**Обратный инжиниринг ПО**

Обра́тная разрабо́тка (обратное проектирование, обратный инжиниринг, реверс-инжиниринг;) — исследование некоторого готового устройства или программы, а также документации на него с целью понять принцип его работы; например, чтобы обнаружить недокументированные возможности, сделать изменение или воспроизвести устройство, программу или иной объект с аналогичными функциями, но без прямого копирования.

Обратный инжиниринг преследует две основные цели: повторное документирование и восстановление проектной модели. Редокументация направлена ​​на создание альтернативного представления модели на том же уровне абстракции. Восстановление модели проекта направлено на воссоздание моделей абстракции из исходного кода, существующей документации, экспертных знаний и всех других источников информации. Цель реверс-инжиниринга программного обеспечения - улучшить его общее понимание как для обслуживания, так и для будущего развития. Его анализ будет проводиться по следующим направлениям:

* работа со сложностью: создание методов и инструментов в сочетании со средами CASE для получения средств извлечения соответствующей информации;
* генерировать альтернативные представления: графические изображения считаются вспомогательными средствами понимания;
* восстановить потерянную информацию: развитие системы значительного размера приводит к потере информации, модификации обычно не документируются;
* обнаруживать краевые эффекты: первоначальный дизайн или последующие модификации могут привести к непреднамеренным краевым эффектам;
* создавать абстракции: дисциплина требует методов и инструментов для создания абстракций на более высоком уровне;
* облегчить повторное использование: обратный инжиниринг может помочь найти потенциально пригодное для повторного использования программное обеспечение.

Одним из широко известных примеров обратной разработки является исследование [BIOS](https://ru.wikipedia.org/wiki/BIOS) [персонального компьютера](https://ru.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D1%81%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80) [IBM](https://ru.wikipedia.org/wiki/IBM), ставшее серьёзным шагом на пути развития производства IBM-совместимых компьютеров сторонними производителями. Создание [сервера](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%80%D0%B2%D0%B5%D1%80_(%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D0%B5)) [Samba](https://ru.wikipedia.org/wiki/Samba) (входящего в состав ОС [GNU/Linux](https://ru.wikipedia.org/wiki/GNU/Linux) и работающего с серверами на базе ОС [Windows](https://ru.wikipedia.org/wiki/Windows)) также потребовало обратной разработки используемого [Microsoft](https://ru.wikipedia.org/wiki/Microsoft) [протокола](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D0%BF%D0%B5%D1%80%D0%B5%D0%B4%D0%B0%D1%87%D0%B8_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85) [SMB](https://ru.wikipedia.org/wiki/SMB). Создание многих [ICQ](https://ru.wikipedia.org/wiki/ICQ)-клиентов также потребовало обратной разработки [протокола](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D0%BF%D0%B5%D1%80%D0%B5%D0%B4%D0%B0%D1%87%D0%B8_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85) ICQ.

Обратная разработка программного обеспечения производится с помощью следующих методик.

1.Анализ обмена данными, наиболее распространённый в обратной разработке протоколов обмена данными, который производится с помощью [анализатора шины](https://en.wikipedia.org/wiki/Bus_analyzer) и [пакетного сниффера](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B0%D0%BB%D0%B8%D0%B7%D0%B0%D1%82%D0%BE%D1%80_%D1%82%D1%80%D0%B0%D1%84%D0%B8%D0%BA%D0%B0) для прослушивания [шины компьютера](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D0%BD%D0%B0_(%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80)) и [компьютерной сети](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C) соответственно.

2.[Дизассемблирование](https://ru.wikipedia.org/wiki/%D0%94%D0%B8%D0%B7%D0%B0%D1%81%D1%81%D0%B5%D0%BC%D0%B1%D0%BB%D0%B5%D1%80) [машинного кода](https://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D1%88%D0%B8%D0%BD%D0%BD%D1%8B%D0%B9_%D0%BA%D0%BE%D0%B4) программы для получения её [листинга](https://ru.wikipedia.org/wiki/%D0%98%D1%81%D1%85%D0%BE%D0%B4%D0%BD%D1%8B%D0%B9_%D0%BA%D0%BE%D0%B4) на [языке ассемблера](https://ru.wikipedia.org/wiki/%D0%AF%D0%B7%D1%8B%D0%BA_%D0%B0%D1%81%D1%81%D0%B5%D0%BC%D0%B1%D0%BB%D0%B5%D1%80%D0%B0). Этот способ работает на любой [компьютерной программе](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0), но требует достаточно много времени, особенно для неспециалиста.

3.[Декомпиляция](https://ru.wikipedia.org/wiki/%D0%94%D0%B5%D0%BA%D0%BE%D0%BC%D0%BF%D0%B8%D0%BB%D1%8F%D1%82%D0%BE%D1%80) машинного или [байт-кода](https://ru.wikipedia.org/wiki/%D0%91%D0%B0%D0%B9%D1%82-%D0%BA%D0%BE%D0%B4) программы для создания исходного кода на некотором [языке программирования высокого уровня](https://ru.wikipedia.org/wiki/%D0%AF%D0%B7%D1%8B%D0%BA_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F_%D0%B2%D1%8B%D1%81%D0%BE%D0%BA%D0%BE%D0%B3%D0%BE_%D1%83%D1%80%D0%BE%D0%B2%D0%BD%D1%8F).

Обратный инжиниринг является технической проблемой по нескольким причинам (неполный список):

* намерения программиста не ясны;
* исходная проблема может быть решена некорректно;
* код был изменен для удовлетворения потребностей в обслуживании;
* программное обеспечение является портом другой среды;
* аппаратная платформа изменилась или эволюционировала;
* изменилась семантика языка.