***Практическая работа № 9***

**Работа по сопровождению программного обеспечения: “обратный” инжиниринг**

*Цель работы:*научиться выполнять работы по обратному инжинирингу

*Теоретическое обоснование*

Обратный инжиниринг (Reverse engineering, Обра́тная разрабо́тка, реверс-инжиниринг; [англ.](http://dic.academic.ru/dic.nsf/ruwiki/6161) reverse engineering) — исследование некоторого устройства или программы, а также документации на них с целью понять принцип его работы и, чаще всего, воспроизвести устройство, программу или иной объект с аналогичными функциями, но без копирования как такового.

Применяется обычно в том случае, если создатель оригинального объекта не предоставил информации о структуре и способе создания (производства) объекта. Использование обратной разработки может противоречить закону об авторском праве и патентному законодательству.

“Обратный” инжиниринг (часто путаемый с реинжинирингом, в том числе, в понимании SWEBOK, прим. автора) или это процесс анализа программного обеспечения с целью идентификации программных компонент и связей между ними, а также формирования представления о программном обеспечении, с дальнейшей перестройкой в новой форме (уже, в процессе реинжиниринга).

Проще говоря, обратный инжиниринг – это анализ современного продукта, в котором исследуются детали и связь между ними, и создание нового продукта из ранее исследуемого на основе последних современных технологий

Обратный инжиниринг является пассивным, предполагая отсутствие деятельности по изменению или созданию нового программного обеспечения. К вопросам обратного инжиниринга, как и к вопросам реинжиниринга, также относятся работы по рефакторингу (см. работы Мартина Фаулера). Рефакторинг – трансформация программного обеспечения, в процессе которой программная система реорганизуется (не переписываясь) с целью улучшения структуры, без изменения поведения. Сохранение “формы” (платформы, архитектурных и технологических решений) существующей программной системы позволяет рассматривать рефакторинг как один из вариантов обратного инжиниринга.

Существуют программы, которые предоставляют как возможность восстановления (обратный, reverse) по исходному коду общего системного проекта (классы, связь между ними и т.п.), так и прямой генерации исходного кода на основе созданного проекта (функциональных блоков бизнес-процесса):  Rational Rose (фирмы Rational Software), Visual Paradigma, StarUML.

Один из типов обратного инжиниринга – создание новой документации на существующую систему (redocumentation).

Другой из распространенных типов – восстановление дизайна системы (design recovery).

Это, по сути, процесс разработки любого изделия (автомобиля, элемента механизма, информационной системы, software продукта и т.д.) в обратном порядке. То есть специалисты, анализируя имеющийся у них образец какой-либо продукции, исследуя его детали и связь между ними, проходят все стадии создания этого изделия. Такой приём даёт возможность узнать новые разработки, материалы, алгоритмы, которые использовал конкурент при создании своего изделия. Данный метод получения чужих коммерческих тайн может являться абсолютно законным при условии того, что образец был получен легально.

*Методические указания*

Для выполнения заданий вам потребуется конспект лекций, выход в Интернет.

*Задания*

* Изучите теоретический материал
* Посетите предложенные сайты и изучите расположенные там статьи, при необходимости законспектируйте:
* Reverse Engineering — <http://lurkmore.to/Reverse_Engineering>
* Реверс-инженер – это хакер, но белый и пушистый — <http://samag.ru/archive/article/2869>
* Простые приемы реверс-инжиниринга UEFI PEI-модулей на полезном примере — <https://habrahabr.ru/post/249655/>
* Реверс-инжиниринг для самых маленьких: взлом кейгена — <https://habrahabr.ru/post/220245/>
* Составьте таблицу «Виды работ при обратном инжиниринге»:

|  |  |
| --- | --- |
| Вид работы | Описание |
| … | … |

*Контрольные вопросы*

* Что такое обратный инжиниринг?
* В каких случаях он применяется?
* Какие программные средства используются при реверси-нжиниринге?
* дизассемблер?
* Что такое программа-отладчик?
* Что такое декомпилятор?

*Форма отчёта*

Конспект, таблица, ответы на контрольные вопросы.