты по статьям (руб.) |
| 1. Материалы, покупные изделия | *См* | 1 335.00 |
| 1. Специальное оборудование для проведения разработки | *Соб* | 17 000.00 |
| 1. Заработная плата разработчиков | *СЗ* | 42 727.27 |
| 1. Отчисления на социальные нужды | *Ссф* | 11 109.09 |
| 1. Затраты на электроэнергию для технологических целей | *Сэн* | 258.81 |
| 1. Затраты на командировки и | *Ском* | - |
| 1. Контрагентские работы | *Скр* | - |
| 1. Прочие затраты | *Сп* | - |
| 1. Накладные расходы | Сн | 38 454.54 |
| **Общая сметная стоимость** |  | **110 884.71** |

Итоговые сметные затраты на разработку проекта составили 110 884.71 рублей.

# Список литературы

|  |  |
| --- | --- |
| [1] | F. Z. William, «Concepts and Techniques in Software Watermarking and Obfuscation,» The Department of Computer Sciences, The University of Auckland, 08 2007. [В Интернете]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.103.8892&rep=rep1&type=pdf. [Дата обращения: 12 04 2014]. |
| [2] | C. Collberg и C. Thomborson, «Software Watermarking: Models and Dynamic Embeddings,» Department of Computer Science, The University of Auckland, 1999. [В Интернете]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.33.8088&rep=rep1&type=pdf. [Дата обращения: 12 04 2014]. |
| [3] | А. В. Чернов, «Анализ запутывающих преобразований программ,» Института Системного программирования РАН, 2003. [В Интернете]. Available: http://citforum.ru/security/articles/analysis/. [Дата обращения: 11 04 2014]. |
| [4] | С. Collberg, С. Thomborson и D. Low, «A Taxonomy of Obfuscating Transformations,» Department of Computer Science, The University of Auckland, 1997. [В Интернете]. Available: http://www.labri.fr/perso/fleury/courses/SS/download/papers/obfuscation-survey-collberg.pdf. [Дата обращения: 11 04 2014]. |
| [5] | И. Ледовских, «Метрики сложности кода,» 27 01 2012. [В Интернете]. Available: http://www.ispras.ru/ru/preprints/docs/prep\_25\_2013.pdf. [Дата обращения: 11 04 2014]. |
| [6] | eRaider, «Защита .NET приложений — всё же, во что заворачивать селёдку?,» 16 10 2010. [В Интернете]. Available: http://habrahabr.ru/post/106262/. [Дата обращения: 11 04 2014]. |
| [7] | А. Трамвон, «Обзор систем защиты ПО для Windows от нелегального использования,» 15 03 2014. [В Интернете]. Available: http://habrahabr.ru/post/215553/. [Дата обращения: 11 04 2014]. |
| [8] | P. Wang, «Tamper Resistance for Software,» Information and Communications University, 2005. [В Интернете]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.105.8556&rep=rep1&type=pdf. [Дата обращения: 12 04 2014]. |
| [9] | G. Wurster, «A generic attack on hashing-based software tamper resistance,» Ottawa-Carleton Institute for Computer Science, 04 2005. [В Интернете]. Available: http://people.scs.carleton.ca/~gwurster/publications/Thesis-2005.pdf. [Дата обращения: 12 04 2014]. |
| [10] | Antelle, «Обзор обфускаторов для .NET,» 22 06 2010. [В Интернете]. Available: http://habrahabr.ru/post/97062/. [Дата обращения: 11 04 2014]. |
| [11] | В. Павлов, «Аспектно-ориентированное программирование,» [В Интернете]. Available: http://www.online-ane.ru/oopAOP.pdf. [Дата обращения: 17 05 2014]. |
| [12] | Д. Рихтер, CLR via C#, 4-е издание ред., Питер, 2013. |
| [13] | Министерство здравоохранения РФ, «СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к ПЭВМ и организации работы»,» 30 05 2003. [В Интернете]. Available: http://www.sysengineering.ru/media/511/legislation\_02.pdf. [Дата обращения: 05 17 2014]. |