**Министерство образования и науки**

**Днепропетровский Национальный Университет**

**имени Олеся Гончара**

**Лабораторная работа №4**

по курсу «Операционные системы

и системное программирование»

выполнил студентк группы ПК-15-1

Гулый Т.О.

проверил доцент

Зайцев В.Г.

**Днепропетровск -2015 г.**

# Понятие песочницы. Установка песочници.

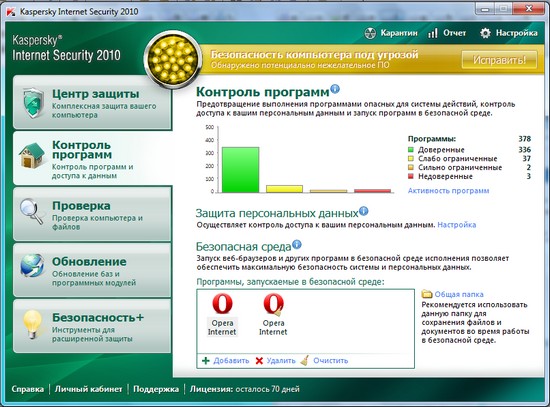
В последнее время кибер-преступники стали столь изобретательны, что сообщения о вирусных эпидемиях не вызывают удивления и стали, в общем, привычными. Однако увидеть новость о распространении нового трояна на 3DNews это одно, а обнаружить этот самый троян на своем компьютере - совсем другое. В Интернете можно найти множество советов относительно того, как не стать жертвой мошенников: от использования современных версий ПО, в которых закрыты все известные уязвимости, и до наличия на компьютере надежного современного решения для обеспечения безопасности.

Однако в некоторых случаях от заражения пользователя не спасает даже самый надежный брандмауэр и самый глазастый антивирус. Это происходит тогда, когда программа, защищающая компьютер, не уверена во вредоносном действии запускаемого приложения или выполняемого на веб-странице скрипта, вследствие чего оставляет решение о разрешении действия за пользователем. Вы вполне можете решить, что антивирус излишне подозрителен или просто, задумавшись, щелкнуть мышкой по кнопке "ОК", тем самым разрешив исполнение вредоносного кода.

Что же делать? Неужели из-за возможности подхватить троян, лучше не запускать новые приложения, а от веб-серфинга и вовсе отказаться? Существует прекрасное решение, которое для многих может стать отличным дополнением ко всем средствам для защиты компьютера от проникновения вредителей. Речь идет о работе с приложениями в "песочнице".

"Песочница" представляет собой изолированную среду, для которой отводится небольшое пространство на жестком диске и которая никак не зависит от  реальной операционной системы. При запуске программы в "песочнице" она работает так же, как обычное приложение, однако не может влиять на любые компоненты системы, которые находятся вне изолированной среды. Это значит, что из "песочницы" невозможно внести изменения в системный реестр, заменить системные файлы или выполнить любые другие действия, которые могут повлиять на стабильность работы системы. Благодаря этому "песочницу" можно использовать для безопасной работы в Интернете и для запуска неизвестных приложений. Такой изолированной среде можно найти и другие применения – например, программисты и тестеры могут запускать в ней нестабильные версии программ.

## "Песочница" в Kaspersky Internet Security 2010

О том, что работа с приложениями в "песочнице" может пригодиться самому широкому кругу пользователей, говорит хотя бы то, что соответствующая возможность в прошлом году появилась в программе Kaspersky Internet Security. Пользователи этого пакета для обеспечения безопасности могут работать с подозрительными приложениями в изолированной среде, если откроют их посредством пункта контекстного меню Windows "Запустить в безопасной среде". Для наглядности окно программы, запущенной в изолированной среде, будет обведено зеленой рамкой.

Kaspersky Internet Security также позволяет составить список программ, работа с которыми может быть потенциально опасна (в него можно включить, например, браузер).  Для этого в настройках приложения необходимо открыть раздел "Контроль программ" и при помощи кнопки "Добавить" внести программу в список. Если после этого открыть программу из окна Kaspersky Internet Security, она будет работать в изолированной среде. Подобную функцию удобно использовать, скажем, в том случае, если во время сессии в браузере вы планируете посещать сайты, которые могут содержать подозрительный код. Кроме этого, такая функция может стать хорошей заменой режиму приватности, который появился в последних версиях популярных браузеров.

Стоит, однако, заметить, что Kaspersky Internet Security предоставляет лишь самые базовые возможности запуска программ в "песочнице". Специализированные приложения имеют гораздо больше возможностей. Рассмотрим некоторые популярные программы, предназначенные для работы в изолированной среде.

## Sandboxie 3.44

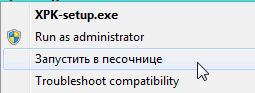
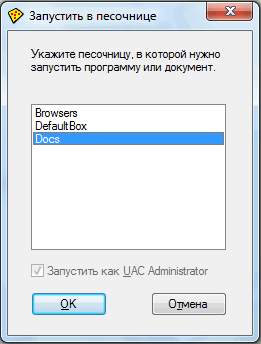
Разработчик: [Ronen Tzur](http://www.sandboxie.com/" \t "_blank)

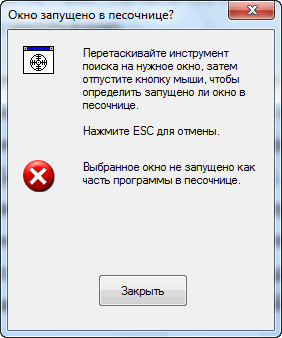
Размер дистрибутива: 1,6 Мб

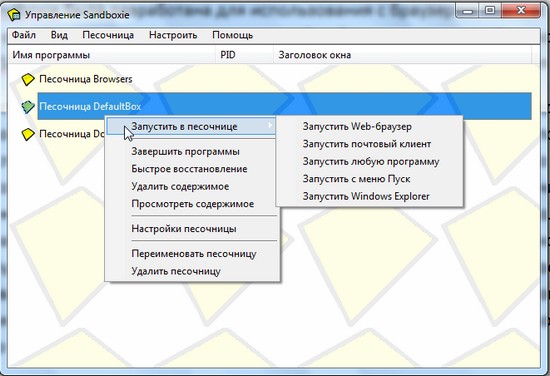
Распространение: shareware

Русский интерфейс: есть

Sandboxie это, вне всякого сомнения, самое известное решение для организации "песочницы". В программе используется классический метод защиты указанное пользователем приложение помещается в изолированную среду, в результате чего оно не может влиять на работу системы. Интересно, что Sandboxie была разработана для использования с браузером Internet Explorer, который является одной из самых популярных мишеней кибер-преступников. Однако в настоящее время Sandboxie может работать практически с любым приложением Windows.

Одна из особенностей Sandboxie, которая отличает ее от многих других программ подобной плана, возможность создания неограниченного количества "песочниц". При этом пользователь может составить список приложений, которые будут запускаться в каждой из них. По умолчанию программа сама создает "песочницу" под названием DefaultBox, поэтому можно начинать работу с Sandboxie сразу же после установки. Для открытия программы или документа в изолированной среде нужно выбрать команду "Запустить в песочнице", которая появляется в контекстном меню Windows.

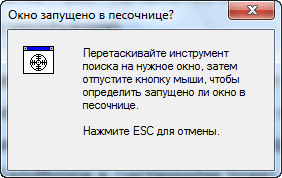
Если в будущем вы создадите дополнительные "песочницы", можно попросить программу открывать файлы и приложения не в DefaultBox, а в другой изолированной среде. Для этого выберите в меню "Пуск" пункт "Начальное меню Sandboxie" и измените "песочницу", которая будет использоваться по умолчанию.

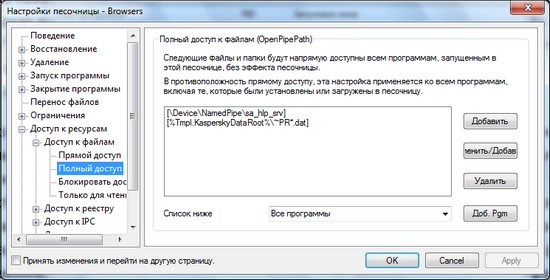
Запускать приложения в изолированной среде можно не только из контекстного меню, но и непосредственно из окна Sandboxie. Для этого нужно щелкнуть правой кнопкой мыши по названию "песочницы" и выбрать соответствующую команду (данное меню доступно и при щелчке по значку Sandboxie в системном трее).

Кстати, для ускорения выбора можно использовать команды "Запустить Web-браузер" и "Запустить почтовый клиент", которые открывают приложения, установленные в системе по умолчанию. Используя контекстное меню "песочниц", можно выполнять и другие команды, например, одним щелчком мыши закрывать все приложения, запущенные в изолированной среде, просматривать содержимое "песочниц" или полностью удалять его.

Для того чтобы быстро идентифицировать программу, которая запущена в изолированной среде, в Sandboxie предусмотрена специальная команда "Окно в песочнице?", при выборе которой на экране появляется специальный прицел, перетащив который на нужное окно, можно получить информацию о статусе программы.

Впрочем, если "песочница" работает с параметрами по умолчанию, то этот инструмент не нужен, так как возле названия приложения в заголовке появляется значок [#]. Если по каким-то причинам показ значка в заголовке нужно отключить, это можно сделать в настройках "песочницы". Кроме этого, можно добавить в заголовок окна название "песочницы", а также нарисовать вокруг окна тонкую рамку любого цвета, которая поможет более наглядно определить принадлежность к ней.

Обратившись к другим параметрам "песочницы", можно гибко настроить разрешения на доступ к разным ресурсам. Так, можно определить, к каким файлам и папкам будет заблокирован доступ, к каким программы смогут обращаться только для чтения, а также настроить взаимодействие с ключами системного реестра.



При необходимости в настройках "песочницы" можно указать приложения, которые будут форсировано запускаться в ней. Иными словами, при запуске указанного файла Sandboxie будет перехватывать приложение и не давать ему работать в обычном режиме. Программа позволяет указать не только отдельные исполняемые файлы, но и папки, при запуске любых приложений из которых они будут открываться в безопасной среде. Последнюю возможность можно, например, использовать для запуска новых программ, которые были скачаны из Интернета в папку Downloads.

## https://3dnews.ru/assets/external/illustrations/2010/07/20/595418/9.gifBufferZone Pro 3.31

Разработчик: [Trustware](http://www.trustware.com/" \t "_blank)

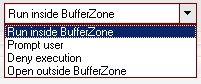
Размер дистрибутива: 9,2 Мб

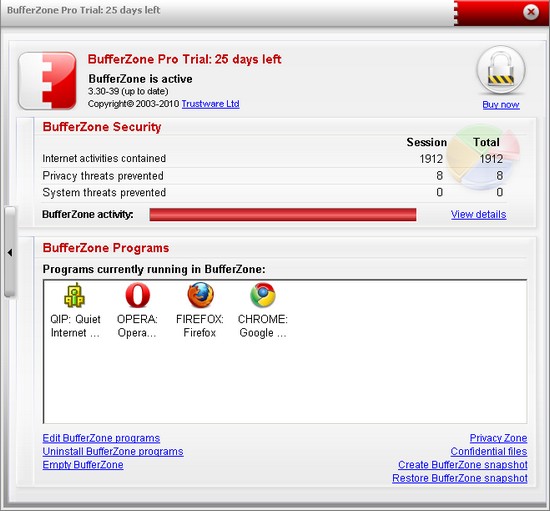
Распространение: shareware

Русский интерфейс: нет

BufferZone Pro – это еще одно хорошее решение для работы с приложениями в изолированной среде. Несмотря на то, что с помощью программы можно запускать в "песочнице" самые разные приложения, она предназначена, прежде всего, для работы с браузерами, IM-клиентами, программами для обмена файлами через пиринговые сети и другим ПО для Интернета. Об этом говорит хотя бы то, что в  BufferZone изначально имеется достаточно обширный список приложений, которые по умолчанию запускаются в безопасном режиме. Среди них Mozilla Firefox, Google Chrome, ICQ, BitComet, Skype, GoogleTalk и другие. Пользователь может редактировать этот список по своему усмотрению, добавляя в него дополнительные программы и удаляя ненужные.

Подобно рассмотренной выше утилите, BufferZone может отслеживать все приложения, которые запускаются на компьютере, и перенаправлять их в "песочницу". Также BufferZone может блокировать запуск любых неизвестных программ.

В отличие от Sandboxie, в этой программе не предусмотрено возможности создания нескольких "песочниц". Окна всех программ, которые запущены в "песочнице", обводятся красной рамкой. Увидеть, какие программы в данный момент работают в изолированной среде, можно также в главном окне BufferZone. Тут же отображается краткая статистика о работе программ в изолированной среде. BufferZone не только подсчитывает, сколько действий всего было произведено такими приложениями, но и ведет учет потенциально опасных операций в системе, а также угроз, относящихся к безопасности, которые удалось предотвратить.

В том случае, если программа, работающая в "песочнице", выполнила вредоносный код или другое деструктивное действие, можно быстро удалить все данные, относящиеся к приложениям, запущенным в изолированной среде. Кроме этого, предусмотрена возможность автоматической очистки таких данных согласно составленному пользователем расписанию.

В BufferZone есть и некоторые дополнительные возможности, которые не имеют непосредственного отношения к организации "песочнице", однако помогают повысить общий уровень безопасности компьютера. Так, при помощи программы можно запретить открытие файлов с внешних жестких дисков, DVD-дисков и с USB-накопителей или разрешить работу с такими данными только в изолированной среде.

В заключение отметим, что помимо платной версии BufferZone Pro имеется также бесплатная редакция программы. В ней реализован ряд ограничений, например, нет возможности создания снимка виртуальной среды и восстановления сохраненных в ней данных. Кроме этого, в бесплатной версии меньше приложений, для которых защита включена по умолчанию.

## Заключение

Выбирая специализированную программу для запуска приложений в "песочнице", нужно иметь в виду, что существует два основных подхода к организации изолированной среды. В первом случае "песочница" создается для указанных пользователем приложений, и во время одной сессии работы за компьютером он использует и такие программы, которые запущены в изолированной среде, и такие, которые работают в обычном режиме. Программы, в которых используется такой подход к организации защиты системы, были рассмотрены в этой статье.

Однако такое решение приемлемо не всегда. Существует второй подход к организации работы ПО в изолированной среде, который подразумевает создание "песочницы" размером с целую операционную систему. При этом создается образ работающей системы, после чего пользователь начинает работать именно с ним, а не с реальной средой. Все произведенные им действия сохраняются только до перезагрузки, а после того, как она выполнена, система возвращается в исходное состояние. Такое решение удобно использовать на общественных ПК, например, в интернет-кафе, в компьютерных классах и т.д. О программах, при помощи которых можно организовать такую защиту, мы расскажем во второй части статьи.

# Понятие виртуальной машины. Создание собственной виртуальной системы

Иногда возникает необходимость получить второй компьютер, на котором можно установить другую операционную систему или безопасно протестировать программы. С этой задачей Вам поможет справиться виртуальная машина. В этой статье мы рассмотрим, что такое виртуальная машина, зачем нужна виртуальная машина, как установить и настроить виртуальную машину.

**Виртуальная машина** – программа, которая эмулирует реальный (физический) компьютер со всем его компонентами (жёсткий диск, привод, BIOS, сетевые адаптеры и т.д.). На такой виртуальный компьютер можно установить операционную систему, драйверы, программы и т.д. Таким образом, Вы можете запустить на своем реальном компьютере  еще несколько виртуальных компьютеров, с такой же или другой операционной системой. Вы можете без проблем осуществить обмен данными между Вашим реальным и виртуальным компьютером.

## Зачем нужна виртуальная машина

Не каждому пользователя ПК нужна виртуальная машина, но продвинутые пользователи довольно часто используют ее.  Виртуальную машину используют для различных целей и задач:

Установка второй/другой операционной системы;

Тестирование программного обеспечения;

Безопасный запуск подозрительных программ;

Эмуляция компьютерной сети;

Запуск приложений, которые нельзя запустить из Вашей операционной системы.

Для наглядности приведу несколько примеров.

На Вашем реальном компьютер может быть установлена операционная система Windows 7, а на виртуальную машину можно поставить Windows XP, Windows 8 или Linux.

Если Вам нужно выбрать программу (например, видео плеер) Вам нужно установить несколько подобных программ, и определить какая из них Вам больше нравится. Что бы ни захламлять Ваш компьютер, протестируйте программы на виртуальной машине.

Я часто использую виртуальную машину, когда пишу статью на сайт. Перед тем как написать материал, я лично все проверяю. Когда я провожу обзор программного обеспечения, мне приходится устанавливать много различных программ, от чего появляется лишний мусор в системе. Да и неудачное шифрование или  скрытие данных могут повлечь неприятные последствия. Уж лучше обезопасить себя и экспериментировать на виртуальном компьютере.

## Обзор виртуальных машин

Существует большое количество различных программ для создания и управления виртуальными компьютерами. Сейчас мы рассмотрим 3 самые популярные программы.

**Виртуальная машина VirtualBox**

**VirtualBox** – бесплатная виртуальная машина, на которую можно установить все самые популярные операционные системы.  VirtualBox поддерживает работу с Windows, Linux, FreeBSD, Mac OS.

VirtualBox поддерживает как 32 так и 64 разрядные версии операционных систем.  VirtualBox поддерживает работу с виртуальными компьютерами, созданными в платной программе VMware Workstation.

Настройка и работа с VirtualBox очень удобная и простая. Программа довольна производительна и стабильна.

VirtualBox обладает широким функционалом, удельным интерфейсом и она совершенно бесплатна. VirtualBox лучшая виртуальная машина для использования дома.

**Виртуальная машина VMware**

**VMware –** наиболее известная и распространенная виртуальная машина. VMware как правило используют для работы крупные площадки или корпорации.

VMware поставляется в двух видах: Workstation и Player. VMware Workstation отличная, но платная виртуальная машина. VMware Player – бесплатная урезанная версия VMware Workstation.

VMware Workstation поддерживает работу с 32 и 64 битными системами, USB 3.0, установку различных операционных систем.

VMware Workstation безусловно лучшая виртуальная машина, которой пользуются крупные компании, но ее стоимость снижает ее популярность среди рядовых пользователей.

**Виртуальная машина Microsoft Virtual PC**

**Microsoft Virtual PC** – еще одна бесплатная виртуальная машина. Она обладает широким функционалом и удобным интерфейсом, но у нее есть один большой недостаток – она работает только с операционными системами Windows. На ней нельзя запустить Linux или Mac OS.

Подведя итог, хотелось бы отметить, что для домашнего использования лучше всего подходит VirtualBox. Далее мы рассмотрим, как установить и настроить виртуальную машину VirtualBox.

## Установка виртуальной машины VirtualBox

Из рассмотренных в предыдущем разделе виртуальных машин, лучше всего использовать VirtualBox. Сейчас мы рассмотрим, как установить VirtualBox, а в следующем разделе будет описана ее настройка.

Скачиваем свежую версию программы с официального сайта.

Запускаем инсталлятор и видим приветственное окно.  Переходим на следующий этап.

На втором этапе установки можно увидеть все компоненты программы, которые будут установлены и директория, в которую будет установлена программа. Директорию для установки Вы можете поменять, а вот компоненты я рекомендую устанавливать все. Может не все компоненты нужны Вам сейчас, но если в будущем они Вам понадобится, то нужно снова устанавливать виртуальную машину. Идем дальше.

Тут нужно отметить, куда Вы хотите поместить ярлыки программы.

На следующем этапе появится предупреждение, что во время установки произойдет временное отключение Вашего компьютера от сети. Если Вы скачиваете что то важное из интернета, то дождитесь окончания загрузки и только потом нажмите кнопку “Yes” в окне установки.

Затем Вам скажут, что если Вы готовы начать установку, то нажмите кнопку “Install”, а если хотите изменить какие-либо параметры, то вернитесь назад. Жмем “Install” и ждем, когда завершится установка.

В процессе установки могут появляться всплывающие окна, с надписью “Установить программное обеспечение для данного устройства?” Жмем кнопку  “Установить”.

Установка окончена. Нажимаем кнопку “Finish”. Виртуальная машина автоматически запуститься после окончания установки.

Переходим к созданию и настройке.

## Создание виртуальной машины VirtualBox

Что бы создать виртуальную машину нужно в окне программы VirtualBox нажать на кнопку “Создать” (в левом верхнем углу).

На первом этапе нужно ввести имя создаваемой машины  и выбрать тип операционной системы. Мы для примера создадим виртуальную машину с операционной системой Windows 7. Идем дальше.

На втором этапе необходимо установить количество оперативной памяти, которая будет выделена для виртуальной машины. Выбирать нужно исходя из потребностей операционной системы. В системных требованиях к Windows 7 указано, что нужно не менее одного гигабайта оперативной памяти. Я указал 1,5 ГБ. Для Windows XP нужно меньше оперативной памяти. В общем берем минимум, который указан в характеристиках операционной системы + небольшой запас. При этом учтите, что нельзя давать виртуальной машине более половины оперативной памяти компьютера, конечно если у Вас не очень мощный компьютер у которого 8 и более гигабайт оперативной памяти.

К виртуальной машине можно подключить виртуальный жесткий диск. Давайте создадим его. Отмечаем пункт “Создать новый виртуальный жесткий диск” и нажимаем на кнопку “Создать”.

Теперь нужно указать тип жесткого диска. Если Вы не знаете форматов, которые там описаны, оставляем как есть и нажимаем “Next” .

Далее нужно указать формат хранения данных на виртуальном жестком диске. Динамический виртуальный жесткий диск может расширятся, а фиксированный имеет строго определенный размер. Смотрите, как Вам будет удобнее.

Указываем имя виртуального жесткого диска и его размер. Нажимаем “Создать”.

## Настройка виртуальной машины VirtualBox

Познакомимся с настройками виртуальной машины. Нажмите кнопку “Настроить” в левом верхнем углу программы.

Появится окно настроек. С помощью изменения настроек Вы можете изменить  различные параметры виртуальной машины (например, количество оперативной памяти, порядок загрузки устройств, включение 2D-ускорения и т.д.)

Все настройки разделены на несколько разделов. В текущей версии программы 9 разделов. Мы не будем рассматривать подробно каждый раздел. Зрительно Вы гораздо быстрее освоите настройки, чем читая лишний текст. При этом, наведя на любой пункт настроек появится окошко, в котором будет описано зачем нужен тот или иной параметр. Я кратко опишу, какие функции можно найти в каждом разделе.

Основные настройки по разделам:

Общее – имя машины, тип ОС, буфер обмена, сменные носители;

Система – Основные настройки аппаратного обеспечения виртуальной машины: оперативная память, чипсет, процессор, ускорение, порядок загрузки устройств;

Дисплей – Настройки видеопамяти, количество мониторов, 2D и 3D ускорение, подключение к удаленному дисплею, захват видео;

Носители – Контроллеры жестких дисков и их настройка;

Аудио – аудиодрайвер и контроллер;

Сеть – настройка сетевых адаптеров;

Com-порты – включение и настройка COM-портов;

USB – Включение контроллера USB и настройка USB – фильтров;

Общие папки – создание и управление общими папками.

Если Вы ошибетесь в настройках — программа проинформирует Вас об этом. В низу окна настроек появится надпись “Обнаружены неправильные настройки”. Наведя курсор на знак восклицания, Вы увидите всплывающую панель, в которой узнаете, что сделали не так и как это можно исправить.

Обычному пользователю достаточно первых 3 разделов настроек. Если виртуальная машина будет работать медленно, то можно увеличить объем оперативной памяти или задействовать большую мощь процессора.

Завершив настройки, нажимаем кнопку “ОК”. Что бы запустить (включить) созданную виртуальную машину нужно нажать на кнопку “Запустить”. Теперь вставляем в привод установочной диск с операционной системой, устанавливаем и настраиваем операционную систему и Ваш виртуальный компьютер готов к использованию.

## Заключение

В этой статье мы рассмотрели, что такое виртуальная машина, зачем она нужна, как установить и настроить виртуальную машину. Установка и настройка виртуальной машины не составляет большого труда.

# Понятие портативного приложения. Создание своего портативного приложения установка.

Портативные приложения становятся все более популярными, но что такое портативное приложение и что его делает таковым? Почему некоторые программы не являются портативными? И почему их портативные версии, порой, можно найти только на сторонних источниках? Это руководство предназначено для объяснения некоторые принципиальных аспектов и ответов на эти и другие вопросы.

## Что означает портативное приложение?

Портативные программы - это приложения, которые будут полностью функционировать, без их установки на вашем компьютере. Другими словами, вам достаточно скопировать такое приложение в любой каталог, а затем запустить его. В отличии от других программ, такие приложения не хранят свои настройки или параметры в реестре Windows и не привязываются к определенной системе каким-либо образом.

## На основе выполнения каких критериев приложение считается портативным?

Приложение считается портативным, если выполняются следующие критерии:

* Приложение запустится без предварительной установки на компьютер.
* Приложение может запускаться с любых носителей, включая съемные устройства хранения данных, такие как флеш-накопители (usb-диски и т.д.), CD и DVD диски. Это позволяет беспрепятственно использовать их на нескольких компьютерах.
* Все созданные программой настройки хранятся рядом с программой (в том же каталоге, подкаталоге и т.д.), что позволяет легко переносить их вместе с программой. Если приложение использует реестр Windows для хранения настроек и конфигурации, то такое приложение не является портативным, так как оно зависит от конкретного компьютера.
* После своего выполнения программа оставляет нулевой след (или почти нулевой) на любом компьютере. Это означает, что временные файлы и настройки реестра должны удаляться, как только программа завершает свое выполнение. Так же это означает, что все файлы, созданные пользователем в рамках использования программы должны быть легко переносимы.

## Почему некоторые приложения являются портативными, а другие нет?

Некоторые программы написаны таким образом, что они нуждаются в определенных файлах и компонентах операционной системы для корректного запуска. Эти программы так же могут изменять файлы и компоненты операционной системы в процессе установки. Кроме того, программы могут хранить настройки пользователя и свою конфигурацию в разных местах Windows. Чаще всего, речь идет о реестре Windows. Это означает, что для их запуска необходимы определенные файлы в системе и/или наличие каких-либо ключей в реестре. И поэтому, просто так перенести их с одного компьютера на другой не представляется возможным.

Портативные приложения, как и следует из критериев в предыдущем пункте, обходят эти ограничения, за счет хранения всех настроек и файлов в той же директории, где хранятся сами программы. Безусловно, портативные приложения так же могут использовать файлы и компоненты операционной системы, но только те, которые являются общими для всех компьютеров. Это означает, что для того, чтобы приложение корректно запустилось, достаточно его открыть из любого места на любом компьютере (с оговоркой на поддержку версий Windows и соответствия техническим требованиям).

## Почему на стороннем ресурсе можно встретить ссылку для загрузки портативной версии непортативной версии?

Некоторые технические специалисты находят способы изменить приложения таким образом, что бы обойти ограничения программ. Другими словами, модифицируют программу таким образом, чтобы все необходимые файлы всегда находились в том же каталоге, что и приложение, и чтобы все настройки программы, включая пользовательские настройки, так же хранились в файлах рядом с программой. Таким образом, освобождая программу от привязки к конкретном у компьютеру. В последствие, такие программы можно использовать из любого места.

Однако, часто, такие модификации делаются другими людьми, а не самими разработчиками программ, поэтому ссылки для загрузки и сами портативные версии программ располагаются на сторонних ресурсах.

## Какие преимущества дает использование портативных приложений?

С того времени, как появились недорогие устройства, позволяющие хранить достаточно много данных (флешки и переносные диски), возможностей для портативных программ стало гораздо больше. Так что если вы используете далеко не один компьютер, то, с помощью портативных версий приложений и переносного устройства для хранения данных, вы сможете продолжать заниматься своими делами на почти любом компьютере, без каких-либо предварительных действий с вашей стороны. Кроме того, при использовании портативных программ, вам не нужно тратить время на установку и не нужно беспокоиться о том, как быстро перенести настройки.

Так же из портативных программ часто составляется инструментарий вида "на всякий случай", который можно оперативно использовать, при необходимости (возникновение срочных задач, исправление ошибок и так далее). Например, если вы загружаетесь с LiveCD, то, часто, установить программу просто не представляется возможным (конечно, иногда есть исключения, но, обычно, это исключения) и поэтому без такого инструментария просто не обойтись.

## Существуют какие-либо риски в использовании портативных программ?

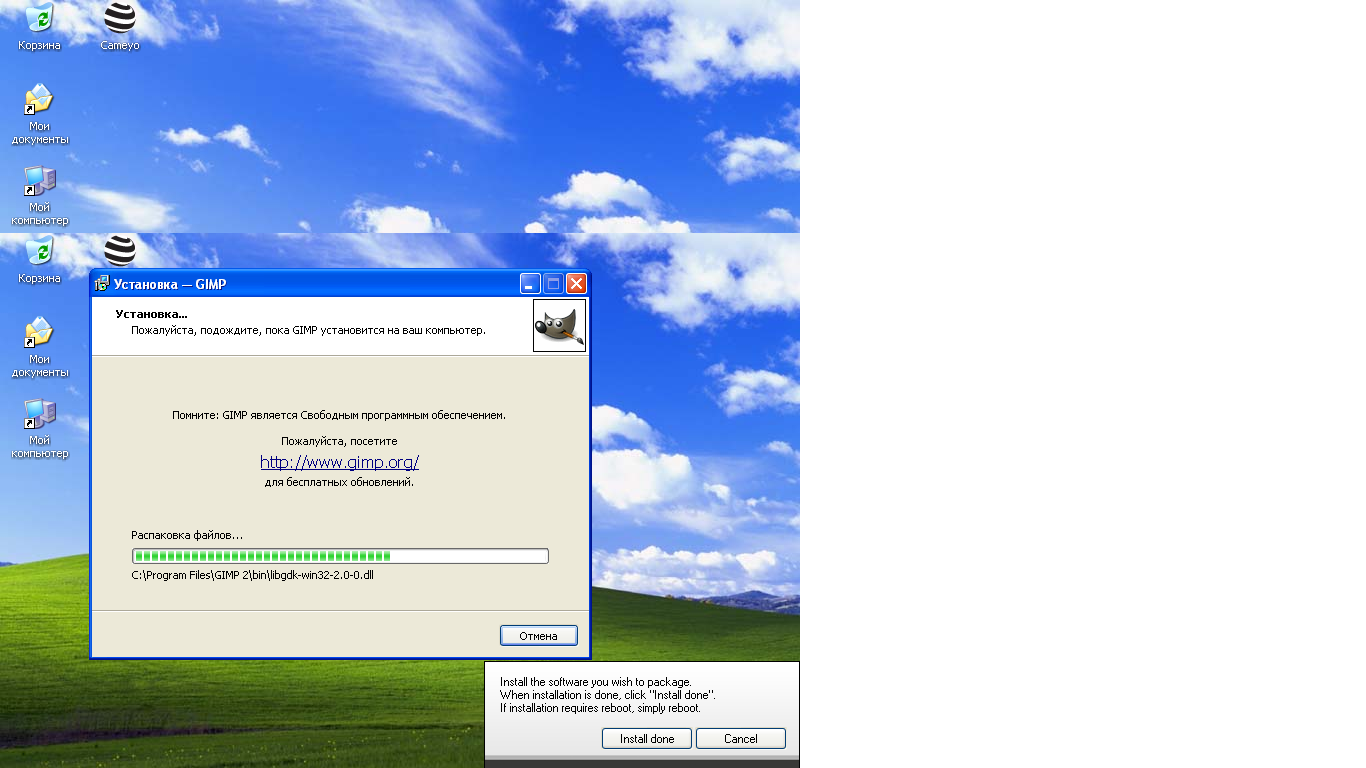
Сами по себе портативные приложения не представляют опасности, так как это те же приложения, только модифицированные так, чтобы данные хранились не в системе, а в локальном каталоге программы. Так что риски по большей части заключаются в особенности их использования, надежности источников портативных версий и предъявляемых системных требований. В первом случае, речь идет о том, что все ваши данные собраны в одном месте и их можно легко скопировать. Во втором случае, речь идет о том, что, иногда, злоумышленники пользуются тем фактом, что портативные версии часто располагаются на сторонних ресурсах. Они создают и выкладывают в сеть свою копию портативного приложения, предварительно заражая ее вредоносным кодом (вирусами, троянами, шпионами и прочим). В третьем случае, речь идет о том, что портативная программа остается программой. Это означает, что нельзя забывать, что на других компьютерах так же должны выполняться системные требования для запуска программ. Безусловно, сегодня, этот риск маловероятен, но все же он вероятен.

Теперь, вы знаете о том, что такое портативное приложение и какие особенности возникают, при его использовании.

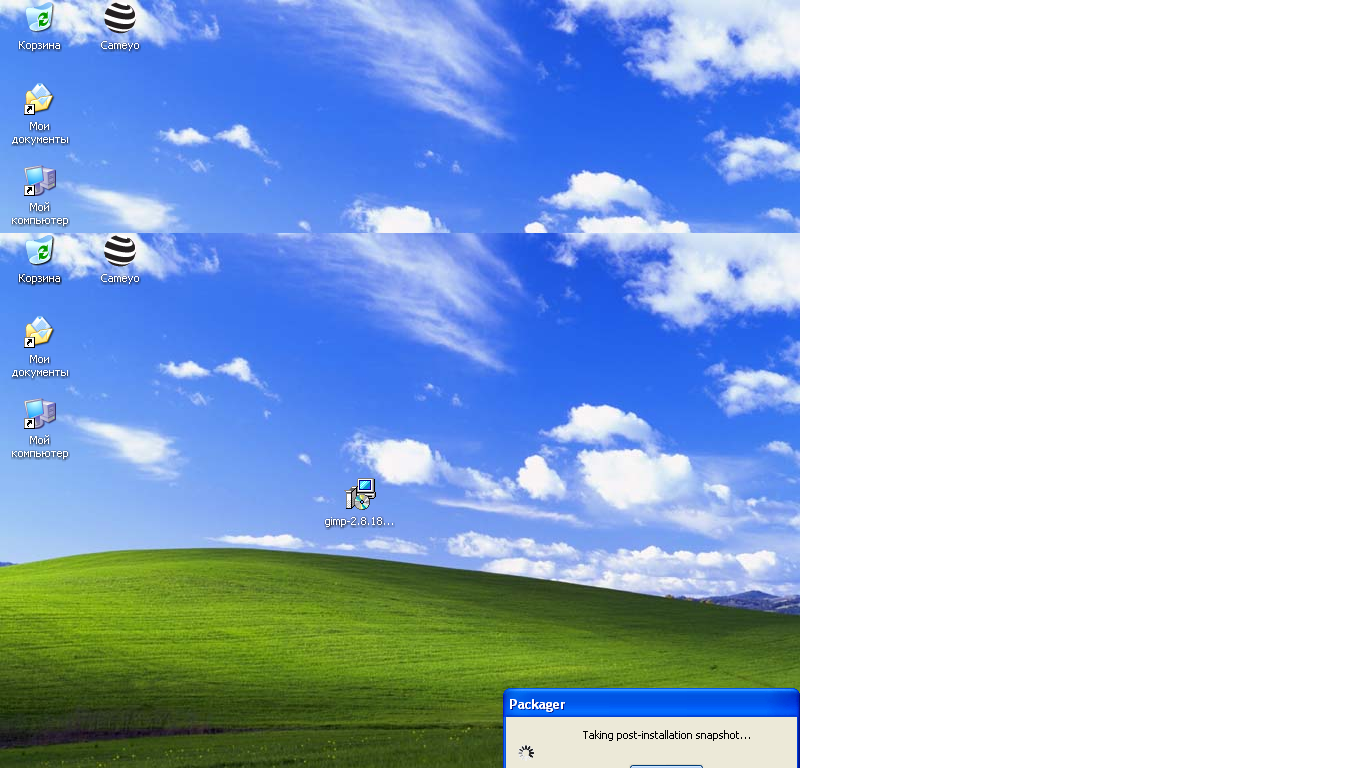
## Создание своего портативного приложения установка.

Было выбрано приложение GIMP для создания его портативной копии. ПО портирования – Cameyo.

1. В виртуальную систему Windows XP SP3 было сброшено инсталятор приложения GIMP и лаунчер Cameyo.
2. После запуска лаунчера было выбрано опцию «Capture installation» в последствии чего было произведено снимок операционной перед инсталяцие избранного ПО.
3. Было запущено инсталяционое приложение. После его работы.



1. После установки было нажата кнопка «Install done» в последствии чего был сделан второй снимок системы.



1. Далее программа сохранила готовый лаунчер-песочницу на диск С:\Documents and settings\Имя\_пользиваетля\Application Data\VOS\Имя\_портируемой\_програмы.
2. Сравнительная характеристика показала что программа работает исправно с небольшими утратами в производительности.

