МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«МИРЭА – Российский технологический университет»
РТУ МИРЭА

Институт искусственного интеллекта
Базовая кафедра №252 – информационной безопасности

ДОКЛАД ПО ПРЕДМЕТУ «РАЗРУШАЮЩИЕ ПРОГРАММНЫЕ ВОЗДЕЙСТВИЯ»

Тема: Правовое регулирование реверс-инжиниринга.

Студент группы ККСО-01-20 *Семин В.В.*

Руководитель *Старший преподаватель*
Трошков Вадим Евгеньевич

Москва 2025

ОГЛАВЛЕНИЕ

1 ПРАВОВАЯ ОСНОВА

Критерии правомерности осуществления декомпиляции содержатся в ст. 1280 Гражданского Кодекса РФ. Согласно данной норме, проведение реинжиниринга возможно при соблюдении следующих условий:

1) Лицо, осуществляющее декомпиляцию, должно владеть ПО на законных основаниях.

Приобрести ПО, получить разрешение на его использование – это первый шаг к правомерному реверс-инжинирингу. Приобретение «пиратской» версии ПО и последующее его декомпилирование является правонарушением согласно ст. 7.12 Кодекса об административных правонарушениях РФ (КоАП РФ). Также правонарушением является использование для декомпиляции взломанных или иных испорченных версий ПО. Это подтверждает Постановление Пленума Верховного Суда РФ N 5, Пленума ВАС РФ N 29 от 26.03.2009: «Судам следует учитывать, что право совершения в отношении программы для ЭВМ или базы данных действий, предусмотренных статьей 1280 ГК РФ, принадлежит только лицу, правомерно владеющему экземпляром такой программы для ЭВМ или базы данных (пользователю)».

Правомерность владения экземпляром ПО определяется наличием у лица оснований владения, установленных договором (например, приобретение экземпляра ПО по договору купли-продажи).

2) Единственно возможная легальная цель декомпиляции – достижение способности к взаимодействию независимо разработанной лицом программы для ЭВМ с другими программами, которые, в том числе, могут взаимодействовать с декомпилируемой программой.

Изучение программы конкурента с целью создания собственной аналогичной программы, по общему правилу, будет считаться незаконным.

Также попытка устранить найденные программные ошибки самостоятельно, то есть без привлечения правообладателя, может привести к появлению ответственности

Постановление Федерального Арбитражного Суда Северо-Западного округа от 07 июня 2013 года по делу N А13-6254/2012): «Исследовав и оценив представленные лицами, участвующими в деле, доказательства по правилам статей 65 и 71 АПК РФ, в том числе заключенные Обществом в 2010-2011 годах договоры на оказание услуг по сопровождению программного обеспечения <…>, судебные инстанции установили, что внесение изменений в программное обеспечение, <…> исправление выявленных ошибок в программном обеспечении <…> без согласия правообладателя <…> приведет к нарушению исключительного права <…> на результат интеллектуальной деятельности».

3) Информация, необходимая для достижения способности программы для ЭВМ к взаимодействию, ранее не была доступна лицу, осуществляющему декомпиляцию, из других источников.

Данные об исходном тексте программы могут находиться в открытом доступе и в этом случае нет необходимости в проведении декомпиляции. Под «другими источниками» понимаются официальный интернет-сайт компании-разработчика или руководство к пользованию программой и прочее.

4) Декомпиляция не должна противоречить обычному использованию программы для ЭВМ или базы данных и не должна ущемлять необоснованным образом законные интересы автора или иного правообладателя.

На практике факт ущемления законных интересов автора или иного правообладателя устанавливается с учетом таких факторов как цель декомпиляции, конкурирование лица, осуществляющего декомпиляцию, с правообладателем, доля дохода, которая может быть утрачена правообладателем из-за действий пользователя и т.п.

Считается, что вред законным интересам правообладателя достигает необоснованного уровня, если декомпиляция его программы причиняет или имеет возможность причинить неразумные потери доходам правообладателя [1].

2 ПРЕЦЕДЕНТЫ

2.1 ДЕКОМПИЛЯЦИЯ ЗАПРЕЩЕНА ПОЛЬЗОВАТЕЛЬСКИМ СОГЛАШЕНИЕМ

Возможна ли декомпиляция в рамках, установленных статьей 1280 ГК РФ, в случаях, когда лицензионное соглашение запрещает реверс-инжиниринг вообще и декомпиляцию, в частности?

Истец (ЗАО "Интеротель") является правообладателем программы для ЭВМ «Отель — 2.3».

По мнению истца, в отсутствие лицензионного договора ответчик (ЗАО "Санаторий"Металлург") неправомерно использовал ПО.

Истец обратился в Арбитражный суд Самарской области с иском к ответчику о взыскании 2 217 402 руб[2].

Постановление Одиннадцатого арбитражного апелляционного суда от 25 октября 2012 года по делу № А55-13189/2012: «Заключение лицензионного договора означает, что пользователь программы вправе совершить в отношении нее действия, предусмотренные ст. 1280 ГК РФ, а также иные действия, обусловленные договором и связанные с эксплуатацией программы. <…> На этот договор в отличие от иных лицензионных соглашений не распространяются правила, установленные пунктами 2-6 ст. 1235 ГК РФ».

Лицензионным договором (пользовательским соглашением) нельзя ограничить лицо в праве осуществлять те действия в отношении ПО, которые предусмотрены статьей 1280 ГК РФ (в том числе и декомпиляцию). Следовательно, положения лицензионных договоров, ограничивающие права лиц на реверс-инжиниринг, не должны признаваться законными [1].

2.2 РЕИНЖЕНЕРИНГ С ЦЕЛЬЮ ЗАЩИТЫ АВТОРСКИХ ПРАВ И С ПРИВЛЕЧЕНИЕМ ТРЕТЬИХ ЛИЦ

Допустимо ли проводить реверс-инжиниринг, чтобы проверить, не является ли исследуемая программа объектом нарушения прав?

Дело № 09АП-23848/2013-ГК [3].

Решение А40-10750/2013 АС города Москвы.

Решение 09АП-18176/2014 9 арбитражный апелляционный суд.

Истец (ООО «Фирма СтройСофт») сообщил, что является правообладателем программы для ЭВМ "Smeta.ru"

Истец утверждает, что 1-й ответчик (ООО "Бюро экономического консалтинга") незаконно передал 2-му ответчику («Национальная ассоциация сметного ценообразования и стоимостного инжиниринга») ноутбук с ПО для исследования.

На основании изложенного истец обратился в суд с требованиями о взыскании 250 000 руб.

На основании сравнительного анализа базы данных второго ответчика, а также содержания приобретенной первым ответчиком у истца базы данных, работающей под управлением программного комплекса истца «Smeta.ru», становится очевидным, что приобретенная у истца база данных является переработанной (модифицированной) базой данных второго ответчика[4].

2.3 РЕИНЖЕНЕРИНГ С ЦЕЛЬЮ МОДИФИКАЦИИ ПО

Допустим ли реверс-инжиниринг с целью автоматизации и улучшения бизнес-процессов?

Подобным прецедентом стало дело № А56-92673/2016.

Спор заключался в следующем. Компания-истец (ООО "ВИАКАРД") осуществляла оказание информационно-технических услуг поставщикам топлива посредством собственного программно-аппаратного комплекса

ViaCard, состоящего из терминалов, установленных на АЗС, с программным обеспечением, позволяющим принимать микропроцессорные карты, а также программного обеспечения, осуществляющего учет произведенных транзакций. Пользователям программно-аппаратного комплекса предоставлялся ограниченный доступ в Личный кабинет системы, функционал которого позволял им проводить взаиморасчеты с клиентами, контролировать лимиты поставок, а также блокировать топливные карты.

Один из клиентов компании — ответчик (ООО "ТЕРМИНАЛ СЕРВИС") — после получения доступа к Личному кабинету системы осуществил реверс-инжиниринг и декомпиляцию системы истца, в результате чего внедрил собственное программное обеспечение, посредством которого вносил автоматизированные транзакции, а также видоизменил форму входа в Личный кабинет и, разместив ее на собственном сайте, открыл неограниченный доступ третьим лицам без необходимости ввода логина и пароля.

Договором, заключенным между сторонами, был предусмотрен запрет на реверс-инжиниринг, декомпиляцию, видоизменение программно-аппаратного комплекса, а за нарушение данного условия предусматривался штраф в размере 50 000 руб. за каждое нарушение. Выявив нарушения договорным обязательств второй стороной, истец обратился в суд с иском о взыскании договорной неустойки, а также компенсации за нарушение исключительного права и иными требованиями.

С ответчика в пользу истца была взыскан штраф за совершение реверс-инжиниринга и декомпиляцию программного обеспечения в размере 35 360 000 рублей, компенсация за нарушение исключительного права на программу для ЭВМ в размере 5 000 000 рублей, штраф за разглашение конфиденциальной информации в размере 400 000 рублей, убытки в размере 1 030 000 рублей и иные расходы, а также возвратить истцу используемые терминалы.

Суд по интеллектуальным правам подтвердил, что ответчик обязан выплатить истцу компенсацию за нарушение исключительного права на систему из базы данных, интерфейса и программы для ЭВМ, установленную на терминалах для оплаты топлива по картам АЗС, а также заплатить штраф за реверс-инжиниринг и декомпиляцию системы [5, 6].

3 ВОЗМОЖНЫЕ ПУТИ РАЗВИТИЯ ЗАКОНОДАТЕЛЬСТВА В ОБЛАСТИ РЕВЕРС-ИНЖИНИРИНГА

3.1 ИСПОЛЬЗОВАНИЕ РЕВЕРС-ИНЖИНИРИНГА ДЛЯ ИМПОРТОЗАМЕЩЕНИЯ

В условиях санкционного давления и ограниченного доступа к иностранным технологиям, реверс-инжиниринг становится важным инструментом для воспроизводства и адаптации зарубежных решений. Это особенно актуально в машиностроении и других отраслях, где требуется замена иностранных компонентов . Возможно, законодательство будет адаптировано для поддержки таких инициатив.

3.2 РАЗГРАНИЧЕНИЕ ЦЕЛЕЙ РЕВЕРС-ИНЖИНИРИНГА

В настоящее время российское законодательство не делает различий между реверс-инжинирингом с целью обеспечения совместимости, исследования безопасности или создания пиратских копий. В будущем возможно введение более чёткой дифференциации, что позволит легализовать добросовестные практики и одновременно пресекать злоупотребления.

3.3 РЕВЕРС-ИНЖИНИРИНГ В ЦЕЛЯХ ВОССТАНОВЛЕНИЯ РАБОТОСПОСОБНОСТИ

Реверс-инжиниринг для восстановления работоспособности ПО или устройства может возникнуть в ситуациях, когда продукт больше не поддерживается вендором или когда разработчик прекращает предоставление обновлений или технической поддержки. В таких случаях, владельцы программного обеспечения или аппаратных устройств могут столкнуться с проблемой, что они больше не могут использовать продукт, так как не имеют доступа к его исходному коду, спецификациям или другим данным, необходимым для его модификации и обновления.

В таких случаях может возникнуть необходимость в реверс-инжиниринге с целью восстановления или продолжения использования устройства или ПО, при этом человек не нарушает авторские права или лицензионные

соглашения с целью создания копий для продажи или распространения. Однако текущие законодательные рамки в России, как правило, не предоставляют четкого разрешения на такие действия.

3.4 ПОВЫШЕНИЕ ЗНАЧЕНИЯ РЕВЕРС-ИНЖИНИРИНГА В УГОЛОВНО-ПРОЦЕССУАЛЬНОЙ И СЛЕДСТВЕННОЙ ПРАКТИКЕ

Реверс-инжиниринг в уголовно-процессуальной практике играет ключевую роль в расследовании киберпреступлений и других преступлений, связанных с высокими технологиями. Этот метод используется для анализа программного обеспечения, восстановления данных, выявления скрытых данных и изучения вредоносных программ. Например, при расследованиях, связанных с программами-вымогателями, реверс-инжиниринг позволяет восстановить зашифрованные данные и выявить механизмы шифрования, что помогает собрать доказательства преступной деятельности.

Особое значение реверс-инжиниринг приобретает в судебной экспертизе, где специалисты проводят анализ цифровых доказательств, таких как фальшивое ПО, кибершпионские программы или вредоносные вирусы. Экспертные заключения на основе реверс-инжиниринга становятся важной частью доказательной базы в уголовных делах, связанных с преступлениями в сфере высоких технологий.

Несмотря на важность реверс-инжиниринга в расследованиях, в российской правовой системе существуют ограничения, связанные с нарушением авторских прав. Однако для следственных органов предусмотрены исключения, что позволяет использовать реверс-инжиниринг в рамках расследований. В будущем роль этого метода в расследованиях будет только расти, что потребует от правоохранителей повышения квалификации и разработки новых законодательных норм.

СПИСОК ЛИТЕРАТУРЫ

1) Нечаев А., Андрусова А. Реверс-инжиниринг: правовое регулирование. [Электронный ресурс] Режим доступа: https://blog.lch.legal/tproduct/388828150-789941865161-revers-inzhiniring-pravovoe-regulirovani (Дата доступа 16.02.2025).
2) 11АП-12337/2012 А55-13189/2012. Картотека арбитражных дел. [Электронный ресурс] Режим доступа: https://kad.arbitr.ru/Card/653960fe-1b3e-4d30-a23a-2d21117bc9e3 (Дата доступа 17.04.2025).
3) Доротенко Д. Право на реверс. Как обратная разработка выглядит с юридической точки зрения. [Электронный ресурс] Режим доступа: https://xakep.ru/2016/09/02/reverse-rights/ (Дата доступа 16.02.2025).
4) С01-207/2013 09АП-23848/2013 А40-10750/2013. Картотека арбитражных дел. [Электронный ресурс] Режим доступа: https://kad.arbitr.ru/Card/ed79a69b-b30d-4a67-873d-b2415de7a43f (Дата доступа 17.04.2025).
5) Реверс-инжиниринг ПО в условиях санкций: копировать нельзя простаивать. Где российскому бизнесу поставить запятую? [Электронный ресурс] Режим доступа: https://habr.com/ru/companies/onlinepatent/articles/741032/ (Дата доступа 17.04.2025).
6) 307-ЭС18-26218 С01-843/2018 13АП-27032/2017 А56-92673/2016. Картотека арбитражных дел. [Электронный ресурс] Режим доступа: https://kad.arbitr.ru/Card/f5603047-72db-4d96-a9a2-2ccf2bc67061 (Дата доступа 17.04.2025).