Вычислительная свобода на компьютере

Облегченное практическое пособие

Пособие создано в рамках проекта LibreTrack

Вычислительная свобода на компьютере. Облегченное практическое пособие

В пособии приведены практические инструкции по установке и настройке свободных операционных систем, использованию технологий виртуализации и туннелирования, а также различных свободных программ и сетевых ресурсов.

Папка с материалами проекта LibreTrack в сервисе Internxt https://share.internxt.com/d/sh/folder/bb248f9bfd080972c8f1/765d77934c48a5857b51e6a2972bc41ae02147b25e53e07878471ae8539077d3

Канал YouTube https://www.youtube.com/channel/UCDhg72ALuEhO0BkkyWHt2JA

Оглавление

1 Предисловие

Данное пособие является вырезкой материалов по настройке безопасной системы на компьютере из полного пособия по вычислительной свободе.[1] Из него удалено множество материалов, которые для обычного пользователя являются явно избыточными. Материалы, требовавшие обновления, актуализированы. Также внесены сведения, которые прежде не входили в полное пособие, но которые также представляются важными для повседневного использования компьютера.

Эти инструкции рассчитаны на пользователей не искушенных в компьютерных технологиях, изложение дается достаточно ясно.

2 До операционной системы

1 Подводные камни аппаратного обеспечения

Прежде чем приступать к методике обеспечения безопасности на компьютере, я хотел бы сказать о том, что необходимо учесть перед приобретением компьютера, на случай если вы, взявшись за это пособие, подумывайте купить его себе.

Крайне желательно, чтобы ваш компьютер был чистым на аппаратном уровне. То есть, чтобы в нем не было шпионящих аппаратных закладок.[2] К сожалению проконтролировать данный момент обычный пользователь не способен. Но тут остается отметить, что все-таки далеко не каждое устройство содержит закладки.

Желательно избегать процессоров Intel, поскольку они содержат инструмент Intel Management Engin.[3] Он создан, чтобы предприятия могли управлять компьютерами удаленно, с помощью технологии Active Management.[4] Несмотря на то, что данная технология работает в изоляции от операционной системы, инструмент Intel Management Engin вызывает тревогу, поскольку имеет доступ к памяти и может отправлять и получать данные через Интернет. Конечно же, он проприетарный, Intel постарались предотвратить всякую попытку сообщества выяснить исходный код. Они скрывают полные сведения о его функционале. Таким образом, этот инструмент является потенциальным бэкдором.[5] В нем неоднократно находили уязвимости,[6] и известны случаи,

когда их эксплуатировали злоумышленники.[7]

У процессоров AMD есть аналогичный инструмент, однако его отключить значительно проще, чем программу от Intel, хотя AMD также раскрыли не все сведения об этой технологии.[8] Для отключения достаточно в BIOS найти параметр AMD PSP и поменять «Enable» на «Disable». Такое отключение будет не полным, но это все же лучше, чем полное включение. Помимо этого, процессоры AMD менее подвержены уязвимостям, чем процессоры Intel.[1] Существует, правда, возражение, что уязвимости в AMD, хоть и встречаются реже, зато сами по себе опаснее — их проще эксплуатировать, и вред от этого может быть больше. К сожалению, я не могу подтвердить либо опровергнуть подобное заявление.[2] Мне не известно, действительно ли оно отражает общую картину имеющихся в этих процессорах уязвимостей, или же такое можно сказать только в отношении отдельных конкретных дыр, которые, вполне возможно, уже закрыты. Данный вопрос требует изучения.

Что касается производительности, то на сегодняшний день AMD, в большинстве случаев, как минимум, не уступает Intel. Исключение составляют только игры, но и там преимущества Intel не существенные. При этом, процессоры AMD еще и дешевле.[3]

При покупке отдельного оборудования, комплектующих, а также полноценных устройств, желательно предварительно проверить их на взаимодействие со свободным ПО. Сделать это можно через специальные сервисы.[4] К сожалению, там можно проверить далеко не все оборудование, особенно новые модели. Однако, в ряде случаев, это может послужить некоторым ориентиром. Также по запросом в поисковиках можно найти форумы, где обсуждается взаимодействие тех или иных устройств с системами GNU/Linux. Там можно найти информацию о совместимости оборудования со свободными системами.[5]

Существуют компании продающие чистые устройства, кстати, с уже предустановленным свободным ПО.[6] Если вы решили купить компьютер, обратите внимание на них.

2 Замечание о встроенном программном обеспечении

Инициализацию и настройку оборудования, а также загрузку операционной системы в компьютере осуществляет встроенное программное

обеспечение. А именно BIOS.[7] Данное ПО является несвободным, а значит, это повод нам насторожиться. Сейчас повсеместно внедрена технология UEFI.[8] Она также является несвободной. Кроме того, что она может ограничить пользователя в некоторых действиях, существует опасность, связанная с возможностью работы в ней через Интернет. Существуют атаки, направленные на компрометацию устройств пользователей, через UEFI.[1]

В идеале такие прошивки желательно было бы заменить на свободные. В частности существует Libreboot.[2] Она полностью свободна, легка в использовании, имеет удобный интерфейс и некоторые дополнительные возможности. Несколько менее приглядной является Coreboot.[3] В ее коде содержаться некоторые несвободные компоненты, к тому же она не очень удобна для неподготовленного пользователя.

К сожалению, оба этих варианта поддерживают очень ограниченный круг оборудования. Причина та же, что и со свободными драйверами, не все производители готовы к сотрудничеству со свободным сообществом. Ввиду этого, рекомендовать это ПО широкой аудитории не приходится. Тем не менее, можете проверить, подходит ли ваше оборудование для свободной прошивки, и в случае успеха, поискать методики по установке.

3 Основная операционная система

3 Выбор операционной системы

Не стану в очередной раз повторяться и говорить почему системы вроде Windows и MacOS не подходят для использования. Что же подходит? Существует несколько семейств свободных операционных систем. Самая известная и распространенная из них GNU/Linux.[4] Наверняка многие слышали о «системе Linux», однако называть ее так некорректно. Linux это только ядро операционной системы.[5] Оболочка же в значительной мере программы GNU, и сама система, как целое берет свое начало из проекта GNU, который начался задолго до того, как было написано ядро Linux. Без данного проекта у нас бы не было ни полностью свободных операционных систем, ни организованного движения свободного программного обеспечения. Поэтому правильно называть системы данного семейства именно GNU/Linux.[6]

На сегодняшний день существуют сотни дистрибутивов GNU/Linux. К сожалению, значительная часть из них создавалась и создается сторонниками не свободного ПО, а открытого, у которого совершенно другие идеологические задачи. Сторонники свободного ПО стараются вернуть своим пользователям свободу. Сторонники открытого делают акцент на практических преимуществах подобного способа разработки. По этой причине они спокойно относятся к включению в свои операционки несвободных компонентов.

Самым популярным на сегодняшний день дистрибутивом GNU/Linux является Ubuntu. Она нашпигована несвободными компонентами, и я категорически ее не рекомендую.[7] Не далеко от нее ушел основанный на ней дистрибутив, также очень популярный, Mint.[8] Поэтому его я тоже не стану рекомендовать.

Ubuntu относится к ветке дистрибутивов, основанных на Debian. О данной системе я еще скажу, пока лишь замечу, что ОС, основанные на ней являются наиболее удобными для простого пользователя. В другие ветки операционных систем семейства GNU/Linux интегрировано меньше программного обеспечения, удобного для простого пользователя.

Вторым по распространенности семейством этичных операционных систем является BSD.[9] У данного семейства две проблемы. Во-первых, классические его дистрибутивы, такие как FreeBSD и OpenBSD не подходят для домашнего использования, ввиду отсутствия удобного интерфейса. На них можно работать в графической оболочке, но ее установка сопряжена с большими сложностями. Есть дистрибутивы с полноценным графическим интерфейсом, рассчитанные на домашнее использование.[10] Но это не отменяет у них второй проблемы, характерной для семейства BSD. Все они снисходительно относятся к некоторым типам проприетарного ПО. Ядро BSD изначально содержит несвободные компоненты (также как и обычное ядро Linux).[11]

Другие семейства свободных операционных систем, крайне мало распространены, и я не могу их рекомендовать уже ввиду их экзотичности.

Что же выбрать? В самом распространенном и продвинутом семействе свободных операционных систем — GNU/Linux — вышедшем из проекта, благодаря которому у нас вообще есть свободное ПО, есть то, что нам нужно. Среди сотен дистрибутивов, содержащих проприетарные компоненты, есть десяток полностью свободных. Все они представлены на сайте проекта GNU.[12]

Они не только не имеют несвободных компонентов в своих сборках, но таковые также отсутствуют в их хранилищах программ (о том, что это такое будет сказано в дальнейшем). Из ядра Linux, используемого в них, удалены несвободные кляксы, или же блобы, объекты кода, распространяющиеся лишь в бинарном виде, как правило, это прошивки для устройств.[13] Данные системы действительно полностью свободные. Из них и стоит выбирать.

Среди них есть независимые, т.е. не основанные на других дистрибутивах, системы. Таковой является Dragora, но у меня с ней подружиться не получилось, поэтому ее в данном пособии не будет.[14] Дистрибутив Giks отказался у меня корректно работать, поэтому он тоже использоваться не будет.[1]

Есть в этом списке и специфические дистрибутивы. Dyne:bolic ориентирован на редактирование видео. Если вы создаете видео, занимаетесь монтажом, обратите внимание на этот дистрибутив.[2] Однако, поскольку в данном пособии речь идет о домашнем компьютере, на котором выполняется широкий круг повседневных задач, данный дистрибутив в нем не фигурирует.

Есть среди этих систем основанные на Arch.[3] Это дистрибутивы Hiperbola[4] и Parabola.[5] Данные системы в этом пособии также использоваться не будут. Во-первых, они имеют большие сложности в установке, а Hiperbola по-умолчанию даже не имеет графического интерфейса, что влечет дополнительные сложности. Во-вторых, как я сказал выше, наиболее предпочтительны для простого пользователя системы ветки Debian.

И в этом списке есть система, основанная на Debian. Дистрибутив PureOS, в целом, вполне добротный, однако мне он показался не очень удачным для домашнего использования.[6] По умолчанию в нем установлен не самый удобный интерфейс, а поменять его на что-то более удобное, мягко говоря, затруднительно. Есть и другие мелкие моменты, которые я бы назвал недочетами. Все это, к сожалению, перекрывает единственное преимущество данного дистрибутива перед Debian, на котором он основан, полное неприятие несвободного ПО. Тем не менее, данный дистрибутив вполне подходит для использования.

Но еще лучше было бы взять дистрибутив основанный на Ubuntu. Взятый за основу самый популярный дистрибутив, позволяет использовать более широкий круг ПО, поскольку многие проекты ориентируются сугубо на Ubuntu,

ввиду ее популярности. А также упрощает его использование, поскольку информацию о том, что и как установить и настроить проще всего отыскать именно для Ubuntu.

В этом списке есть и такие. Дистрибутив Trisquel имеет широкий набор программ, крайне приятный интерфейс и к тому же гибко настраиваемый.[7] Он полностью соответствует критериям свободных ОС и вместе с тем, крайне удобен в использовании. Есть еще дистрибутив Utito, но мне он не понравился.[8] Это уже по-видимому дело вкуса.

Если вы всю жизнь просидели на Windows, вы элементарно привыкли к определенному дизайну. Ярлыки закреплены по рабочему столу, панель задач расположена внизу, а в левом ее углу, кнопка меню. Таков интерфейс Trisquel, и вероятно, к нему будет проще адаптироваться бывшему пользователю Windows. Но если захотите чего-то другого, дизайн всегда можно поменять. Это все в добавок к широкому функционалу и набору ПО.

Конечно Trisquel тоже не лишен недостатков. Некоторое программное обеспечение в нем не полностью русифицировано, но лишь некоторое. Кроме этого, большинство программ представлены не самыми свежими версиями. Однако обновления безопасности приходят регулярно, поэтому эта проблема не критична. Именно Trisquel я рекомендую в качестве основной операционной системы.

Кроме этих операционных систем, есть только пара дистрибутивов, которые я могу рекомендовать для использования. Один из них, это уже упоминавшийся Debian.[9] Изначально в нем отсутствуют несвободные компоненты, из ядра также выпилины несвободные кляксы. Однако в его хранилищах присутствуют разделы с несвободными программами, и хотя изначально эти разделы отключены, в целом Debian лоялен к установке несвободного ПО.[10] Однако, без действительно целенаправленной установки вами такого ПО, оно не будет присутствовать в этой системе. У Debian, к сожалению, есть еще одна проблема. Это компонент systemd. Данный инструмент является инициализатором. Он используется для запуска различных программ, при загрузке системы. Его проблема в том, что это больше чем инициализатор. Помимо основной своей функции он также интегрирован со множеством других компонентов. Это чревато тем, что если в нем возникнет какая-то проблема, это может отразиться на многих функциях системы.[11] Также большой функционал подразумевает большой код, а чем больше код, тем

сложнее его проверять. В данном инструменте много раз находили уязвимости, в том числе, критические. Их исправляли, но есть высокая вероятность того, что в нем продолжают присутствовать другие. Также в нем присутствует функция использования в качестве DNS серверов от Google.[12] Это используется, конечно, не на постоянной основе, но все же при некоторых обстоятельствах может стать проблемой.[13] Особенно это нежелательно для систем, активно контактирующих с Интернетом. Инструмент systemd присутствует не только в Debian, но и в других системах, включая рекомендуемые полностью свободные, в том числе, Trisquel.[14] Но ввиду его удобства и того факта, что он основан на Ubuntu, ввиду чего многие программы будут работать именно в нем, а не в других системах, я продолжаю его рекомендовать. Однако, вместо Debian лучше было бы порекомендовать что-то подобное, но без столь неприятного компонента, как systemd. И существует дистрибутив, основанный на Debian, но использующий другие инициализаторы, будучи во всем остальном идентичным. Этот дистрибутив называется Devuan.[1] Его недостаток перед классическим Debian в том, то в нем по-умолчанию, включены разделы репозиториев с несвободными программами. Но их можно легко отключить. Также эта система менее забагована чем последняя версия Debian. Таким образом, система Devuan более предпочтительный вариант, чем Debian.

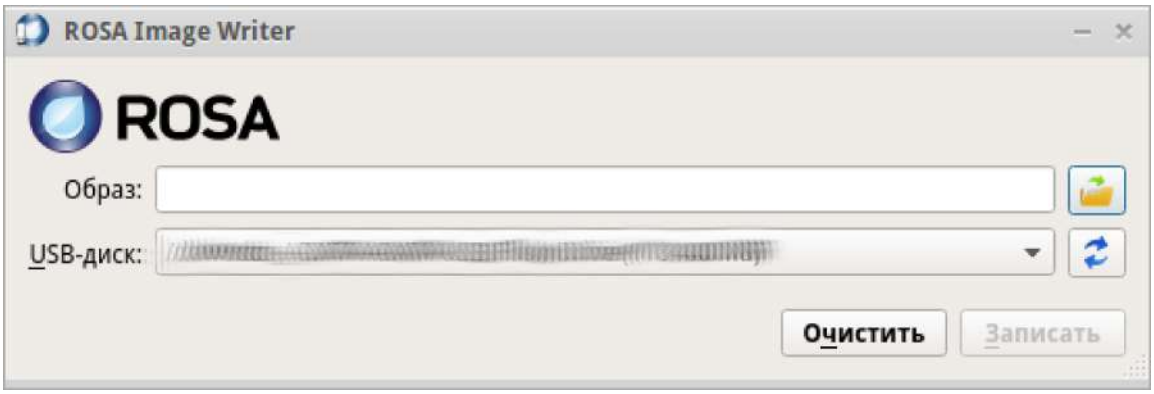
Ну а всецело рекомендуемый мной Trisquel будет рассматриваться в качестве основной операционной системы в данном пособии.

4 Запись Trisquel на флешку

Для начала, идем по ссылке и скачиваем последнюю версию операционной системы Trisquel.[2] На момент написания данного пособия это Trisquel 11. После того, как iso-образ скачан, его нужно записать на флешку (можно также записать на диск, но этот допотопный вариант я здесь рассматривать не буду). Существует много программ для записи образов на носитель. Среди свободных программ можно отметить Rufus.[3] Весьма многофункциональный. Однако, он имеет версию только для Windows. Все-таки было бы разумно уже осваивать программы, которые работают и под GNU/Linux. Кроме того, обилие функций может только запутать неискушенного пользователя. Единственная известная мне свободная кроссплатформенная (работающая на разных системах) программа для записи образов на флешку — Rosa. Скачиваем и устанавливаем

данную программу.[4] Установка совершенно стандартная, если вы пользуетесь компьютером, то уже наверняка не раз ее проводили, поэтому на ней я останавливаться не буду, просто следуете инструкции.

После установки вставляем в компьютер флешку, объемом не менее 4 Гб и запускаем программу. Откроется окно в котором нужно будет указать свою флешку, как устройство для записи (нижнее поле). И выбрать записываемый образ ОС (верхнее поле), то есть образ Trisquel.



После этого остается только нажать «Запись» и дождаться конца этой записи.

По окончании можно закрыть программу. Теперь у нас есть флешка, с которой мы будем загружаться и устанавливать Trisquel на свой компьютер.

5 Установка Trisquel

Прежде чем приступать к установке новой ОС, необходимо сделать копию всей информации, которая есть на вашем компьютере, если у вас этой копии нет. А вообще, никогда не храните информацию, которая хоть сколько-нибудь для вас важна, в одном экземпляре. Всегда делайте запасную копию, а лучше не одну. Также рекомендую, если пользуйтесь Интернетом через Wi-Fi, пройти на сайт производителя Wi-Fi-адаптера и скачать драйвер для него, поскольку бывают случаи, что для той или иной модели Wi-Fi-адаптера нет свободного драйвера, и после установки новой системы, вы не сможете воспользоваться Интернетом. Для сетевых карт проводного Интернета, а также большинства USB-модемов, таких проблем не известно. Если резервное копирование на отдельный носитель сделано, можно двигаться дальше.

Вставив флешку с записанным на нее образом Trisquel в компьютер, перезапускаем его. Иногда случается, что когда используется перезагрузка

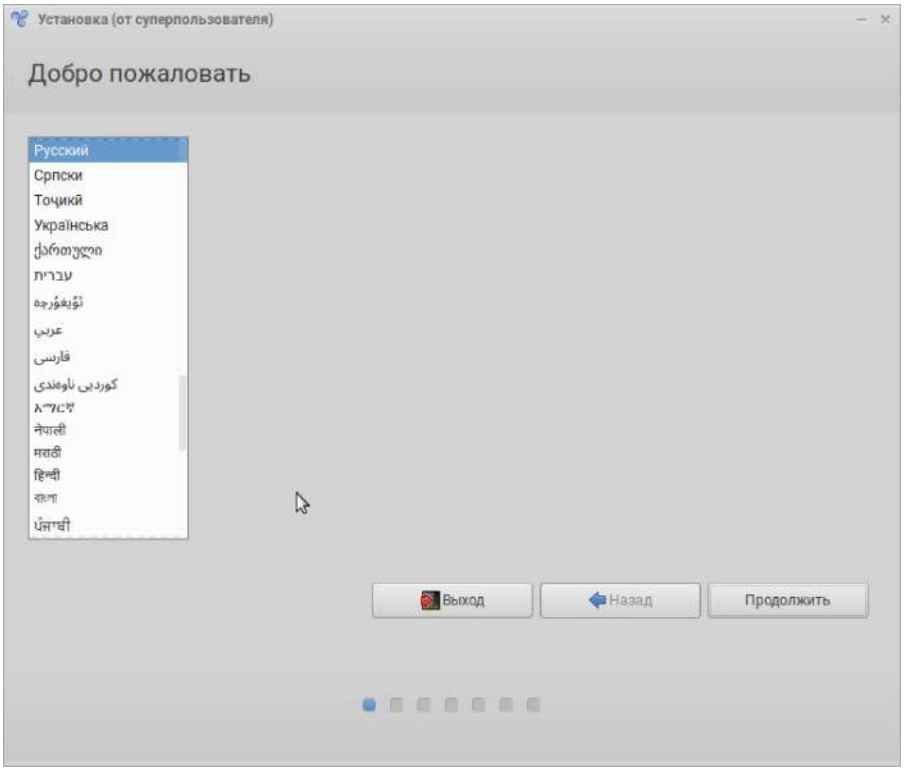
Windows с последующим входом в систему на флешке, и запускается процесс установки, операционка устанавливается некорректно. Поэтому лучше компьютер не перезагружать, а выключить и затем включить. Часто в системе заложено, что когда в компьютер вставлена загрузочная флешка, он автоматически начинает загружаться с нее. В этом случае перед вами сразу откроется меню Trisquel. Но иногда, компьютеру нужно самостоятельно указать с какого устройства загружаться. Когда компьютер только начал загружаться, нужно открыть интерфейс BIOS, или UEFI, который сейчас чаще всего можно встретить. Для этого нужно до того, как начнет загружаться сама операционная система успеть нажать определенную клавишу. На всех компьютерах, с которыми я работал, стационарных и ноутбуках, старых и современных, это была клавиша F2. Но вообще может быть и другая, например F7 или Esc. После ее нажатия откроется меню BIOS (UEFI).

Здесь стрелками на клавиатуре (← →) нужно перейти во вкладку «Boot». В данной вкладке откроется список устройств, с которых может производиться загрузка. На первом месте, скорее всего будет HDD. Это жесткий диск, на котором стоит ваша операционная система. Где-то под ним будет располагаться вставленная загрузочная флешка. Стрелками на клавиатуре (↑ ↓) нужно выбрать устройство, стоящее на первом месте (скорее всего HDD) и нажать Enter. Откроется окно, где также будет перечень устройств. Из него нужно выбрать вашу флешку (USB) и нажать Enter. Если к компьютеру подключено через USB несколько загрузочных устройств, к примеру, операционная система установлена на внешнем жестком диске, подключенном через USB-кабель, то флешка может не отобразится, на ее месте в графе USB окажется это устройство. В этом случае, под списком устройств будет строка «USB Priority». Необходимо спустится к ней, нажать Enter, и в появившимся окне также на первом месте выставить вашу флешку (ее, если что, узнайте по названию и объему памяти). Когда все сделано, загрузка будет производится с загрузочной флешки, когда она вставлена.

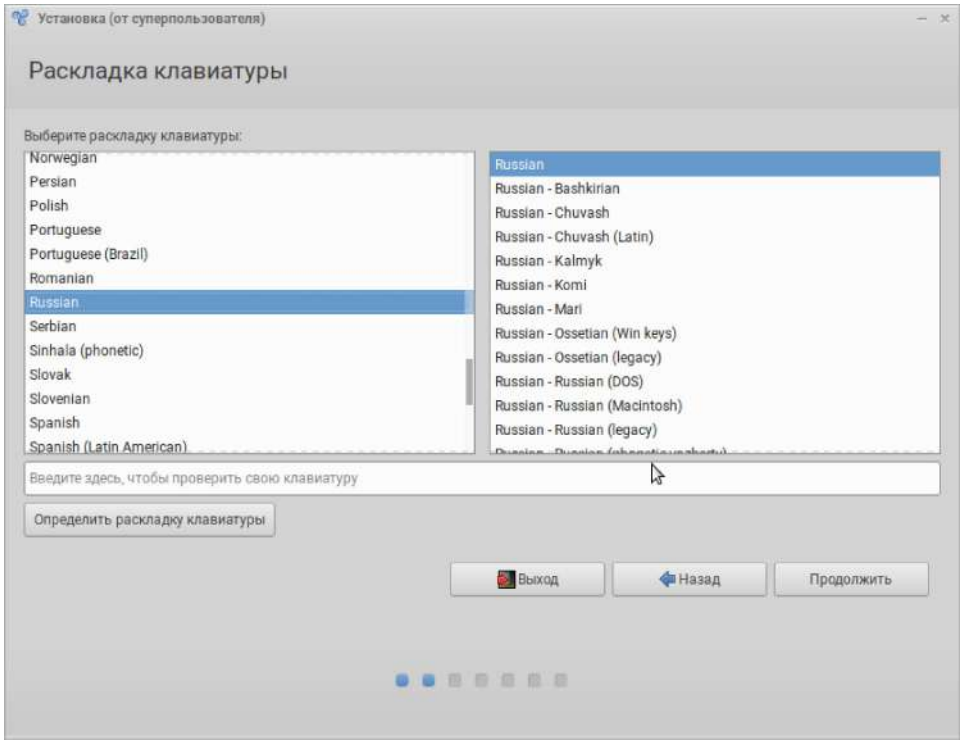
Стрелками на клавиатуре (← →) переходим во вкладку «Exit» и в ней также стрелками (↑ ↓) выбираем графу «Save change and reboot» и нажимаем Enter. Компьютер начнет перезагружаться, и когда он перезагрузится перед вами появится меню Trisquel, в котором вам нужно будет стрелками на клавиатуре выбрать свой язык и также нажать Enter. Откроется загрузочное меню.

Первой строкой стоит «Запустить Trisquel без установки». Если нажать на нее, то можно без установки поработать с системой, познакомиться с ней. Я рекомендую выбрать именно этот вариант. Конечно, можно было бы сразу выбрать «Установить Trisquel», но такая установка иногда завершается с багом. После открытия рабочего стола, нажимайте на нем на ярлык «Установка Trisquel».

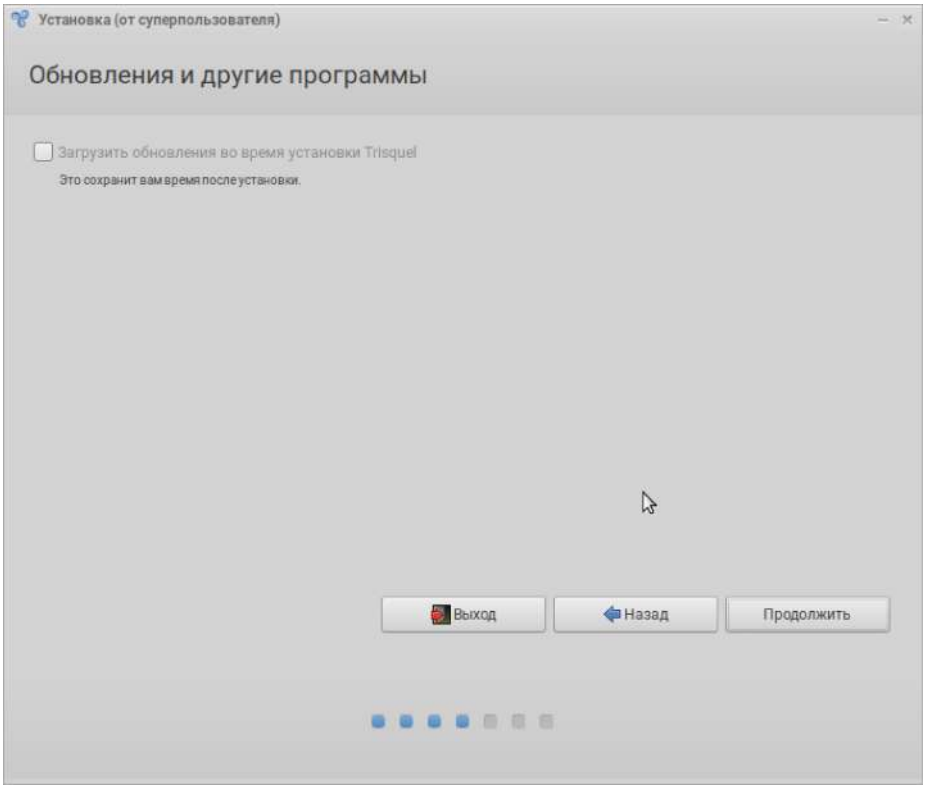
Откроется первое окошко установки, где нужно будет выбрать язык, и нажать кнопку «Продолжить».



Затем выбираем раскладку клавиатуры.



В следующем окне нужно указать, какой сетевой интерфейс использовать для подключения к Интернету, а затем, скачивать ли обновления с Интернета во время установки. Я рекомендую на время установки не подключать Интернет, поэтому пропускаем этот шаг.

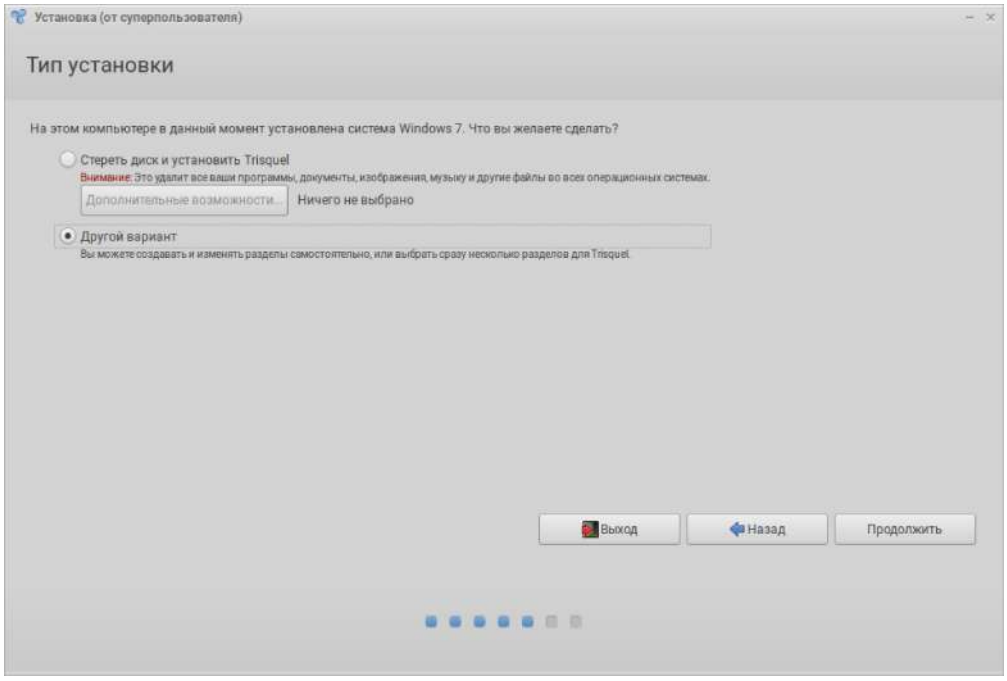


В следующем окне необходимо указать куда и как устанавливать систему. И тут есть несколько моментов. Trisquel, как и любая другая система GNU/Linux, может существовать на одном жестком диске с Windows. Однако, я не рекомендую такую установку. Если Windows вам нужен (при первой установке GNU/Linux я рекомендую пока не удалять его, чтобы в случае возникновения проблем, вы не остались вовсе без рабочего компьютера), лучше купите для новой операционки отдельный жесткий диск. Совместную установку я не рекомендую, хотя бы потому что в этом случае вы не сможете зашифровать диск, что мы собираемся делать. Шифрование диска защитит ваши данные, если к компьютеру получит доступ кто-то посторонний, например, если он будет украден. Также использование шифрования диска поможет предотвратить установку буткитом в операционную систему вредоносных модулей, представляющих непосредственную опасность. Буткит — это вредоносное ПО, заражающее загрузчики, например UEFI, об атаках на который уже было сказано выше.

Можно просто стереть нынешнюю операционную систему и поставить на ее место Trisquel, но тут всплывает другой момент. Если мы выберем автоматическую разметку, то программа установки самостоятельно выделит пользовательский раздел, оставив мало дискового пространства для корневого

каталога, что сделает затруднительным создание виртуальных машин, для которых просто не будет места, и среди прочего создаст раздел подкачки. Бытует миф, что файл подкачки всегда нужен, и его размер должен быть не менее размера вашей оперативной памяти. Пятнадцать лет назад это было актуально, но сейчас это вовсе не так. С файлом подкачки две проблемы, во-первых, он серьезно тормозит систему. Во-вторых, когда определенный объем дискового пространства выполняет роль оперативной памяти, существует вероятность того, что такие сведения, попадающие в оперативную память, как пароли, могут попасть на жесткий диск. И если из оперативной памяти они удаляться максимум после перезагрузки компьютера, то на диске они могут задержаться. И если кто-то посторонний получит доступ к вашему диску, у него есть шанс получить ваши пароли. В связи с вышесказанным, файла подкачки следует избегать. Если у вас всего 4 Гб оперативы, то файл подкачки все же желателен. Если же у вас 8 Гб и более, то в файле подкачки нет никакой необходимости.

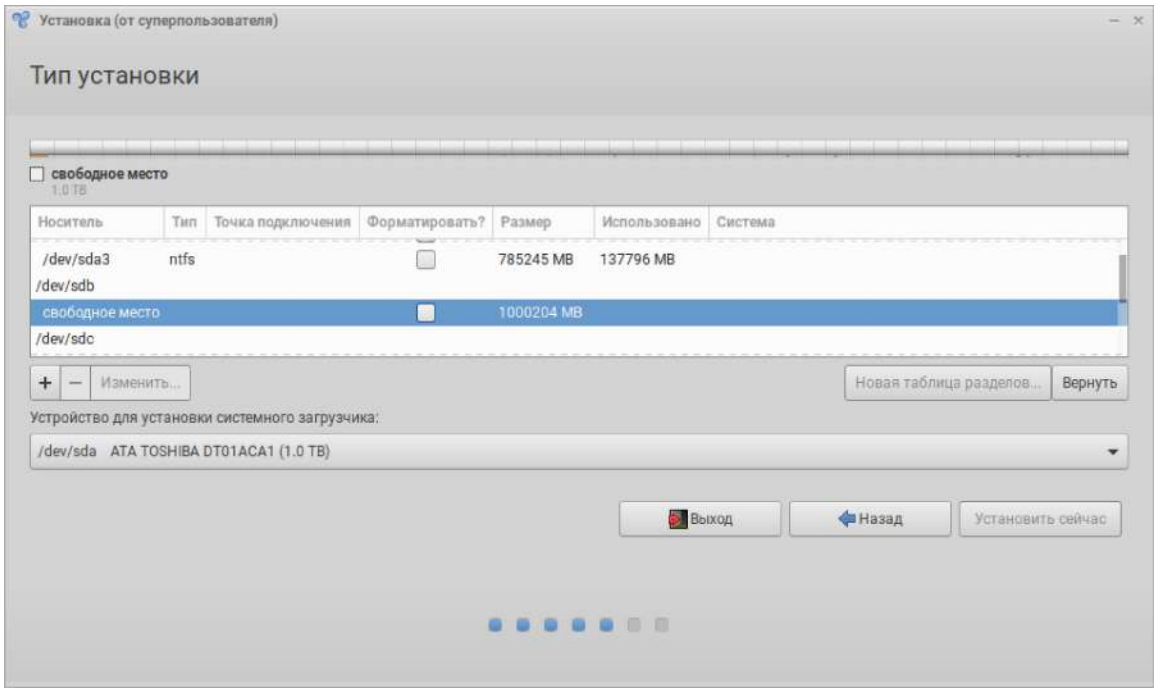
Ввиду всего вышесказанного, чтобы произвести действительно оптимальную установку, нам следует выбрать пункт «Другой вариант». В этом случае мы будем вручную размечать диск. Это куда сложнее, но я проведу вас.



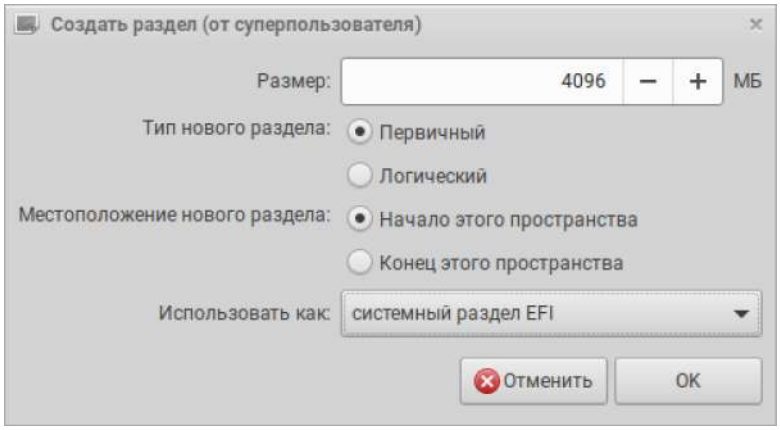
В открывшемся окне отображаются подключенные к компьютеру носители и их разделы. Нам нужно выбрать тот, на который будем устанавливать. Если подключен всего один диск, то проблем это не вызовет. В случае множества

устройств, можно ориентироваться по размерам и содержимому. Если заменяем Windows, то справа будет указано, на каком диске он установлен. Кстати, спешу заметить, что GNU/Linux можно устанавливать на флешки. Я сейчас говорю не о загрузочных флешках, а о полноценной установке, которую мы сейчас производим. Это также выгодно отличает операционные системы этого семейства от той же Windows, которую на сегодняшний день, невозможно установить даже на внешний жесткий диск, то есть диск, подключенный через USB-кабель. Главное, чтобы флешка была объемом не менее 32 Гб (конечно, в таком случае не получится в ней создать множество виртуалок, что мы собираемся делать, поэтому все же рекомендую полноценный жесткий диск от 500 Гб и более). И конечно, речь не идет о той же самой флешке, с которой мы производим установку.

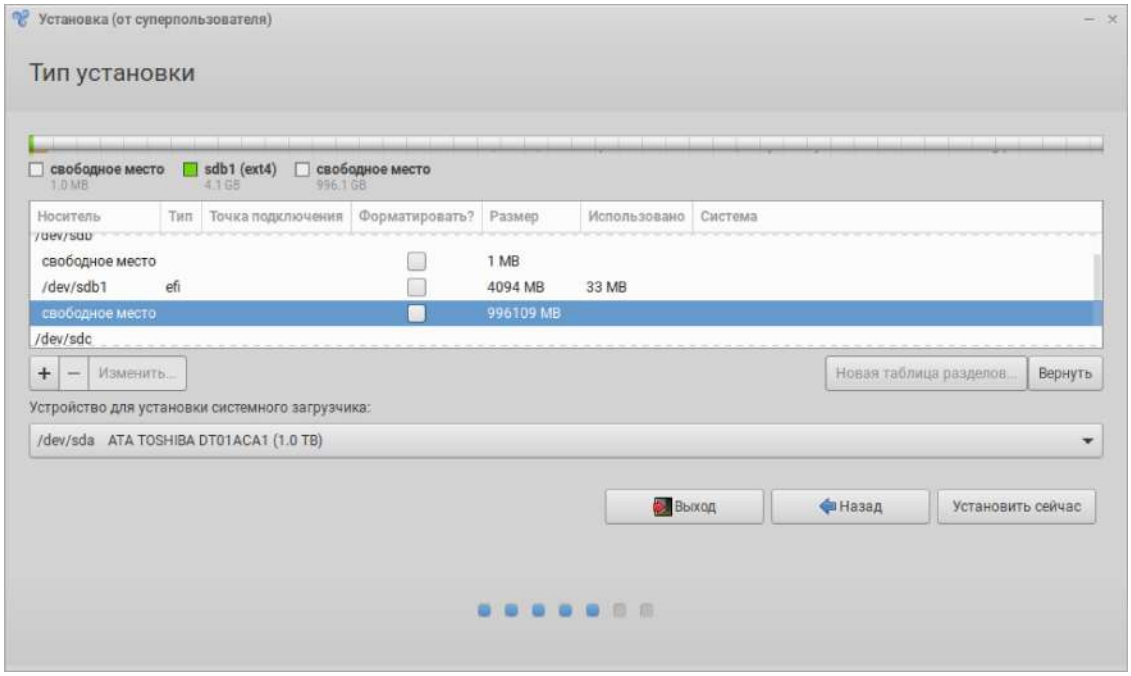
Выбрав диск, с него необходимо удалить все разделы. Для этого нужно выделить раздел и щелкнуть по знаку минус (–) внизу слева. Проделать это нужно для каждого раздела, пока под маркировкой устройства (/dev/sda, или /dev/sdb, или /dev/sdc, или /dev/sdd и т.д.) не останется только надписи «свободное место». Также можно выделив сам диск нажать на кнопку «Новая таблица разделов» внизу справа. Это также очистит диск оставив только свободное место. После этого, выделив это место, нажимаем кнопку плюс (+) внизу слева.



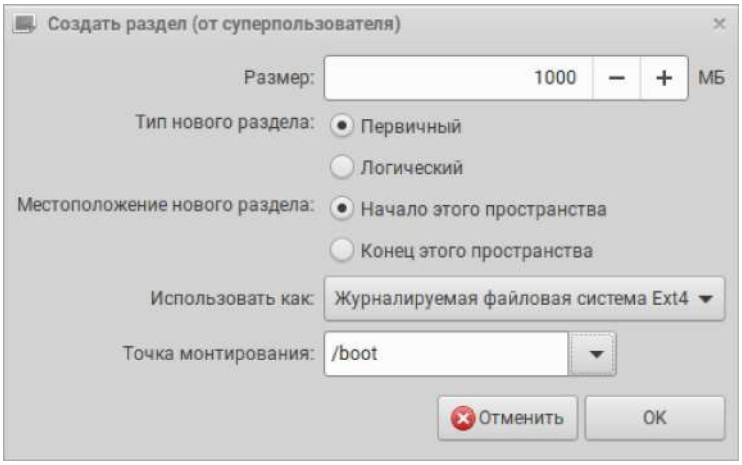
В открывшемся окне, в верхнем поле задаем размер раздела. Это будет один из загрузочных разделов, который необходимо оставить нешифрованным. Объем лучше задать с некоторым запасом, скажем 4096 Гб, хотя много пространства и не используется. В поле «Использовать как» выбираем «Раздел EFI».



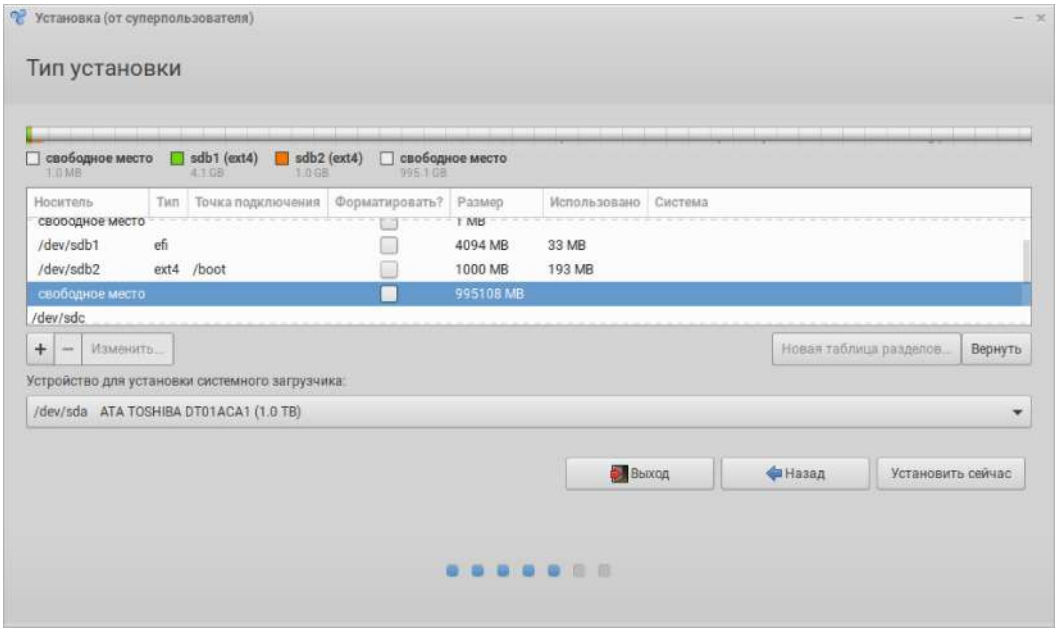
Нажимаем «Ok». Снова выбираем «свободное место».



В открывшемся окне, в верхнем поле задаем размер раздела. Это будет еще один загрузочный раздел, который необходимо оставить нешифрованным для проверки целостности ядра. Большой размер ему не нужен. Можно задать с запасом 1000 Мб. В поле «Использовать как» выбираем «Файловая система ext4», метку тома /boot.



Нажимаем «Ok». Теперь снова выбираем «свободное место».

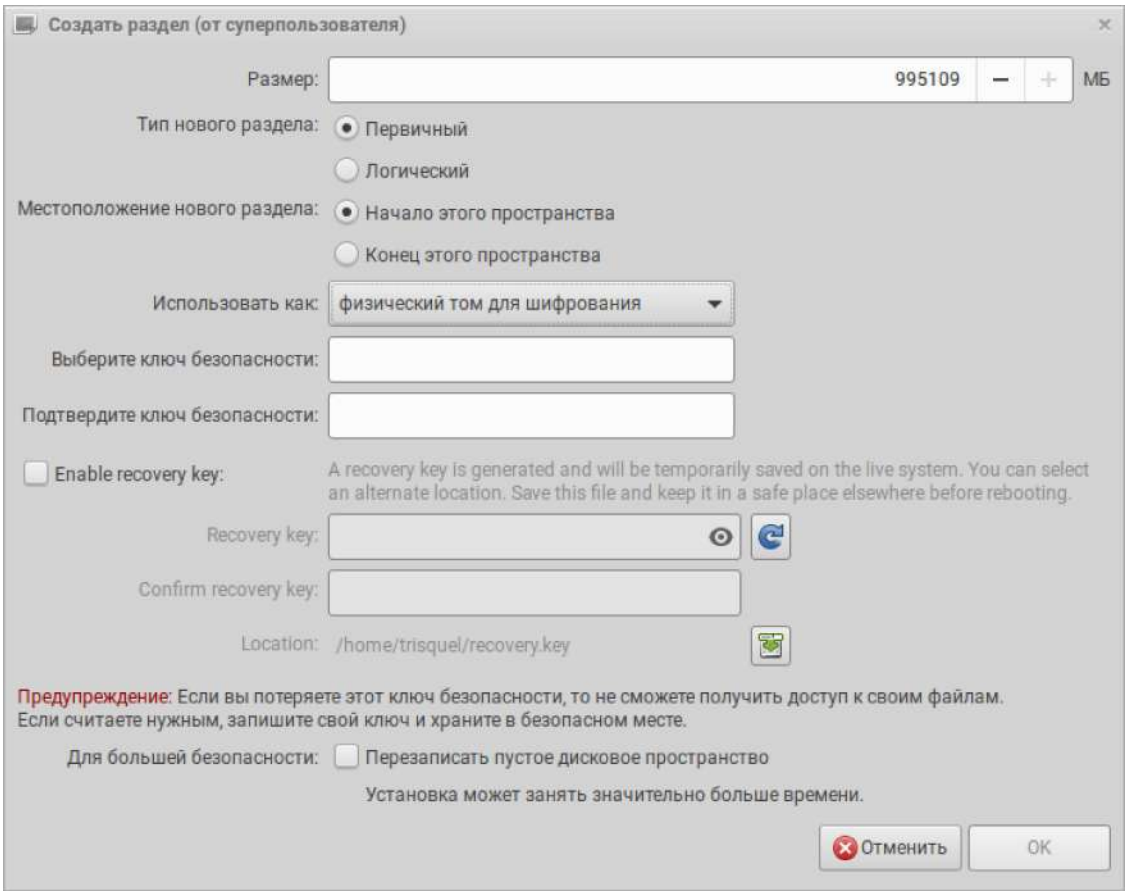


В открывшимся окне в верхнем поле оставляем весь оставшийся объем диска. «Использовать как» выбираем «Физический том для шифрования». Окно раскроется, и появятся поля для ввода пароля. Данный пароль необходимо будет вводить при каждом включении компьютера, поэтому нужно соблюсти баланс между надежностью и удобством. Пароли в одно слово или небольшой набор цифр, совершенно ненадежны и их применение противопоказано. В свою очередь чрезвычайно длинный набор совершенно случайных символов, при высокой надежности, крайне неудобен. Баланса можно достичь, если за основу взять сочетание слов, при этом чтобы одна или несколько букв были заглавными, или как вариант, чтобы одна или более букв в словах отсутствовали. В начало, конец или середину, можно добавить пару-тройку и более цифр. Все это должно сочетаться так, чтобы вам было относительно легко запомнить. При этом нужно набирать русские слова латинскими буквами. Обращаю внимание, не менять раскладку клавиатуры, а набирать именно русские слова латинскими буквами. Например informacionNaya44ezopasnosTT. Разумеется, слова и цифры не должны содержать никакой информации относящейся к вам лично, даты рождения, фамилии дальнего родственника и т.д. Программа укажет вам на надежность выбранного пароля. Справа от поля ввода будет прописано плохой он или хороший. Нужно чтобы надпись была зеленая. «Хорошего» пароля вполне достаточно. Несмотря на кажущуюся сложность, ввиду регулярного ввода, подобный пароль запомнится достаточно легко. Однако, по своему опыту скажу, что если вы в течении длительного времени не будите прикасаться к своему компьютеру, и соответственно вводить

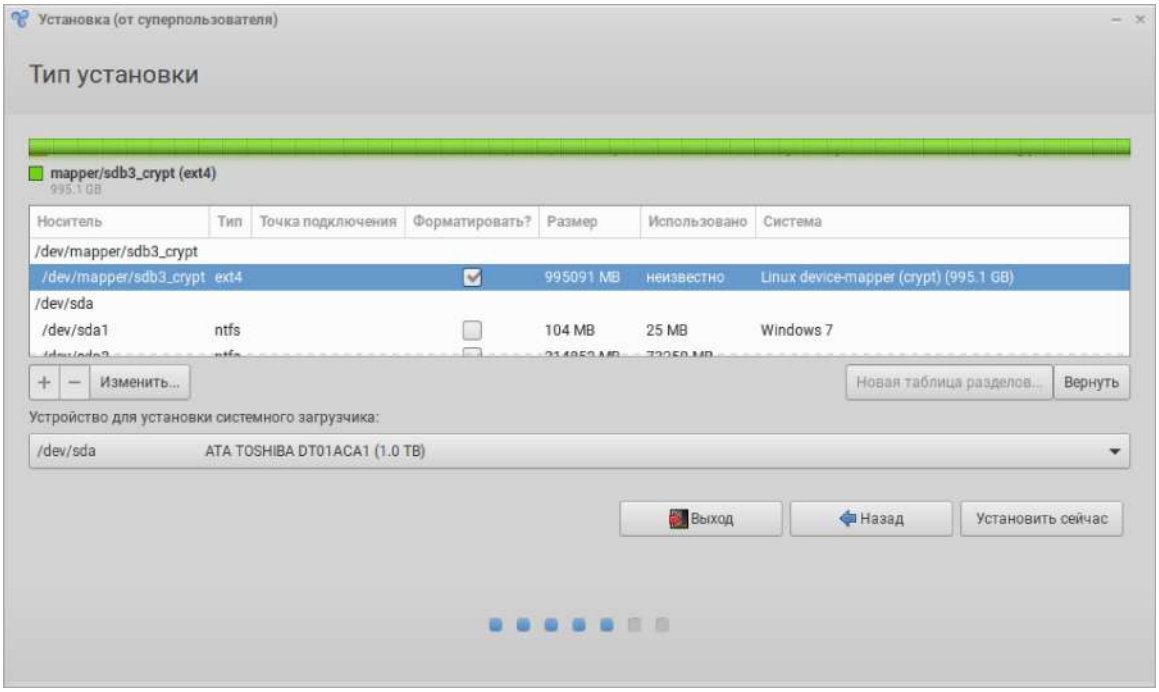
пароль, например, уедите в отпуск, есть вполне реальный риск его забыть. Поэтому обращаю внимание, на предупреждение, которое написано в окне. Если считаете нужным, запишите себе этот пароль и храните в надежном месте. Тут уже главное не забыть в каком именно месте вы храните пароль.

После ввода пароля, подтверждаем его, вводя еще раз. С паролем разобрались.

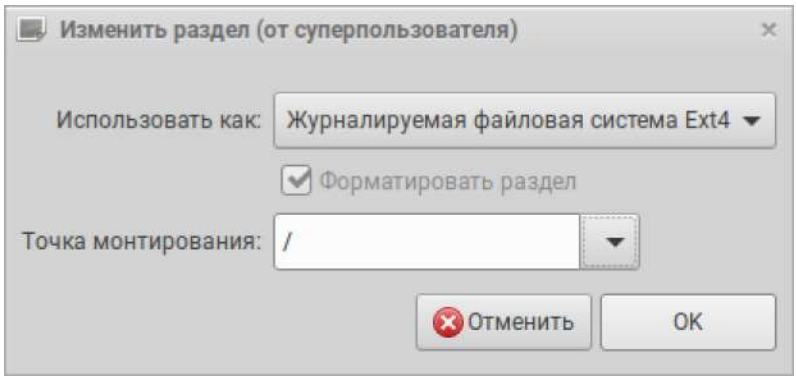
Галочку на перезапись пустого пространства ставить не нужно. Если это ваш личный компьютер, которым вы пользуйтесь месяцы или годы, а не взяли накануне на барахолке, то значительно увеличивать время установки, перезаписывая пространство, совершенно излишне. Для чего нужно перезаписывать пустое дисковое пространство я объясню позже.



Когда в этом окне все сделано, нажимаем «ok» и ждем, пока применяться изменения. В окне разметки появится новый раздел.



Теперь нам нужно выделить его и нажать кнопку «Изменить» внизу слева. Откроется уже знакомое окно, где в нижнем поле нужно выбрать /. Это значит, что данный раздел будет корневым.

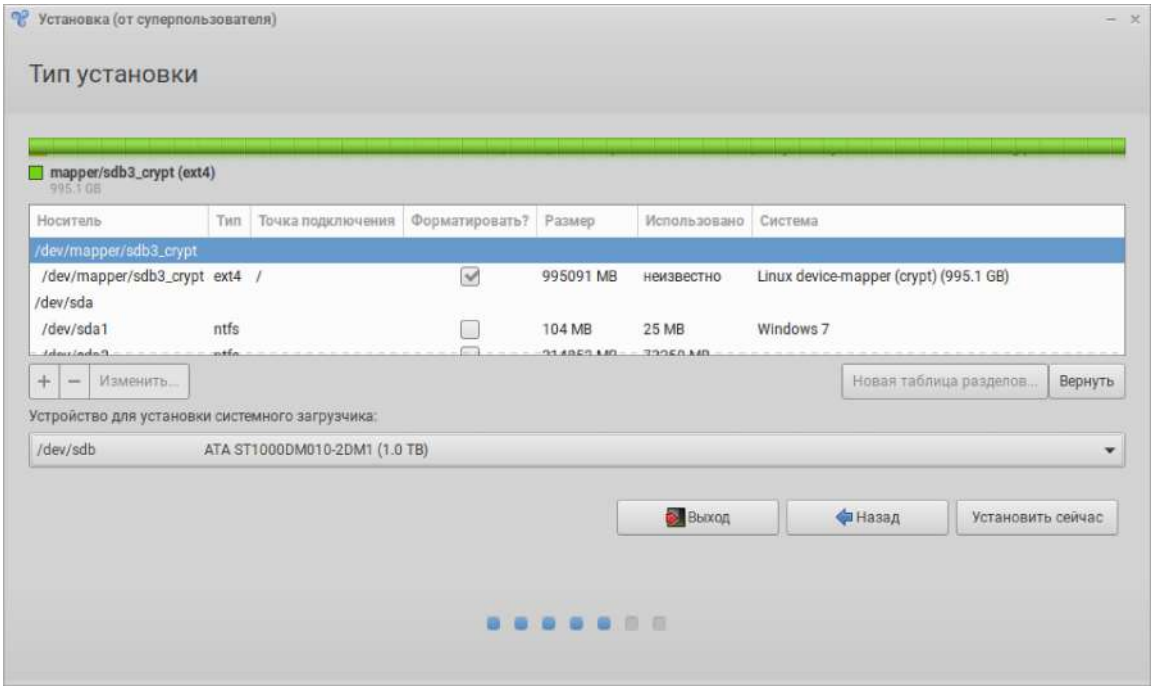


После этого нажимаем «ok». Если хотите, чтобы система была установлена на одном диске, а файлы собирайтесь хранить на другом, к примеру, операционку устанавливайте на SSD, а для файлов у вас HDD, существует возможность поместить на него пользовательский каталог /home. Однако я этого не рекомендую. Во-первых, каталог /home содержит не только файлы пользователей (т.е. ваши личные файлы), но и некоторые системные, поэтому, вынесение его на отдельный носитель может незначительно затормозить работу. Во-вторых, в некоторых случаях не удается корректно провести установку с такими параметрами. Поэтому, лучше HDD для файлов потом отформатировать и зашифровать. Также спешу заметить, что поскольку в

дальнейшем мы будем создавать много виртуальных машин для разной Интернет-активности, чтобы все они работали быстро, т.е. располагались на SSD, они должны все на него помещаться. Для этого его размер должен быть не менее 480 Гб (хотя, если собираетесь ограничиться несколькими виртуалками и не будите создавать виртуальные диски большого размера, может хватить и устройства на 240 Гб).

Необходимо заметить, что на компьютерах, у которых функция шифрования диска вшита в BIOS, бывает невозможно установить Trisquel с таким шифрованием. После установки система отказывается запускаться. Если у Вас именно такой компьютер, и установка таким способом завершится неудачей, то можете потом переустановить систему без шифрования, а его осуществить с помощью встроенной в BIOS функции.

Теперь нужно выбрать устройство для установки системного загрузчика. Это должен быть основной диск, с которого производится загрузка компьютера, и на который мы сейчас устанавливаем операционную систему. Причем это должен быть весь носитель, а не отдельный раздел. Выбираем соответствующий носитель. У всего диска, а не раздела, справа указаны имя и размер. Когда все сделано, нажимаем кнопку «Установить сейчас».

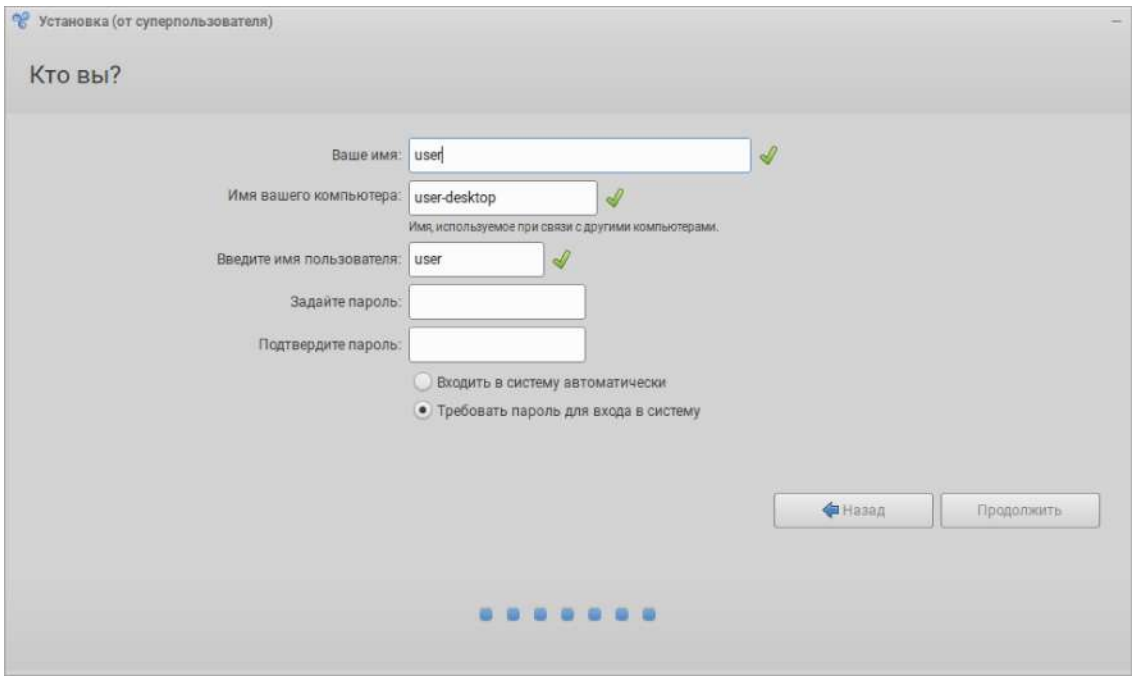


Если выскочит предупреждение, что мы не указали ни одного раздела подкачки, нажмите «Продолжить». Далее выскочит сообщение, записать ли

изменения на диск. Нажимаем «Продолжить».

В следующем окне выбираем регион, где находимся.

В последнем окне установки нужно задать данные учетной записи. Имя, в принципе, можете задать какое хотите. Единственное, чего категорически не рекомендую, это указывать свое настоящее имя и тем более фамилию. Такие данные могут быть доступны, во время подключения к сети, тем, кому видно ваше соединение. Таким образом, вы можете лишний раз идентифицировать себя не пойми перед кем, что поставит под угрозу вашу безопасность. Можете в качестве имени указать просто user. Все это касается и имени компьютера, и имени пользователя. В имени компьютера придется использовать некоторое разнообразие, чтобы различаться при подключении к локальной сети. Пароль, чтобы не путаться, рекомендую ставить тот же, который вы задавали при шифровании диска. Исключение может быть только если вы не единственный пользователь этого компьютера, и вам придется предоставить другим его пользователям ключ к дешифровке, но при этом вы не хотите, чтобы они попали в вашу учетную запись. Если вы единственный пользователь данного компьютера, то может считаться допустимым ставить автоматический вход в операционную систему, поскольку от несанкционированного доступа защитит пароль для дешифровки диска. Но при этом пароль здесь задавать все равно нужно, поскольку он будет использоваться при внесении системных изменений, к примеру, установке нового ПО. При таких операциях данный пароль придется вводить. Когда все заполнено, нажимаем кнопку «Продолжить».



Начинается процесс установки, который займет какое-то время. По окончанию нужно будет перезагрузить компьютер. Об этом выскочит соответствующее уведомление. Когда во время перезагрузки компьютер начинает включаться, можно вытащить флешку, чтобы снова не загрузиться с нее, и вновь зайти в BIOS, чтобы убедиться, что загрузка начинается с нужного диска. С этой процедурой, думаю, разберетесь.

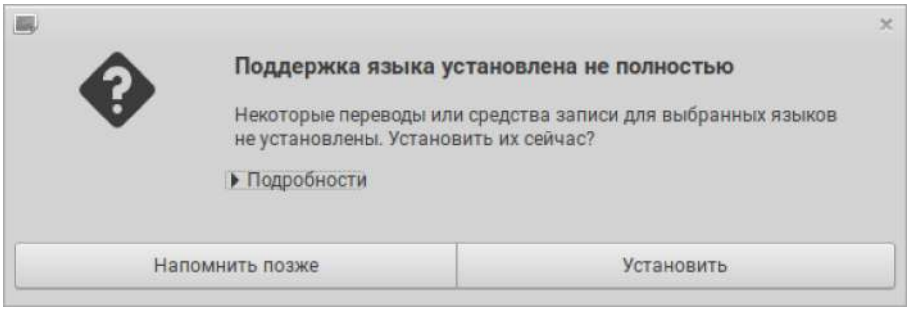
При загрузке по середине экрана появится поле для ввода пароля для дешифровки диска. Вводим, нажимаем Enter. Затем, после загрузки, если вы указали при установке, требовать пароль при входе в систему, появится заставка, и слева будет поле для ввода пароля. Вводим его, после чего появится рабочий стол.

Вы в операционной системе Trisquel.

6 Обновление операционной системы

Прежде чем знакомиться с данной системой, первое, что я рекомендую сделать, это подключить Интернет и обновить систему. Значок подключения к Интернету внизу справа. Также при подключении и отключении вверху справа выскакивает уведомление. Если вы пользуйтесь беспроводным Интернетом, и у вас возникают проблемы с подключением, то скорее всего в системе отсутствует драйвер для Wi-Fi-адаптера. В этом случае нужно установить заранее скачанный драйвер. Также, если, например, экран разворачивается с низким разрешением, или имеют место графические артефакты, то скорее всего, некорректно работает свободный драйвер для видеокарты. Возможно проблема решиться после обновления, но если нет, то драйвер для видеокарты, возможно, также нужно будет установить отдельно, о чем я скажу далее.

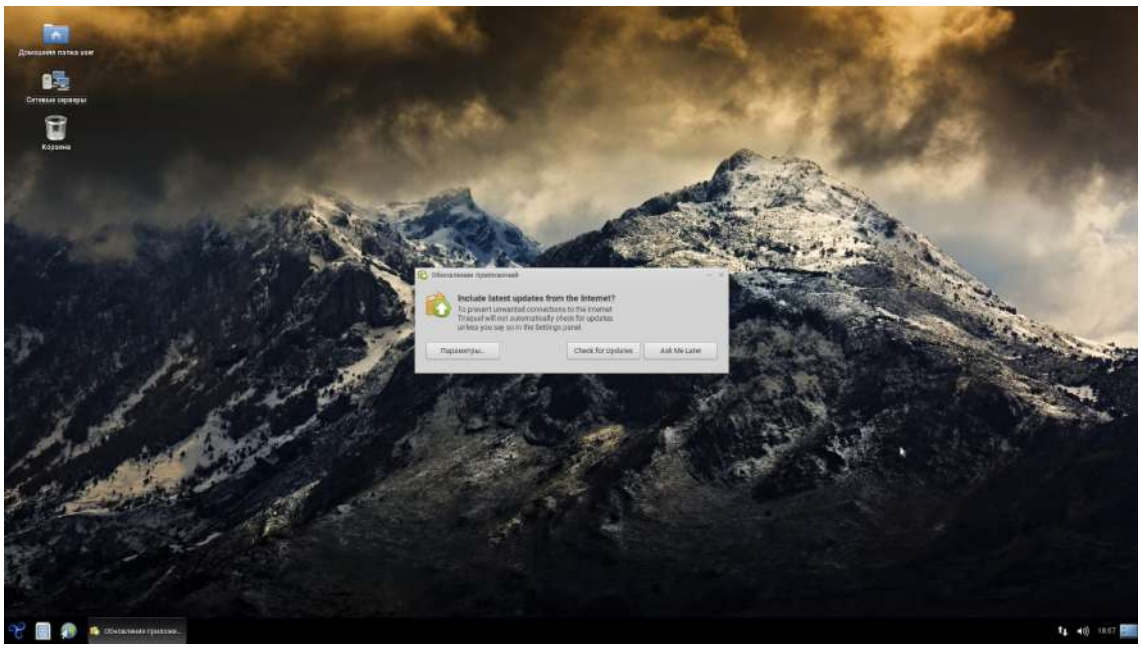
Когда система запустится, может сразу выскочить уведомление, что необходимо провести обновление языкового пакета. Нажмите «Выполнить это действие сейчас». Откроется еще одно окно. Нажимаем кнопку «Установить».



Если этого сообщения нет, то идем в Меню, вкладка «Система», затем «Администрирование», и в ней щелкаем «Язык системы». Далее все по описанной выше методике.

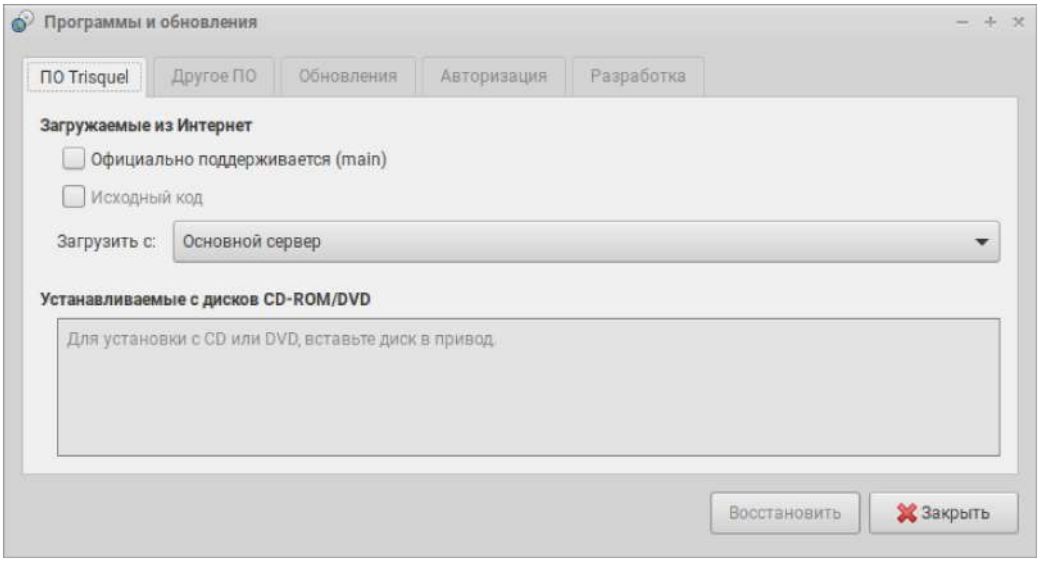
Когда установка закончится, можно приступать к обновлению системы.

Чтобы обновить систему, пройдите в Меню (кнопка в виде логотипа системы внизу слева, там же где у Windows). Там наведите мышь на категорию «Система», в нем на «Администрирование» и уже в нем на ярлык с соответствующим названием «Обновление приложений». Выскочит окно программы обновления.



Если нажать на кнопку «Параметры», откроется программа по управлению хранилищами из которых производится установка нового ПО, и обновление уже установленного. Здесь мы ничего менять не будем, просто объясню этот момент. В GNU/Linux установка программ происходит из репозиториев — хранилищ приложений. Репозитории Trisquel содержат исключительно свободное ПО, поэтому устанавливая приложения только из них, вы всегда будите иметь на своем компьютере только свободные программы. Это и есть тот простой принцип, о котором я говорил.

В первой вкладке настраивается то, в какой форме приложения загружать. Можно в виде уже скомпилированных бинарных файлов (официально поддерживаемые), или непосредственно в виде исходных кодов. А также с какого сервера загружать. Эта вкладка не выполняет своей функции, поскольку в Trisquel 11 репозитории добавлены отдельно.



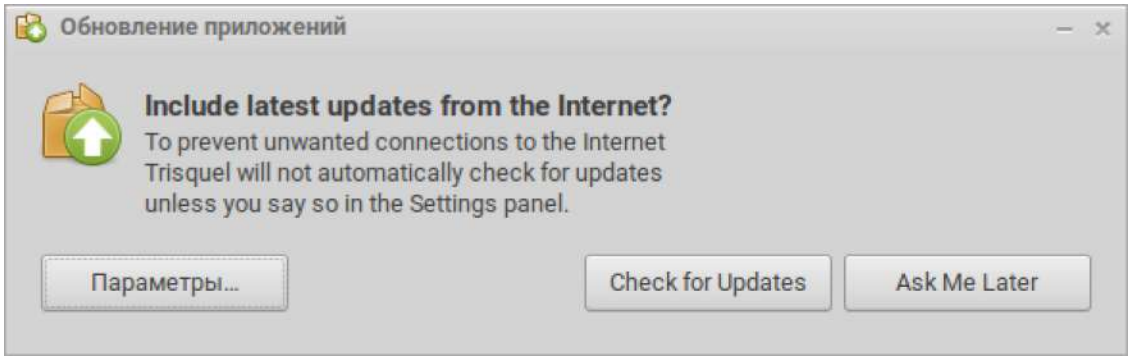
Во второй вкладке указываются непосредственно репозитории, а также другие источники. Здесь можно добавить диски или дополнительные репозитории.

В третьей вкладке настраивается из каких разделов хранилищ будет устанавливаться и обновляться ПО. Обновления безопасности, а также рекомендуемые обновления, связанные с иными аспектами приложений. Можно подключить также тестовые версии. В этом случае будут устанавливаться более свежие, но вместе с тем, нестабильные версии, поэтому по умолчанию данный раздел отключен. Также здесь настраивается автоматическая проверка обновлений и уведомление о них. Поскольку эту систему не планируется держать подключенной к Интернету постоянно, то автоматическую проверку не следует подключать. Оставляем в этом пункте «Никогда».

В четвертой вкладке настраивается проверка подлинности устанавливаемых приложений, путем сравнения электронных подписей. Это делается для того, чтобы удостовериться, что никто не подменил скачиваемые приложения по дороге от сервера до вашего компьютера. Все происходит автоматически, вам может только выскочить предупреждение, если вдруг подлинность не будет подтверждена.

В последней вкладке настройки предназначенные для продвинутых пользователей, поэтому о ней я вообще говорить не буду.

Итак, мы открыли приложение для обновления, и для начала нужно обновить сам список приложений и их версии, чтобы увидеть какие обновления вообще есть. Нажимаем «Check for Updates».

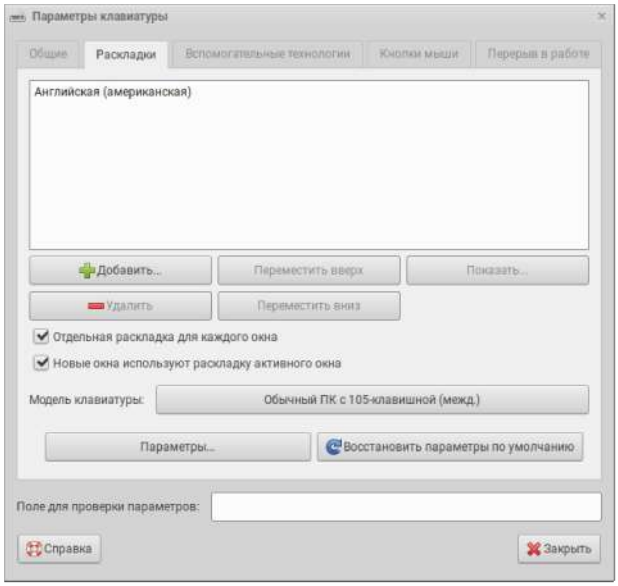


Начнется загрузка списка пакетов, после чего выскочит окошко с информацией о том, какие пакеты нужно обновить и какой объем нужно скачать. Нажимаем «Установить сейчас».

Начнется процесс скачивания и установки, после которого нужно будет перезагрузить компьютер.

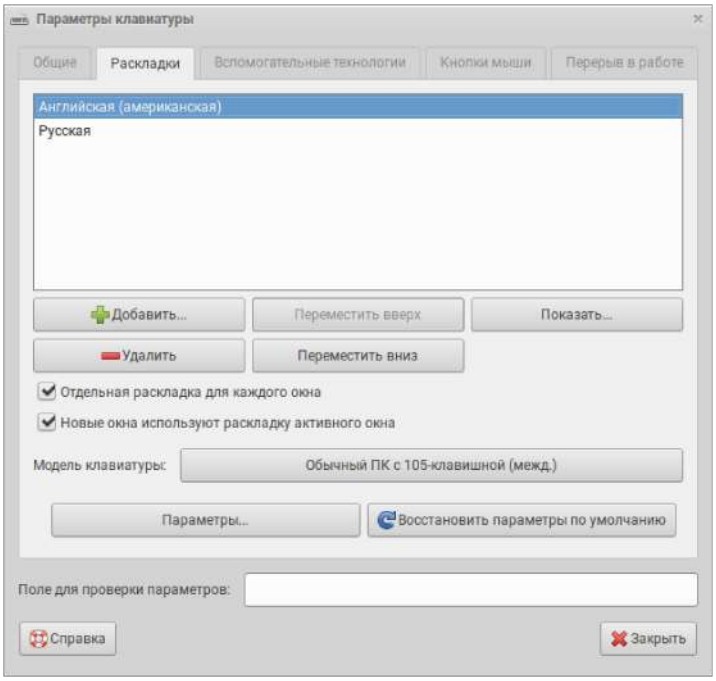
7 Добавление раскладки клавиатуры

Когда система полностью обновлена, первым делом нужно добавить раскладку клавиатуры, если она не добавилась автоматически при установке системы, чтобы мы могли вводить текст и на своем языке. Для этого открываем Меню, вкладка «Система», в ней «Оборудование», и выбираем «Клавиатура».

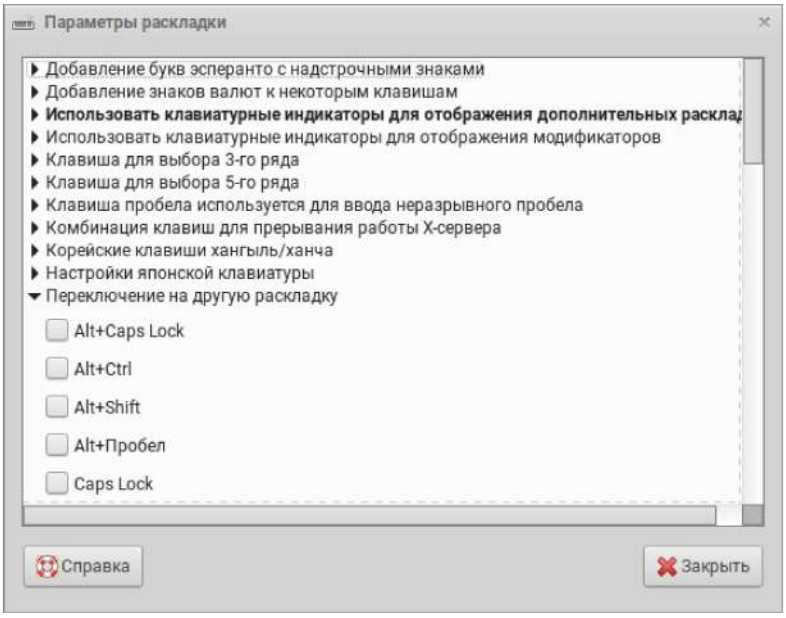


В появившемся окне нажимаем на кнопку «Добавить». В выскочившем окне наверху слева выбираем свою страну и язык и нажимаем «Добавить».

Теперь нажимаем кнопку «Параметры».



В выскочившем окне открываем вкладку «Переключение на другую раскладку» и выбираем то, которое удобнее.



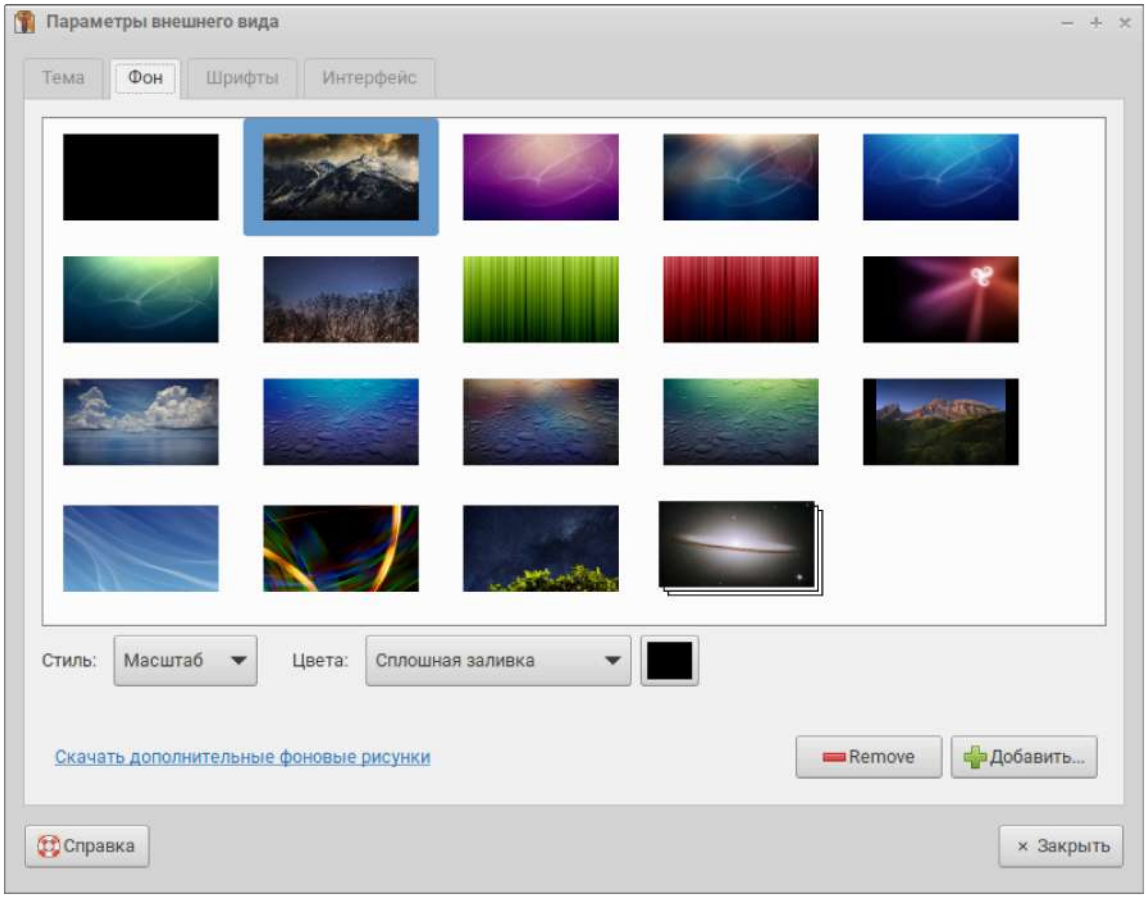
Окно можно закрыть.

8 Знакомство с операционной системой

Для начала можно посмотреть возможности по настройке дизайна. Если щелкнуть правой кнопкой мыши по панели задач и выбрать свойства, можно

настроить цвет, размер, заливку и расположение панели. На нее можно также добавить новые апплеты или удалить те, что есть.

Точно также если щелкнуть правой кнопкой мыши на рабочем столе и нажать «Настройка внешнего вида», то выскочит окно по настройке дизайна операционной системы. Можно выбрать темы, каждую из которых также можно настраивать, изменить фон рабочего стола, также шрифты и другие элементы интерфейса.



Изначально в системе Trisquel есть все что нужно для простого бытового использования компьютера. Предлагаю пробежаться по меню, чтобы посмотреть все это.

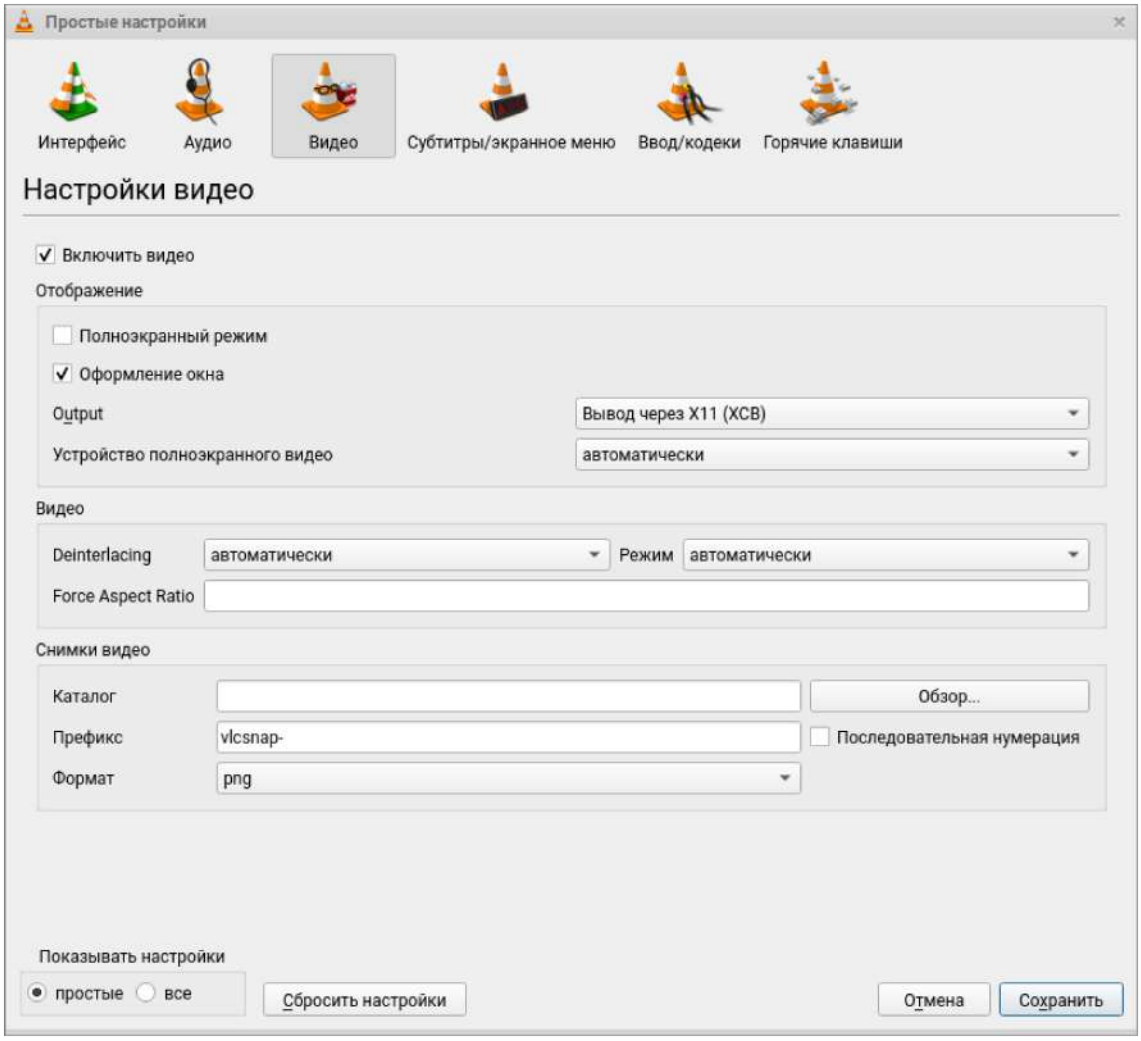
Поскольку данную систему не планируется держать подключенной к Интернету, категорию «Интернет» я рассматривать не буду. Напоминаю, что Интернет-активность мы будем осуществлять только из-под виртуальных машин, а основную операционную систему подключать к Интернету только для обновления и установки нового ПО.

В категории «Офис» находится набор офисных программ. Здесь установлен пакет LibreOffice.[5] В данном пакете есть все необходимые программы. Writer — программа для создания и редактирования текстовых документов, аналог Word. Calc — создание электронных таблиц, проведение самых разных вычислений, аналог Excel. Impress — создание и редактирование презентаций, аналог PowerPoint. Также есть Draw — создание и редактирование рисунков, блок-схем.

В категории «Графика» находятся программы для взаимодействия с графическими изображениями. Программа «Выбор цвета MATE» это просто утилита для управления цветом, которую используют другие программы. Viewnior предназначен для просмотра изображений. «Графический редактор GIMP», это редактор графических изображений, аналог Photoshop.[6] Это весьма мощный инструмент с огромным набором функций.[7] «Сканер документов», это утилита для сканирования документов и изображений, с помощью сканера.

В категории «Аудио и видео» находятся программы, как не трудно догадаться, для работы с видео и аудио. Brasero позволяет записывать CD и DVD диски. Chesse это программа для создания снимков при помощи веб-камеры. Здесь же находится приложение для регулировки звука. Также медиаплеер VLC, который, наверное, знаком многим, кто до этого не интересовался свободным ПО.[8]

О плеере VLC нужно сказать отдельно. Данный плеер позволяет не только смотреть видео и слушать аудио, но также в нем присутствует возможность конвертации файлов и даже некоторые функции редактирования. Однако, может возникнуть проблема с воспроизведением видео. Тогда войдите в графу «Инструменты» и выберите категорию «Настройки». В открывшемся окне, откройте вкладку «Видео» и в графе «Вывод» поставьте «Вывод через X11 (XCB)». После этого видео должно проигрываться нормально.



В категории «Игры» находятся, собственно, игры. Тут есть «Пасьянс Айслериот» в котором собрано полтора десятка различных пасьянсов. Есть «Мины», аналог «Сапера». С остальным любители играть сами разберутся.

В категории «Стандартные» находятся базовые прикладные программы, такие как калькулятор, простенький текстовый редактор Pluma и т.п.

В категории «Прочее» находятся иные прикладные программы различного назначения. Среди них отдельно стоит отметить «Системный монитор MATE». Крайне полезная программа. Если ее запустить, то на первой вкладке отображаются данные об операционной системе и оборудовании. Во второй вкладке показано, какие процессы активны и сколько они потребляют ресурсов, а также можно управлять процессами, приостановить, прервать и т.д. В третьей вкладке идут графики. Наверху загруженность процессора. Для каждого ядра идет отдельный график. Под ним загруженность оперативной памяти и файла подкачки. Внизу Интернет-трафик, отдельные графики для входящего и

исходящего трафика. В четвертой вкладке отображаются подключенные диски и разделы, указано, сколько места на них занято, а сколько свободно.

Программа «Установка/удаление приложений», это менеджер для поиска, установки и удаления программ. К нему мы вернемся позже.

Категория «Переход» позволяет переходить по каталогам файлов, открывая файловый менеджер. Также его можно открыть, если нажать на иконку на панели задач возле меню.

В категории «Система» находятся приложения для настройки системы. Она в свою очередь разбита по категориям и, в принципе, интуитивно понятна. По категориям «Параметры» и «Администрирование» разбросаны все программы для настройки. «Центр управления» открывает окно, в котором находятся сразу все настройки.

Если у вас после обновления имеются проблемы с отображением на экране, то можно попробовать разрешить это, установив более свежие версии драйверов для графических ускорителей из сторонних репозиториев.[9] Также это может помочь, если вы при работе наблюдаете периодические зависания. К сожалению, полноценное добавление репозиториев (включающие импорт ключей для проверки подлинности приложений) в данной ОС возможно только через терминал. Поэтому, будучи в нем, набираем строчку

```
sudo add-apt-repository ppa:graphics-drivers/ppa
```

И нажимаем «Enter». После этого, нужно будет ввести пароль root и снова нажать «Enter». Когда появится строка с надписью «Нажмите [ENTER] чтобы продолжить или Ctrl-C для отмены добавления», нажимаем «Enter». Произойдет импорт ключей, и репозиторий будет добавлен.

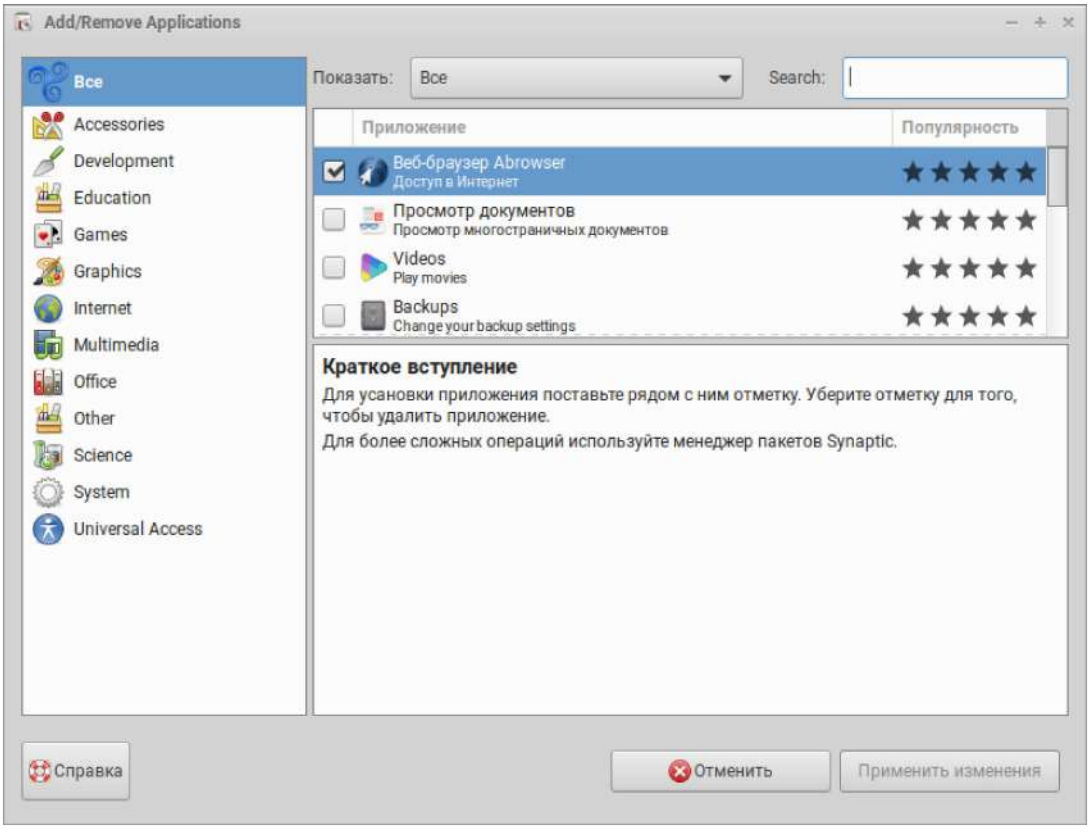
Терминал можно закрыть. Теперь снова необходимо произвести обновление системы и перезагрузить компьютер. Если после перезагрузки проблемы с графикой не исчезли, то можно попробовать настроить конфигурационные файлы. Но здесь все зависит от конкретной модели видеокарты, поэтому решение придется искать в Интернете. Если и эти методы не помогают, то единственным выходом остается установка проприетарного драйвера. Такие драйвера есть в том репозитории, который был подключен последним. К этому варианту я рекомендую обращаться только в самом крайнем случае. Как устанавливать программы (в том числе драйвера) из

репозиториев будет рассказано далее.

Теперь можно заняться установкой приложений, которых в системе изначально нет, но которые могут понадобиться.

9 Установка программ

Итак, открываем Меню и запускаем «Установка/удаление приложений». Открывается окно, в котором слева указаны категории, а в основной части идет список самих приложений. Пара слов о самом менеджере. Он весьма удобен в использовании, если вы точно знайте название нужной вам программы, или просто просматриваете категории в поисках того, что приглянется. Но у него есть свои минусы. Во-первых, для многих приложений отсутствуют описания. Во-вторых, при поиске по ключевым словам, т.е. когда вы не знайте точного названия нужной вам программы, он не всегда бывает понятливым. Также пароль необходимо вводить при установке каждой отдельной программы.



Первое приложение, которое нам следует установить, это Bleachbit. Я уже упоминал его. Оно используется для чистки системы от мусора, такого как содержимое кеша, временные файлы и т.д. Кроме того, с помощью него можно

не просто удалять файлы, а затирать их. Однако, сейчас я не буду отвлекаться и объяснять что это такое, о том как работать с Bleachbit будет сказано отдельно. Сейчас же набираем в строке поиска «Bleachbit», ставим галочку на появившемся приложении и нажимаем кнопку «Применить изменения». При этом нужно будет ввести пароль. Как я и говорил, его нужно будет вводить каждый раз, когда делаются какие-то изменения в системе, к примеру, устанавливаются новые приложения.

Следующая программа, которая может оказаться крайне полезной GParted. [10] Это программа для работы с дисками и их разделами. Создавать, редактировать, удалять, форматировать в самые разные форматы, все это позволяет программа GParted. На самом деле мы уже фактически ей пользовались, когда размечали диск для установки системы. Так что в общих чертах часть ее функционала вы представляете. Процедуру установки снова повторять не стану, думаю, она ясна.

Еще одно крайне полезное приложение HardInfo. Искать ее лучше именно по этому названию. Однако в списке приложений она может отобразится как «Информация о системе и тестирование». Данная программа позволяет просматривать во всех подробностях сведения о системных характеристиках, а также о каждом составляющем оборудования, таком как процессор, оперативная память, видеокарта, дисковод и т.д. Ищем в строке поиска и устанавливаем.

Также есть приложение ZuluCrypt. Позволяет шифровать файлы, каталоги, разделы или целые накопители. В нем присутствует также и система отрицаемого шифрования.[11]

И наконец, Virtual Mashine Manager.[12] Менеджер виртуальных машин, с помощью которого мы будем создавать виртуальные машины из-под которых будем осуществлять Интернет-активность.

Мы установили большую часть необходимых нам программ, однако вы можете поискать в менеджере то, что еще вам нужно. Например, можете добавить программы из пакета LibreOffice. Base — создание баз данных и управление ими, аналог Access. Math — создание и редактирование научных формул и уравнений. Если вы занимаетесь видеомонтажем, делаете фильмы, вы можете найти различные видеоредакторы. Пожалуй самым продвинутым является Flowblade.[13] Если занимаетесь аудиомонтажем, пишите музыку, можете найти звуковые редакторы, к примеру Audacity.[1] И нотный редактор

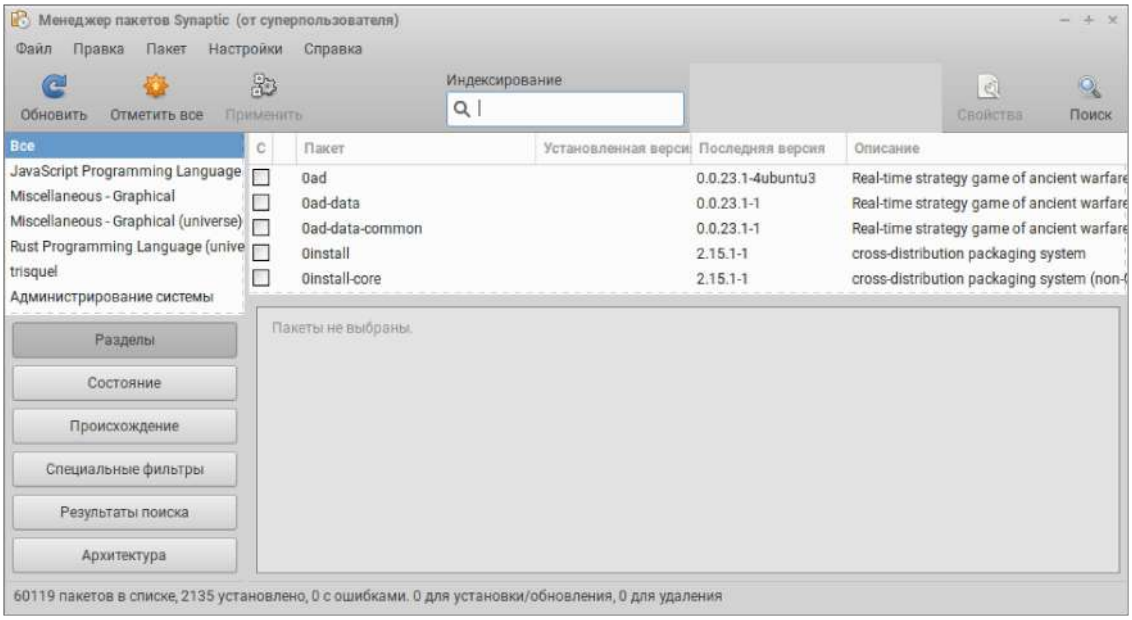
MuseScore.[2]

Тут необходимо сделать отступление и рассказать о форматах видео и аудио. Форматы также бывают свободные и несвободные. Обычно под словом «формат» простой обыватель понимает то, что написано в заголовке файла после его названия, т.е. расширение. На самом деле расширение только указывает с помощью какой программы данный файл можно открыть. Видео и аудио кодируются при помощи определенных кодеков. И будучи закодированными этими кодеками, могут быть помещены в контейнеры. «Формат» mp3 на самом деле является одним из кодеков аудио. В свою очередь, аудиозаписи, закодированные данным кодеком могут быть помещены в контейнер, например mpeg. В случае видео контейнер будет содержать как видео, закодированное к примеру кодеком Divx, так и аудиодорожку, закодированную, например, также mp3. Таким контейнером является, например, mp4. Повторяю для ясности, mp3 кодек аудио, mp4 контейнер, в который помещены видео и аудио, закодированные какими-либо кодеками.[3] Все перечисленные кодеки и контейнеры являются проприетарными. Поэтому, если вы занимаетесь созданием видео или аудио, рекомендую присмотреться к свободным кодекам и контейнерам, и стараться использовать именно их в своей деятельности. Свободным кодеком видео является Theora.[4] Также Dirac, который разработан для высококачественного видео.[5] А также VP9, который является наиболее распространенным кодеком видео на Интернет-сайтах.[6] Свободными кодеками аудио являются Vorbis[7] и Opus,[8] а также FLAC,[9] кодирующий аудио без потерь. Свободный контейнер, в свою очередь, Ogg.[10] При помещении в него видео, расширение будет .ogv, а с аудио .oga. Данный контейнер отличается тем, что в него можно засунуть только свободные кодеки. Еще один свободный контейнер Matroska.[11] Расширение его для видео будет .mkv, а для аудио .mka. В этот контейнер уже можно запихнуть любые кодеки, не только свободные. Также существует контейнер WebM, который наиболее распространен на страницах сайтов в Интернете.[12] Существуют и иные свободные кодеки и контейнеры, но эти наиболее распространенные.

Если вы делаете чертежи, то этичной заменой проприетарным AutoCAD и Компасу станет LibreCAD.[13] Если вам приходится заниматься 3D-моделированием, обратите внимание в первую очередь на программу Blander.[14] Вы можете найти и приложения для узкой научной деятельности. К примеру

для моделирования механики твердого тела есть программа CalculiX.[15] А для расчетов механики сплошных сред OpenFOAM.[16] Есть даже прошивки для специального оборудования. Кто знает, возможно вы работаете именно на том калориметре или хроматографе, программы для управления которыми есть в репозиториях Trisquel. Есть немало программ для математических расчетов и моделирования. И конечно, множество приложений для программирования.

С менеджером приложений мы работу закончили, однако, нам нужно установить еще кое-какие программы. Менеджер приложений предлагает только сами приложения. Он не рассчитан на работу с отдельными пакетами и даже полные приложения отображает не все. В Trisquel есть и другой менеджер пакетов Synaptic. Заходим в Меню, категория «Система», затем «Администрирование» и выбираем «Менеджер пакетов Synaptic». Для запуска программы набираем пароль. В данном менеджере его не придется вводить при установке каждого пакета. Открывается окно Synaptic. Данный менеджер менее интуитивен, однако у него есть ряд преимуществ. Он отображает действительно все пакеты, находящиеся в хранилищах. В нем лучше работает поиск по ключевым словам. Он работает с отдельными пакетами, и вы всегда можете увидеть в подробностях, какие компоненты вам устанавливаются.



Если вам нужно установить драйвер для графического оборудования, то можете поискать его здесь. Для этого нажимаем «Поиск» и набираем в открывшемся окне название производителя вашей видеокарты. Нажимаем

«Enter», затем щелкаем правой кнопкой мыши на появившийся в списке пакет с соответствующим названием. Выбираем «Установить». Выскочит окно, в котором будет показываться, какие еще пакеты будут установлены и сколько для этого будет скачано. Нажимаем «Ok». Когда пакеты отмечены, нажимаем кнопку «Применить». Начнется скачивание и установка. Когда все будет установлено, выскочит уведомление. Нажимаем «Ok». Здесь же можно найти драйвера для другого оборудования. Их ищите по названиям этого оборудования.

Нужно установить кое-какие пакеты для программы виртуализации, чтобы она могла полноценно работать. Для этого ищем и устанавливаем пакет qemu по вышеописанной методике. При установке к нему подтянутся другие пакеты.

Нам нужно установить Firewall. В менеджере приложений есть межсетевые экраны, но они крайне неудобные. Мы будем устанавливать ufw, с графической оболочкой. Набираем в строке поиска gufw и устанавливаем соответствующий пакет.

К сожалению, ни одна система не застрахована от сбоев. И последствия сбоя, если он произойдет, могут закрепиться в системе надолго. Решить такую проблему может откат системы к состоянию, предшествовавшему сбою. Поэтому сейчас мы будем устанавливать приложение именно для этого. Наиболее удобной программой является TimeShift.[17] В строке поиска набираем TimeShift, выбираем среди выпавших результатов пакет с соответствующим названием и устанавливаем. После установки программу можно закрыть.

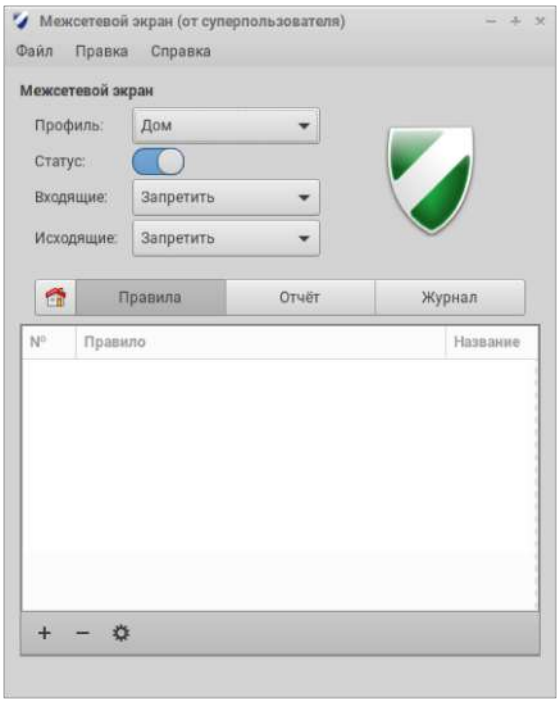
Теперь, когда все необходимое установлено, нужно перезагрузить систему, затем снова войти в Synaptic и удалить пакет virt-viewer, который был установлен вместе с программой виртуализации. Это инструмент удаленного управления ей. Он нам не нужен и при этом является потенциальной дырой в безопасности. После этого Synaptic можно закрыть. Теперь необходимо настроить межсетевой экран.

10 Настройка Firewall

Открываем Меню, категория «Система», в ней «Параметры», затем «Интернет и сеть», там «Межсетевой экран».

Существует две методики настройки. По одной, трафик по умолчанию разрешается, и устанавливаются отдельные запретительные правила. По другой, весь трафик запрещается, а устанавливаются отдельные разрешающие правила.

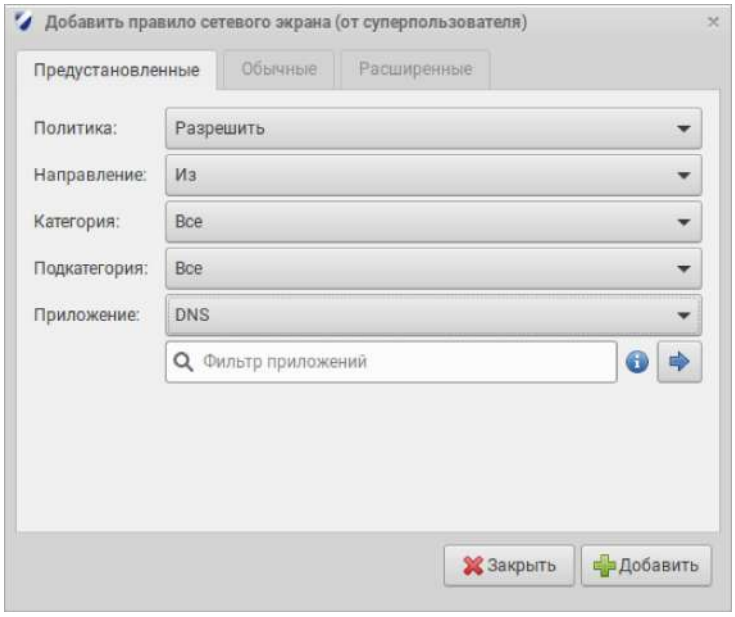
Мы будем действовать именно по второй методике. Первое, что нужно сделать, после того, как открылось окно, передвинуть ползунок вправо в графе «Статус» чтобы включить Firewall. Затем как для входящего, так и исходящего трафика поставить «Запретить».



Теперь, когда весь трафик запрещен, сетевое соединение полностью заблокировано. Нужно устанавливать правила. Открываем вкладку «Правила» и нажимаем на знак плюс (+). В открывшемся окне, в графе «Направление» ставим «Из», чтобы трафик был только исходящим (входящий запрещен), а в «Приложение» выбираем DNS. Поясню, что это такое.

Как уже было сказано, сайты в Интернете имеют ip-адреса и именно по ним обращаются при переходе на сайт. Но ip это последовательность цифр, тогда как сайт всегда имеет буквенное название. DNS-сервер, это по сути, хранилище, справочник, где указано, по какому ip-адресу находится какой сайт. И когда вы идете на какой-то сайт, обращаясь по его имени, например gnu.org, ваш компьютер сначала спрашивает DNS-сервер, — по какому адресу находится данный сайт. И получив ответ (ip-адрес), идет на него. Без включения запросов DNS по Интернету гулять будет невозможно.

Когда все выставлено, нажимаем кнопку «Добавить». Окно при этом не закроется, и не выскочит никого уведомления, но правила добавятся.



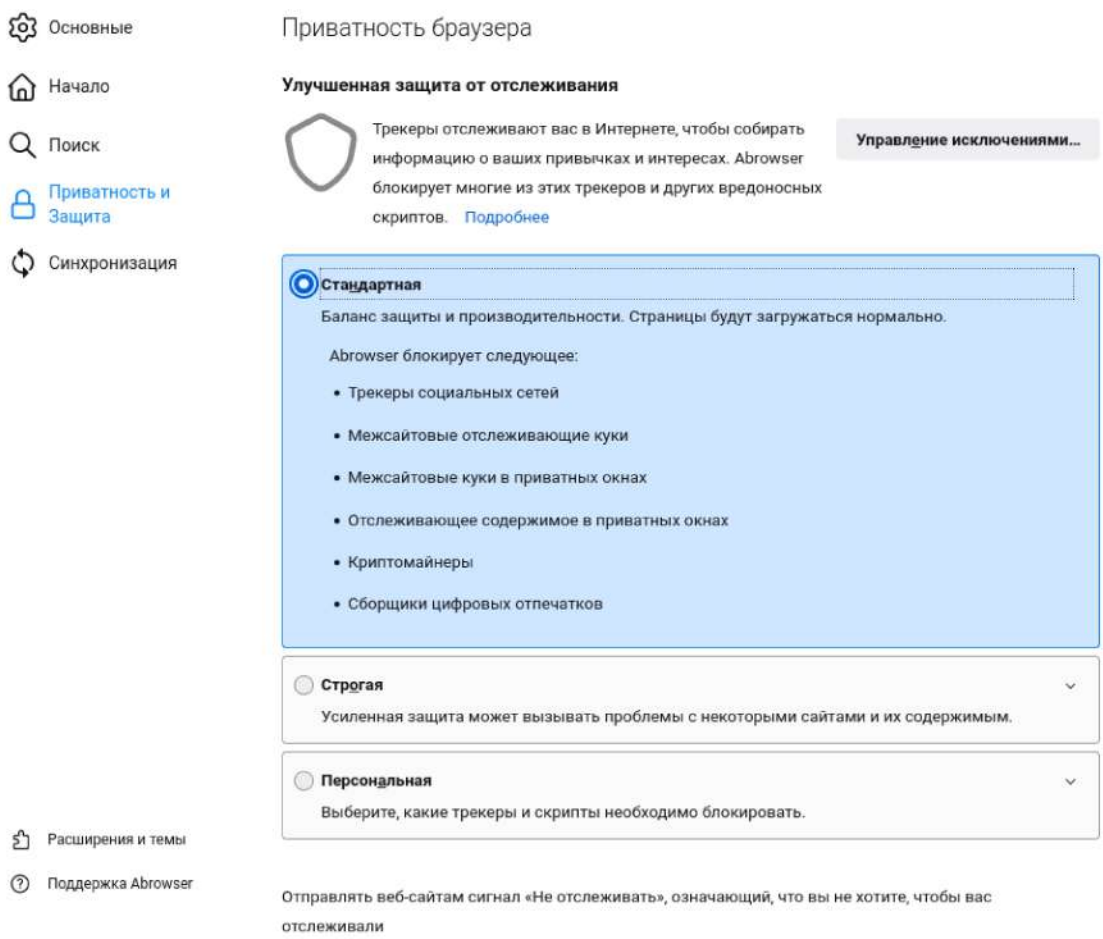
Теперь в строке «Приложение» выбираем HTTP — обычный Интернет-протокол, и также его добавляем. А затем HTTPS — шифрованный Интернет-протокол.

После того как все правила добавлены можно закрыть окно Firewall. Этого вполне достаточно в основной системе, для обновления и установки нового ПО, а также для Интернет-поисков, в случае их острой необходимости, при отсутствии пока еще виртуальных машин. Именно для такого экстренного случая мы сейчас и настроем браузер.

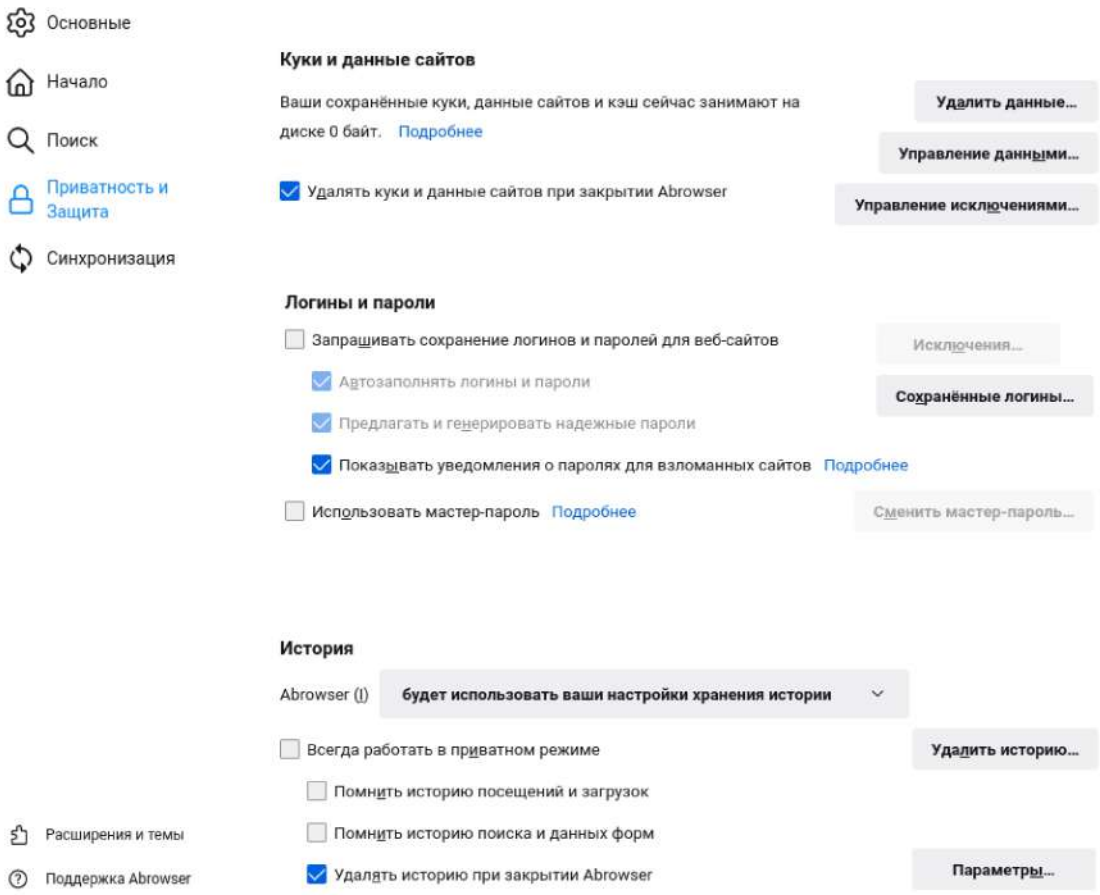
11 Настройка браузера

На панели задач, возле значка файлового менеджера, возле Меню, значок браузера. Нажимаем на него. Открывается окно Интернет-обозревателя. В Trisquel предустановлен Abrowser. Он основан на Firefox, единственном из широко известных браузеров, который является свободным и приемлемым для использования.[18] Основным отличием от последнего является отсутствие на странице поиска расширений несвободных расширений. В остальном Abrowser полностью ему аналогичен. Гибок в настройке интерфейса, функционала, в том числе, за счет установки расширений из хранилищ Mozilla. Однако, данный браузер, также как и Firefox по умолчанию не подходит для Интернет-серфинга. Его необходимо настроить.

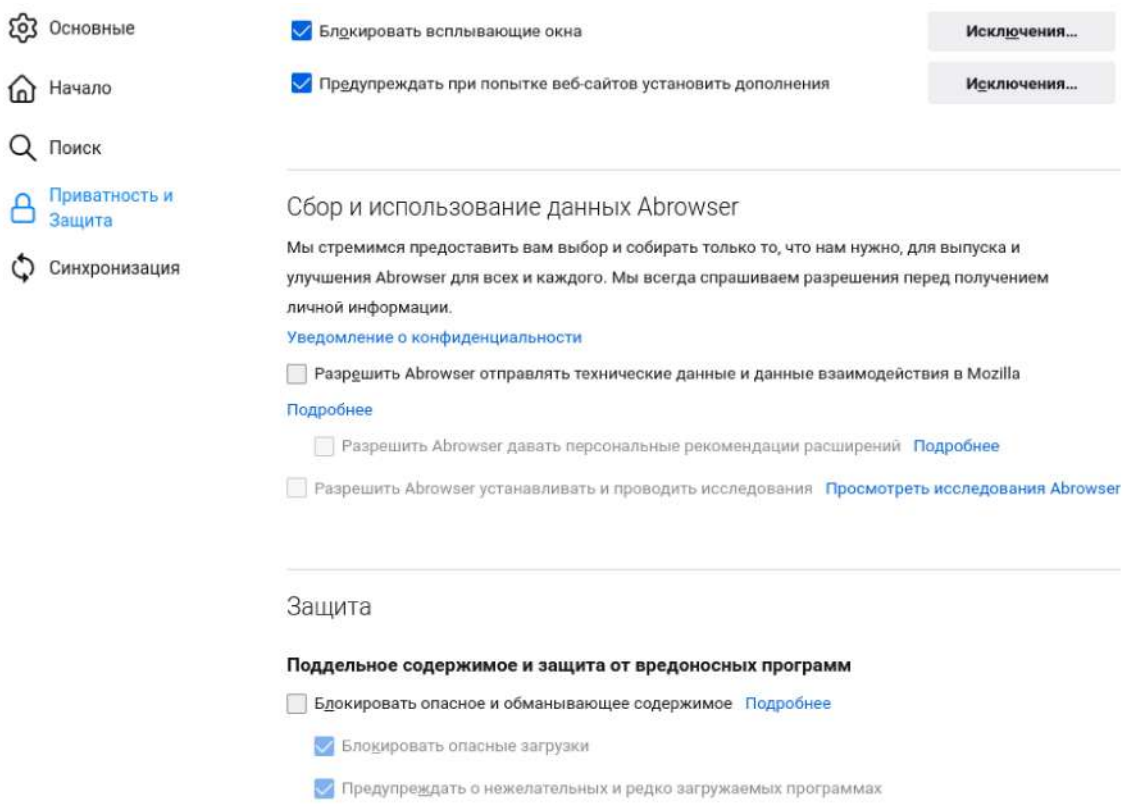
Открываем наверху справа меню, находим и нажимаем «Настройки». В появившемся окне идем во вкладку «Приватность и защита». Здесь выбираем «Стандартная».



Ставим галочку на «Удалять куки и данные сайтов при закрытии Abrowser». Снимаем галочку с пункта «Запрашивать сохранение логинов и паролей для веб-сайтов», если она стоит. Выбираем «будет использовать ваши настройки хранения истории». Ставим галочку на «Удалять историю при закрытии Abrowser». Остальные галочки должны быть сняты.

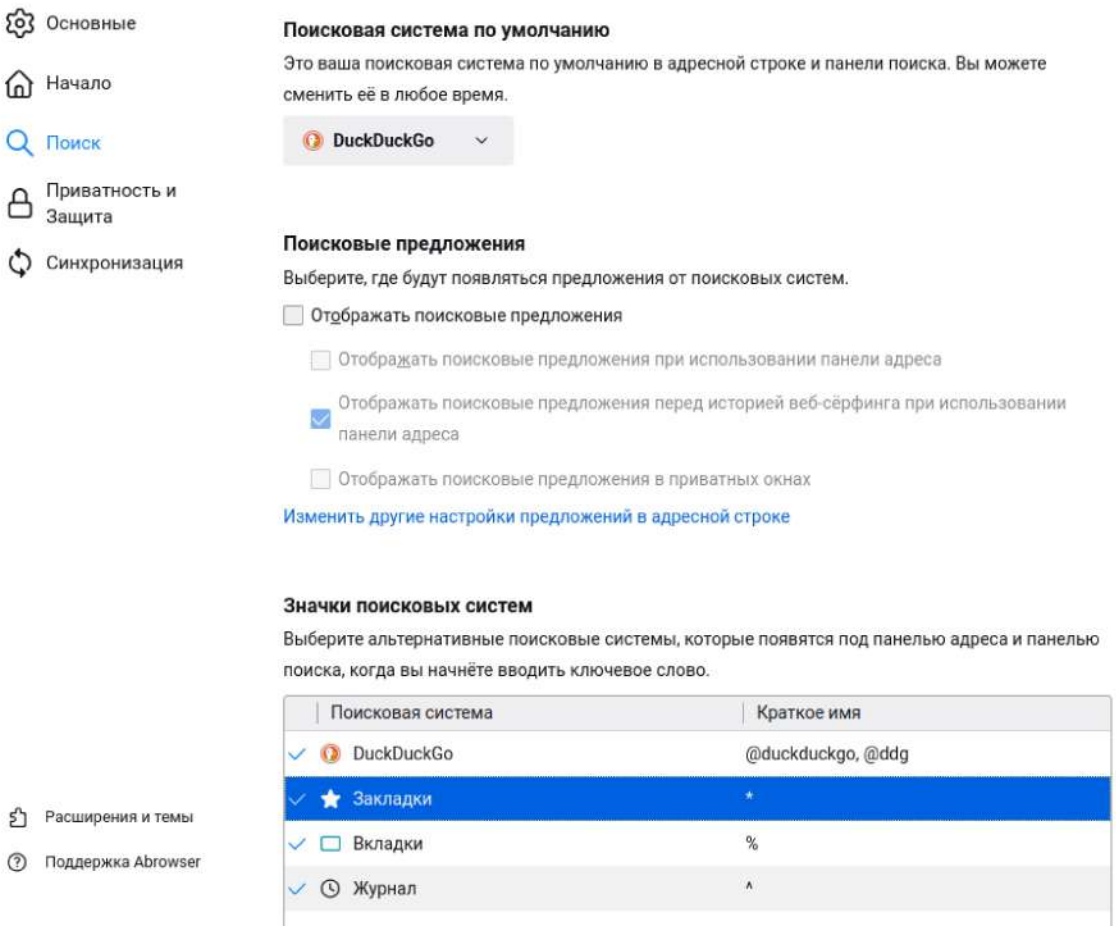


Проверяем, чтоб не стояла галочка на «Блокировать опасное и обманывающее содержимое». Данная блокировка осуществляется за счет проверки на упоминание сайта в черных списках, которые предоставляются сервисами Google. Эти списки хранятся и сверяются локально (происходит лишь периодическое скачивание их с серверов Google). Однако хеши загрузок сверяются удаленно. Таким образом, можно говорить, что данная функция, во-первых, осуществляет взаимодействие с Google, что уже не очень хорошо. Во-вторых, через нее в некоторой степени, реализуется слежка со стороны корпорации. В-третьих, это замедляет скорость взаимодействия с сайтами, не сильно, конечно, но все-таки. При этом, никакой реальной необходимости в данном функционале нет. С хоста мы будем посещать только проверенные сайты (например для скачивания драйверов), кроме того, без необходимости не будем включать скрипты (о том, что это значит, я скажу далее). А в дальнейшем, когда будем серфить из-под виртуальных машин, для нас вредоносный функционал сайтов уже будет не особо существенен.



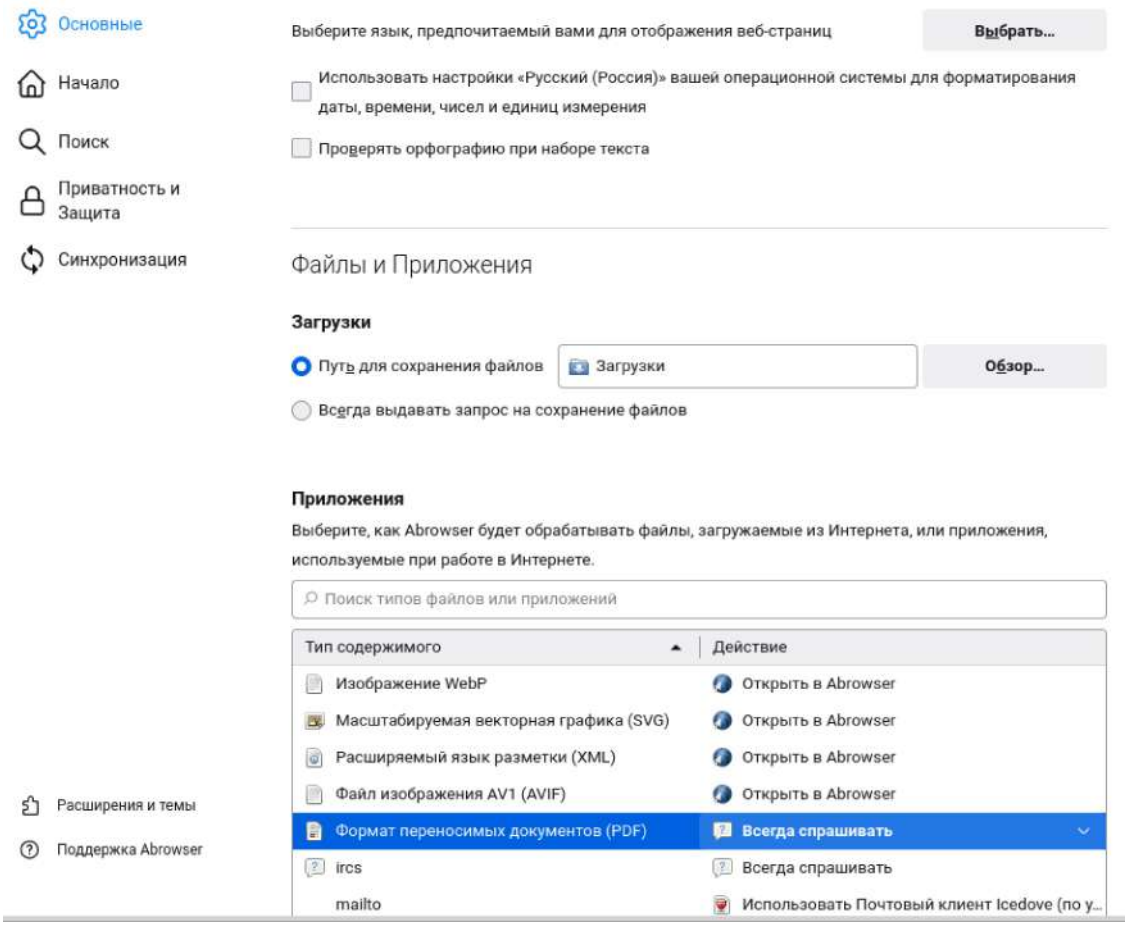
Также снимаем галочку с «Запрашивать у OCSP-серверов подтверждение текущего статуса сертификатов». С помощью этой функции проверяется действенность сертификатов шифрования используемых сайтами. В ходе этой проверки устанавливается соединение с сервером, имеющим сведения о сертификатах. И соответственно, им становится известно о том, какие ресурсы вы посещаете. Поскольку отзывы сертификатов явление довольно редкое, данная функция обеспечивает скорее слив информации, чем безопасность.

Во вкладке «Поиск» проверяем, чтобы в качестве поисковой системы по умолчанию стояла DuckDuckGo. Снимаем галочку с «Отображать поисковые предложения», т.к. данная функция также может быть использована для отслеживания. И среди поисковых систем вычищаем все. Оставляем только DuckDuckGo и Trisquel. Также можете оставить Википедию. Остальные поисковики, такие как Google и Яндекс, шпионят и не подходят для использования. О поисковиках я еще расскажу отдельно.

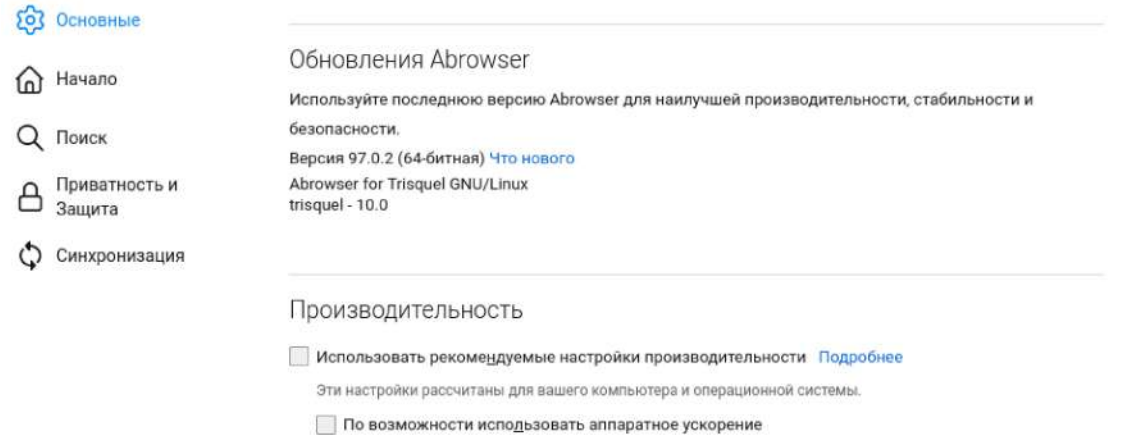


Во вкладке «Начало» все оставляем без изменений, или настраивайте, как вам нужно.

Во вкладке «Основные» снимаем галочку с «Проверять орфографию при наборе текста. Там где «Приложения», у «Portable Document Format (PDF)» меняем действие на «Всегда спрашивать», т.к. данный тип документов может быть использован для проведения вредоносных действий.



Снимаем галочку с «Использовать рекомендуемые настройки производительности» и «По возможности использовать аппаратное ускорение», т.к. в этом случае задействуется видеокарта, и появляется потенциальная возможность считать ее характеристики, и таким образом, еще раз вас пометить и идентифицировать.



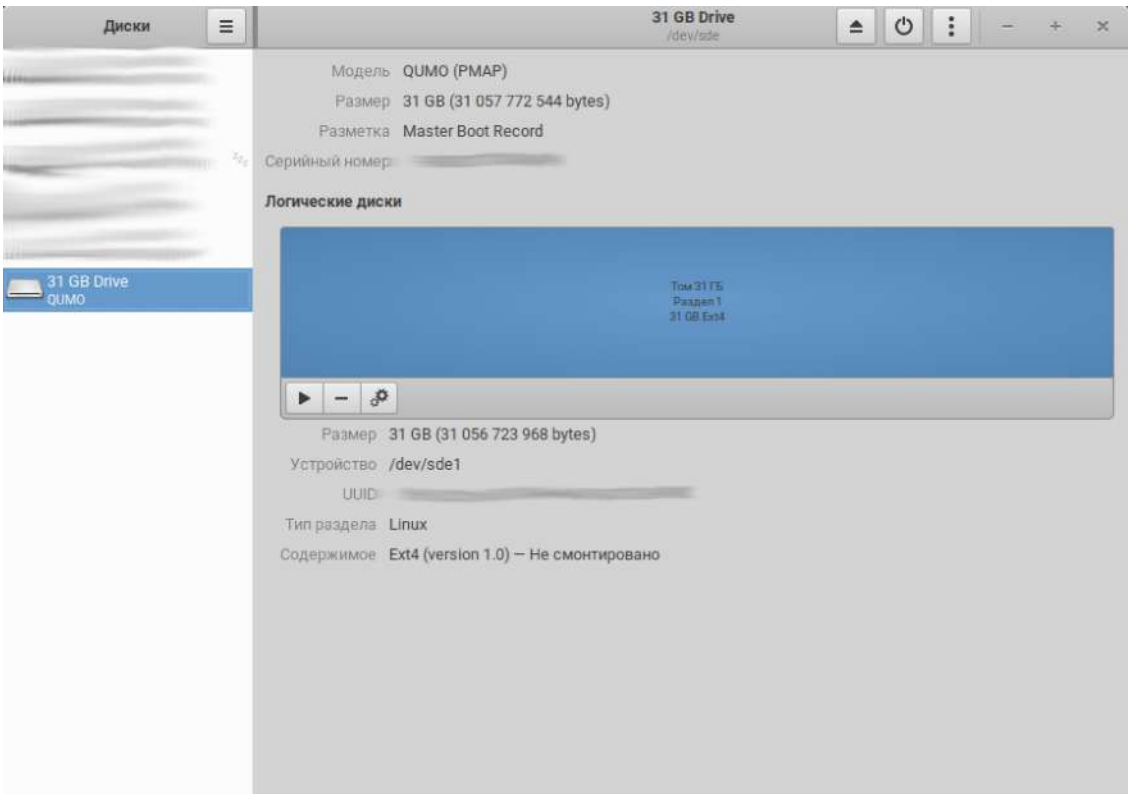
После проделанных настроек, браузер следует перезагрузить.

В принципе, этих настроек достаточно для этого браузера. Поскольку мы не собираемся использовать его на постоянной основе, настраивать его более серьезно нет необходимости. Более серьезная настройка будет показана, когда речь пойдет о виртуальной машине, из которой мы будем осуществлять Интернет-активность.

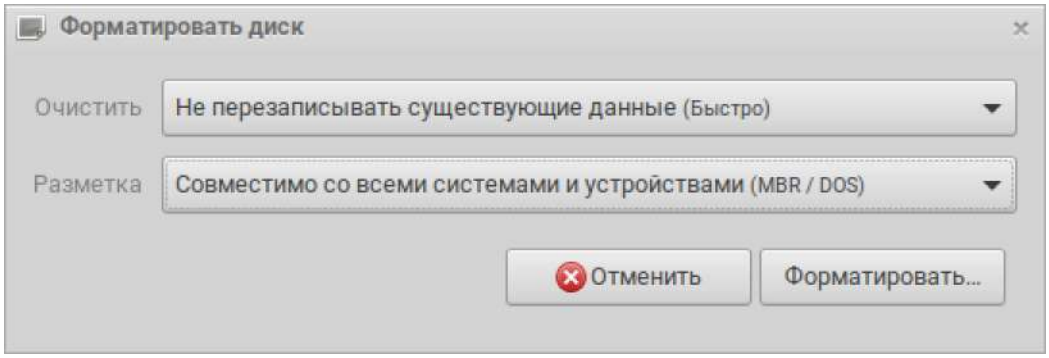
12 Шифрование носителей

Сейчас я хотел бы показать, как шифровать отдельные накопители. Это особенно актуально для тех, кто установил систему на SSD, а для файлов хочет использовать HDD. Но также этот способ подходит для шифрования любого отдельного носителя, будь то жесткий диск, флешка, SD-карта или SSD. Предупреждаю, что накопитель, зашифрованный подобным образом, можно будет расшифровать и открыть только в среде GNU/Linux. В операционных системах Windows или MacOS, этого сделать не получится. Для этого мы будем использовать программу «Диски», которая по-умолчанию установлена в Trisquel.

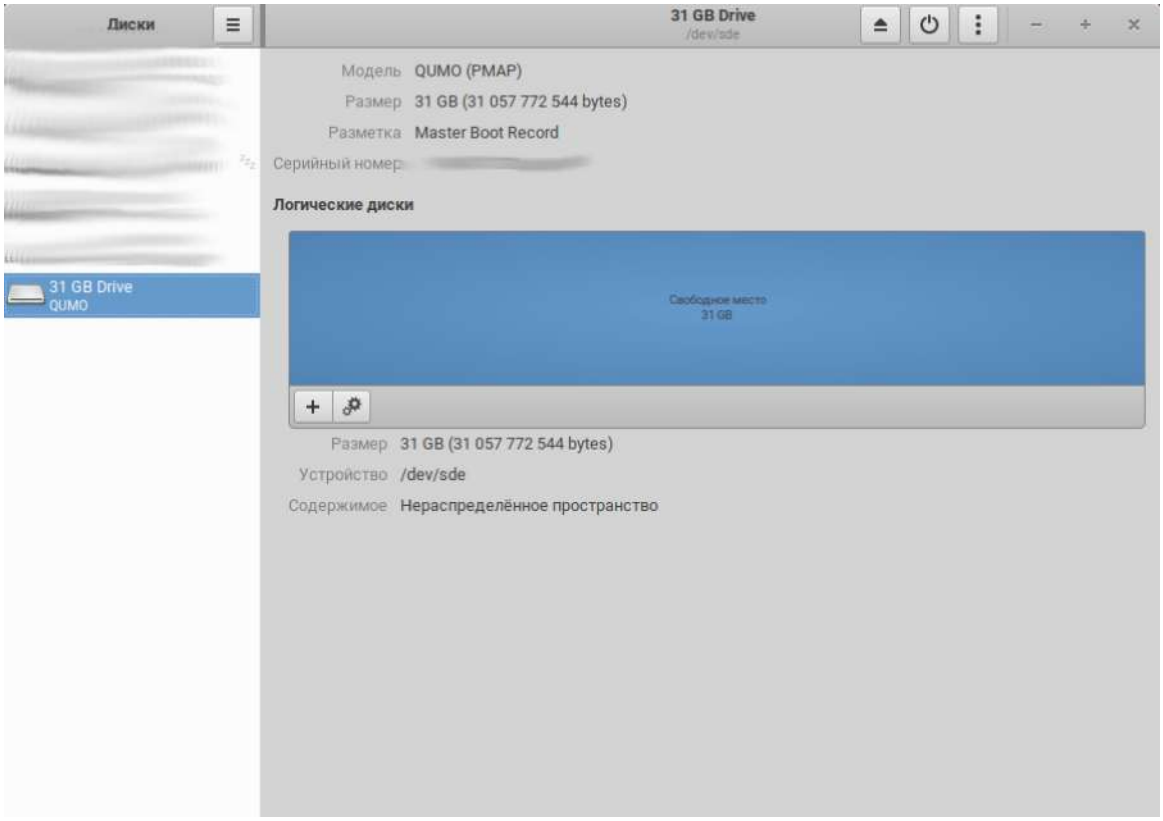
Идем в Меню, категория «Администрирование» и выбираем «Диски». Открывается окно программы, в котором в поле слева нужно выбрать тот носитель, который вы хотите зашифровать.



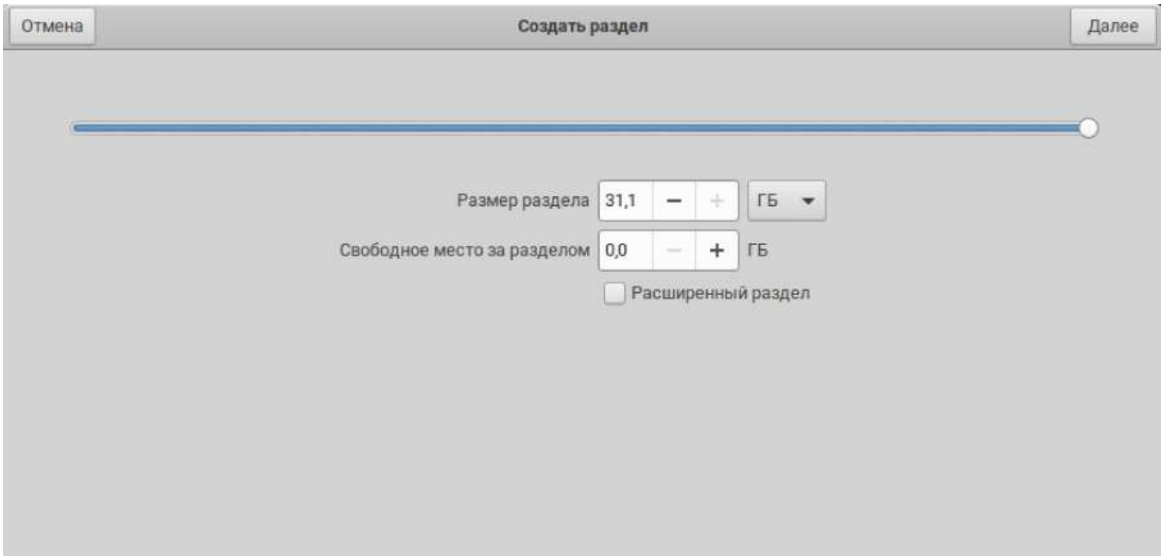
После этого, нажимаем на кнопку с тремя полосками вверху справа и выбираем «Форматировать диск». Выскочит окно, в котором в верхнем поле указываем «Не перезаписывать существующие данные (быстро)», а в нижнем, если объем диска менее 2 Тб, указываем MBR, если более, то GTP.



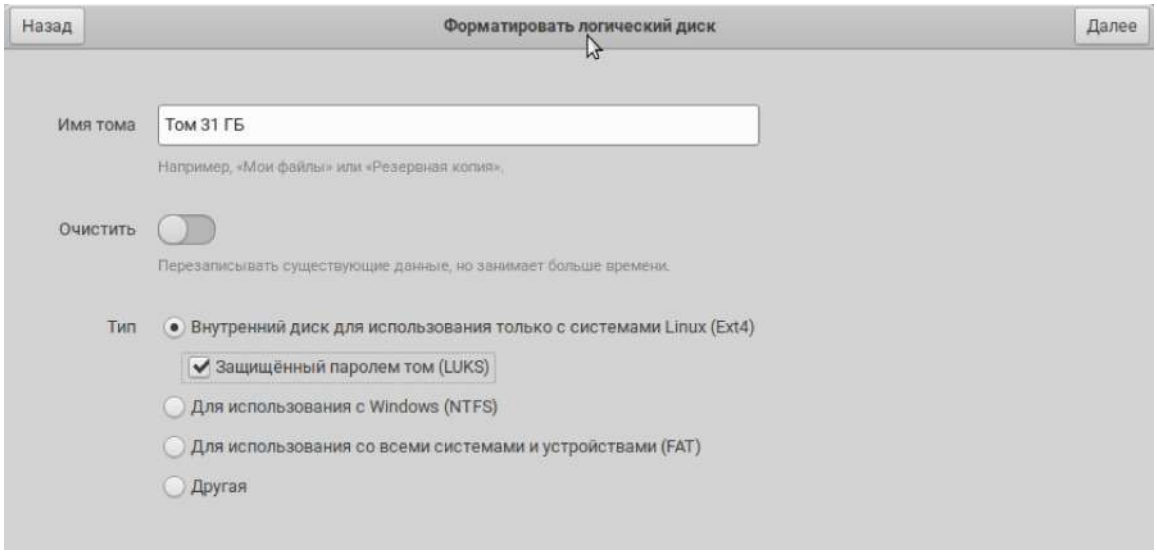
Нажимаем «Форматировать». Выскочит запрос на подтверждение форматирования. Нажимаем «Форматировать». Устройство станет пустым.



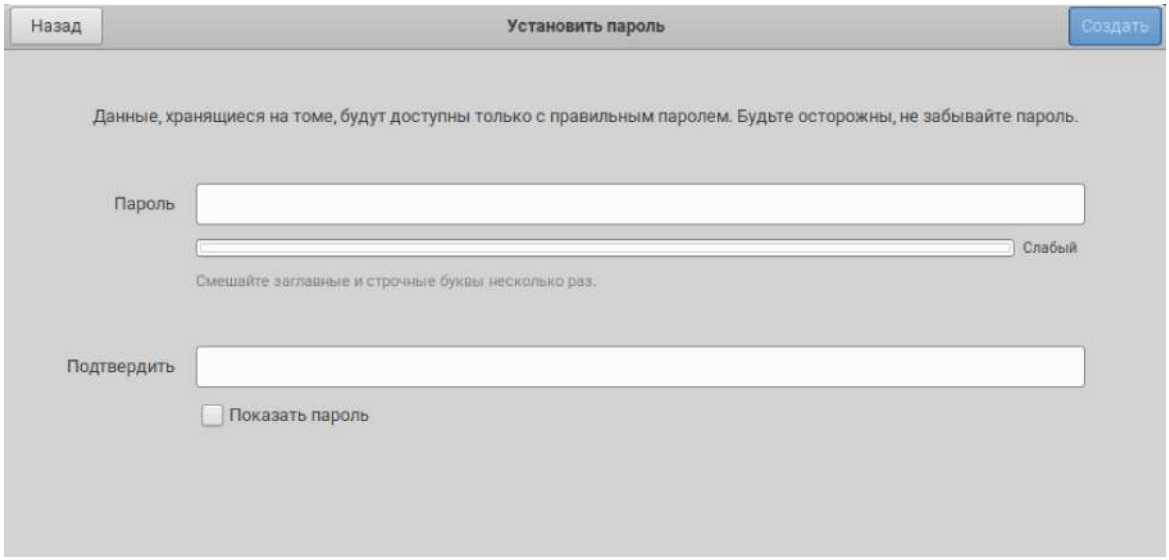
Теперь необходимо создать раздел с файловой системой. Нажимаем значок «плюс» слева под обозначением дискового пространства. Выскочит окно, в котором необходимо указать размер раздела. Если не хотим разбивать носитель на разделы, то оставляем все пространство.



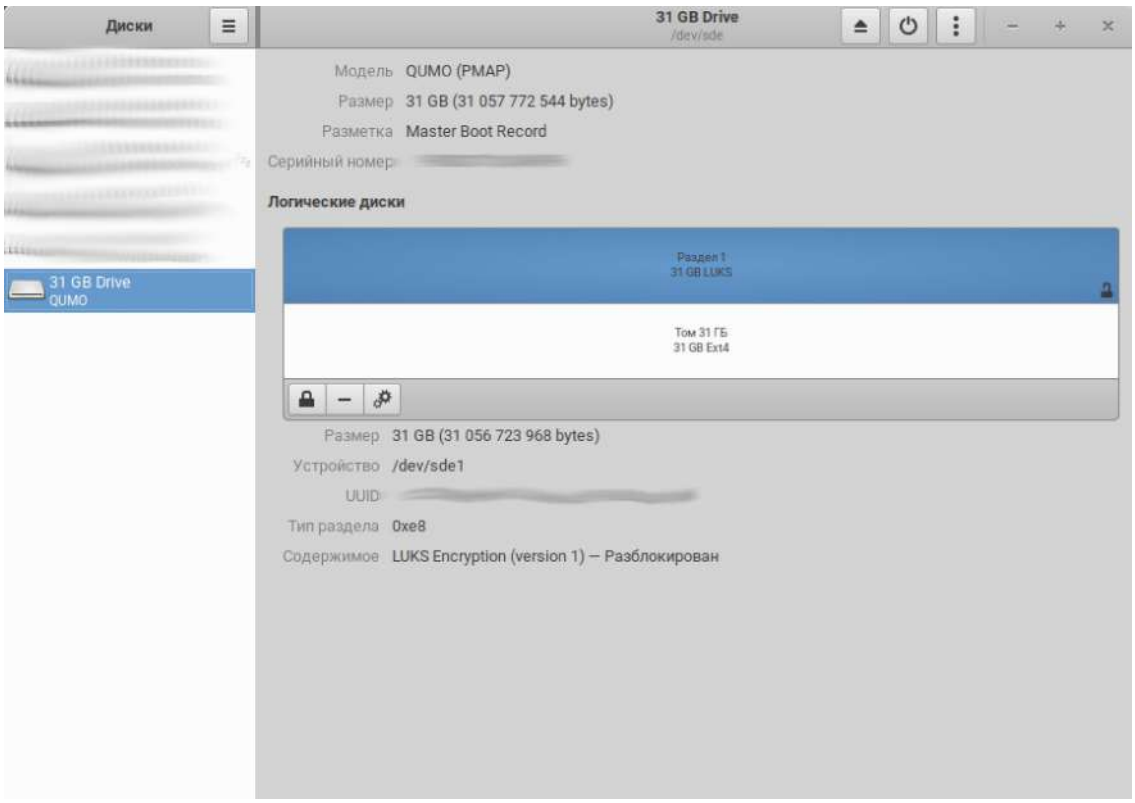
Нажимаем «Далее». Теперь необходимо указать имя тома. Придумывайте, какое хотите. Затем указываем «Файловая система EXT4» и устанавливаем галочку на «Зашифровать диск LUKS». К слову, если вам необходим диск, который будет открываться в системе Windows, то можете выбрать NTFS, но такой носитель нельзя зашифровать. Также если нужна высокая совместимость с различными устройствами, и при этом вы не собирайтесь помещать на накопитель файлы более 4 Гб, то можно также выбрать FAT32. Здесь же есть функция для перезаписи дискового пространства. О том, что это такое и для чего может понадобится, я объясню позже. Сейчас не рекомендую ее активировать, если ваш диск вы не подобрали где-то на барахолке накануне. Когда все указано, нажимаем «Далее».



Теперь необходимо дважды набрать пароль. Если используйте диск, как часть системы, для хранения пользовательских файлов, то можете использовать тот же пароль, что и для шифрования системы. После этого нажимаем «Создать».



Начинается процесс создания зашифрованного раздела. Скорость создания зависит от объема накопителя. После окончания шифрования, программу можно закрыть.

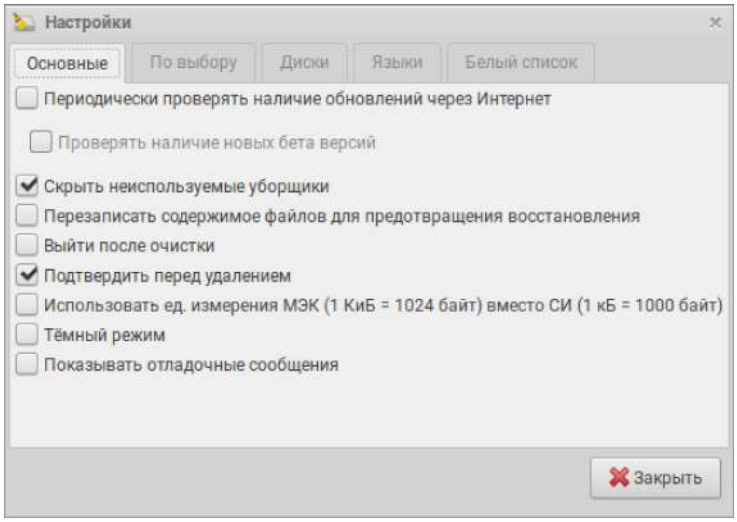


Теперь открываем файловый менеджер и в поле справа отсоединяем только что отформатированный диск, с помощью кнопки рядом (он был подсоединен по ходу работы с программой). После этого, нажимаем на него, выскакивает окно для ввода пароль, которым зашифрован диск. Потом выскочит еще одно окно, на этот раз пароль суперпользователя, чтобы разрешить присоединение диска. После его ввода зашифрованный диск будет открыт. Теперь можно переносить файлы на него и с него.

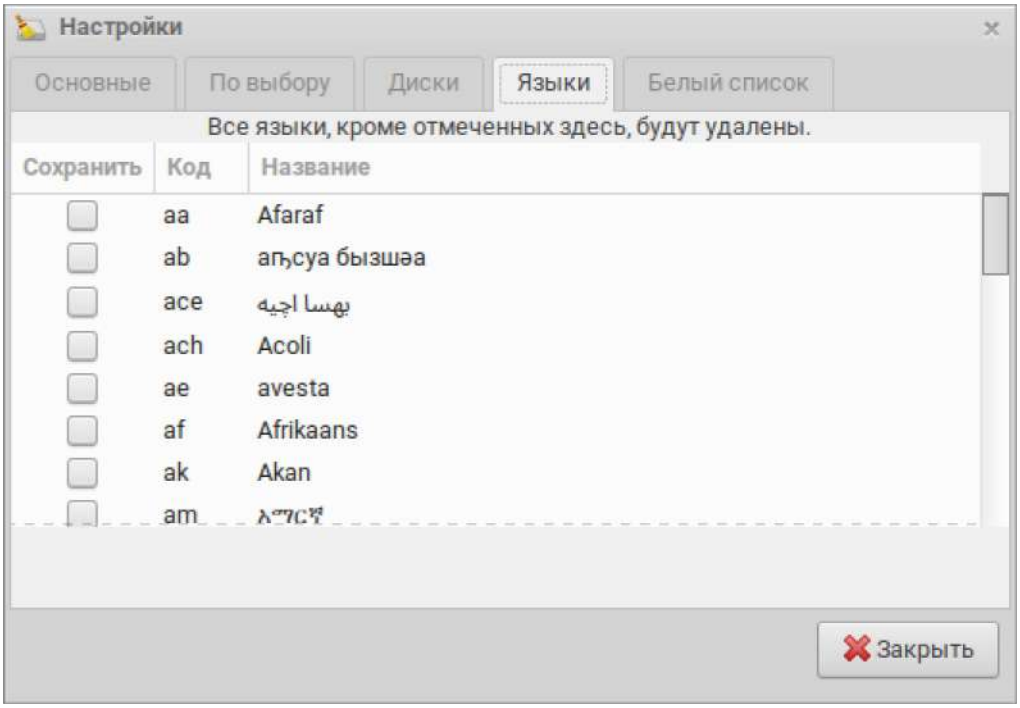
13 Работа с Bleachbit

Идем в Меню, затем в «Прочее» и нажимаем Bleachbit. Вместе с программой выскочит окно первичной настройки. Здесь можно поставить галочку на «Перезаписывать удаленные данные». Поясню, что это значит. Когда вы удаляйте файл, он не стирается с вашего диска. Просто место, которое он на нем занимает, помечается как свободное. Но данные фактически продолжают находится на носителе до тех пор, пока на их место не будет записано что-то другое. Таким образом, если вы удалили какую-то информацию, при получении к вашему компьютеру доступа кого-то постороннего (например при краже, или если кто-то из домочадцев втихаря решил полазить по вашим файлам), она теоретически может быть получена им. Для предотвращения этого, файлы можно не удалять, а затирать. То есть не просто помечать занимаемое ими место как свободное, а перезабивать его нулями, делая действительно пустым. Именно это и позволяет осуществлять функция перезаписи. Часто можно встретить заявление, что единичная перезапись может оставить часть информации и для надежности нужно производить многократное затирание. Действительно, остаточная намагниченность может сохраняться на диске и оставлять доступным какое-то количество старой информации. Однако, в подавляющем большинстве случаев, однократная перезапись все же удаляет все данные и ее вполне достаточно (ни одна организация по восстановлению данных, не возьмется за восстановление информации с диска, если на нем было произведено однократное затирание). Кроме того, если и останется какое-то количество данных, то полноценному восстановлению они вряд ли будут подлежать. Что касается популярного мифа, что перезаписей должно быть тридцать пять, то он родился из-за неправильного понимания метода Гутмана, где было сказано, что цикл из тридцати пяти перезаписей убирает данные со всех типов дисков, тогда как для каждого конкретного типа нужно лишь

несколько циклов перезаписи.[19] Ввиду того, что многократная перезапись имеет довольно сомнительное преимущество перед однократной, а также ввиду значительного увеличения временных затрат в случае многократного затирания, Bleachbit производит однократную перезапись. Также следует отметить, что подобный способ затирания данных был разработан для жестких дисков (HDD), в твердотельных накопителях (SSD) и флешках другие принципы записи информации, поэтому на них данный способ не всегда работает корректно. Также информацию сложнее удалить таким способом с дисков, на которых используются журналируемые файловые системы, такие как EXT4, которая и применяется в GNU/Linux. Имейте это ввиду. На самом деле при несанкционированном доступе к компьютеру, шифрование диска защищает и удаленные, но не затертые данные точно также как обычные, поэтому данная функция для простого пользователя может не быть необходимостью. Тем более, что затирание занимает значительно больше времени, чем простое удаление. В общем, использовать его или нет, решайте сами.



Во вкладке «Локализации», проверяем, чтобы галочки стояли на нужных вам языках.



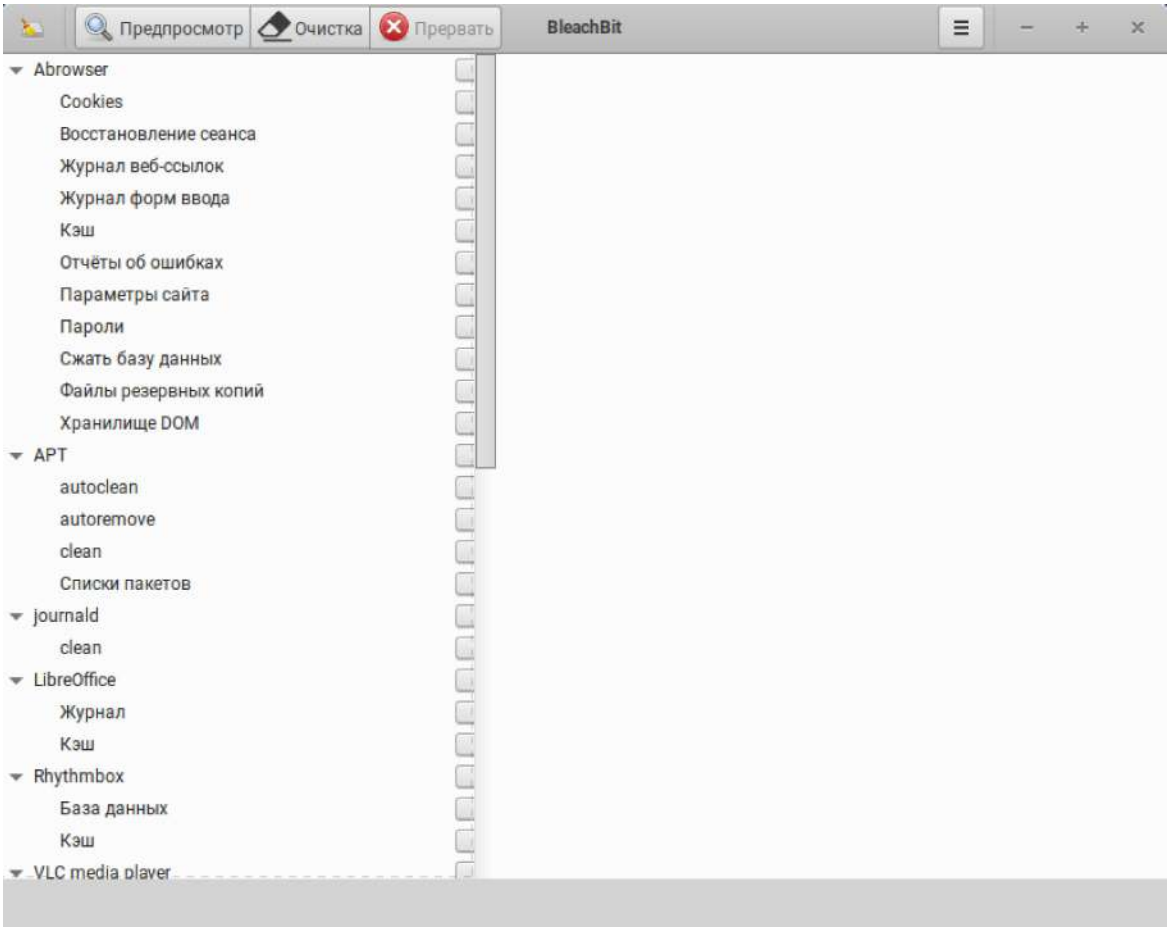
В остальных вкладках все оставляем как есть. Нажимаем «Закрыть».

В окне программы слева идет список того, что в системе следует подвергать очистке. С помощью этой программы можно удалять как отдельные файлы, так и каталоги. Для этого идем в «Файл» и там выбираем «Удалить файл» или «Удалить каталог». При этом, если вы выбрали перезапись данных, файлы и каталоги будут не просто удаляться, а затираться. То же касается и данных представленных в списке. В этом списке отмечаем галочками все, кроме «Глубокое сканирование», а также в «Система» оставляем не отмеченными «Память» и «Свободное место».

«Память» это оперативная память. Даже после выключения компьютера в ней до новой загрузки могут сохраниться последние побывавшие в ней данные, и их в лабораторных условиях можно восстановить. Поэтому вообще очищение ее может быть актуальным, но пожалуй лишь перед выключением компьютера. К тому же данная функция экспериментальна и может проходить не совсем корректно.

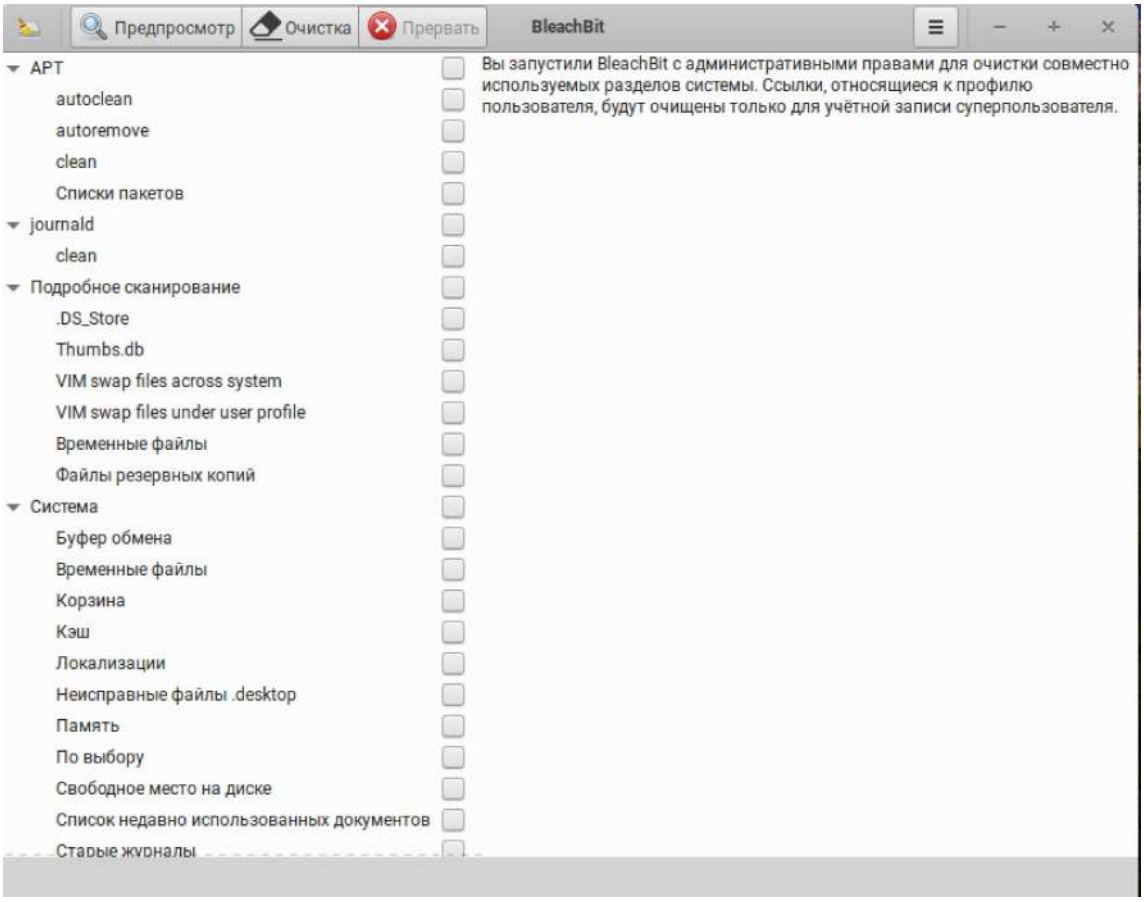
«Свободное место» может потребоваться затереть если вы собираетесь диск отдать кому-то или продать. Или если до этого какая-то серьезная информация была не затерта, а удалена обычным способом. Регулярно же ее выполнять нет абсолютно никакой необходимости, а многим она вообще может быть не нужна.

Также, если не хотите удалять другие локализации, кроме тех которыми пользуетесь, можете не ставить отметку на «Локализации» (они удаляются только чтобы освободить место). А также «По выбору», если ничего не выбирали в соответствующем пункте.



Для удаления всего отмеченного нажимаем на кнопку «Удалить» (красный круг с перечеркиванием). Имейте ввиду, что пока мы работаем не от суперпользователя, не все отмеченные данные удалятся. Для того чтобы удалить все, необходимо сначала провести очистку из-под обычного пользователя, а затем от суперпользователя.

Работа с Bleachbit от суперпользователя находится там же в Меню. Запускаем ее и настраиваем точно также. Перезапись данных, отметка нужных языков, отметка всех пунктов, кроме «Глубокое сканирование» и в «Система», «Память», «Свободное место», а также, возможно «Локализации» и «По выбору».

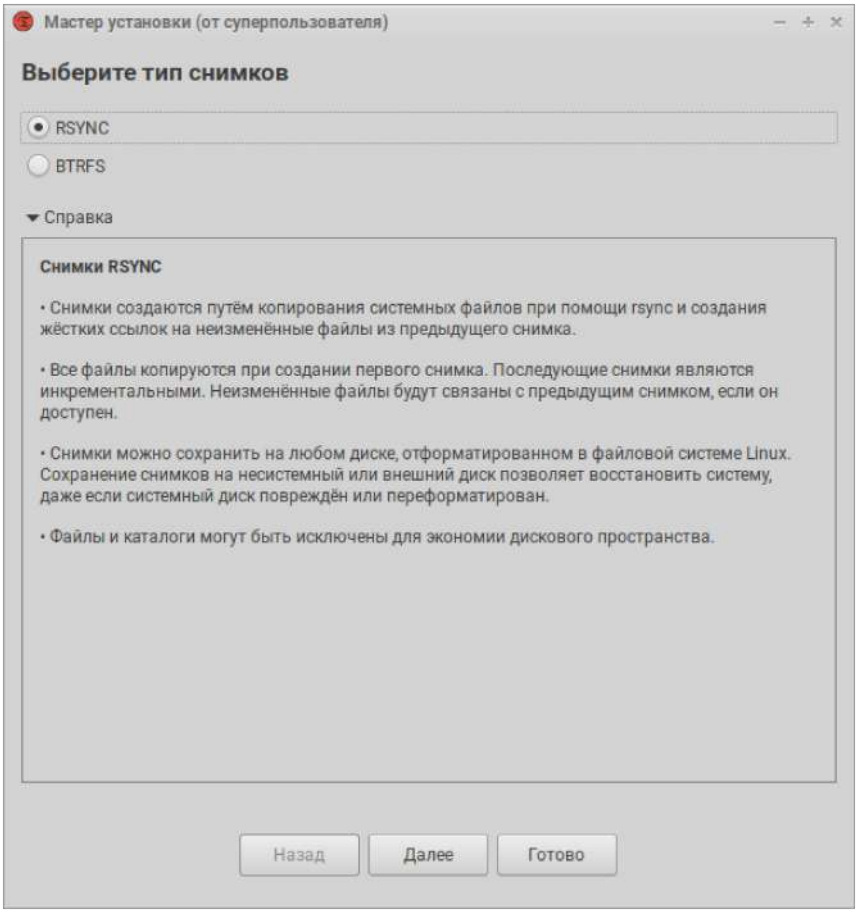


После того, как почистили систему, можно создать точку восстановления.

14 Работа с TimeShift

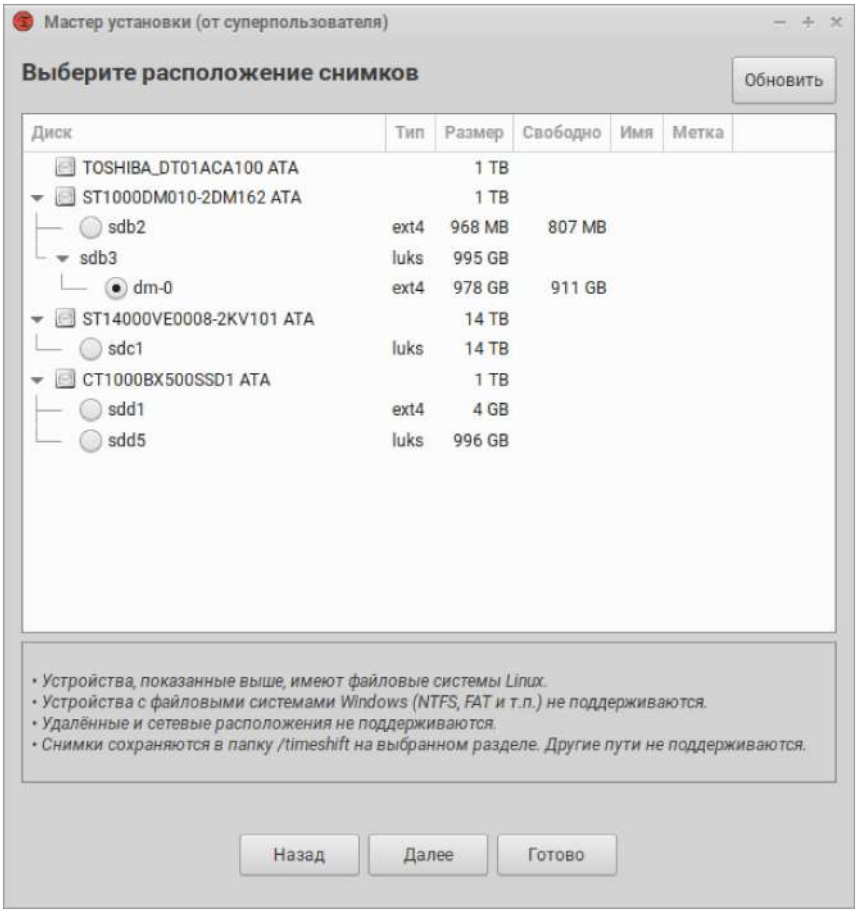
Идем в Меню, категория «Прочее», выбираем TimeShift. Так как данная программа работает на уровне конфигурации системы, для ее запуска необходимо ввести пароль. С помощью данной программы можно создавать точки восстановления системы, и в случае возникновения сбоя, сохраняющегося при перезагрузке компьютера, систему можно будет откатить в состояние, предшествовавшее этому сбою.

После запуска выскочит окно, в котором нужно будет выбрать тип снимков. Поскольку мы используем файловые системы ext4, то оставляем «BSYNC». Если нажать на «Help», то откроется информация о том, как именно создаются снимки данной программой.



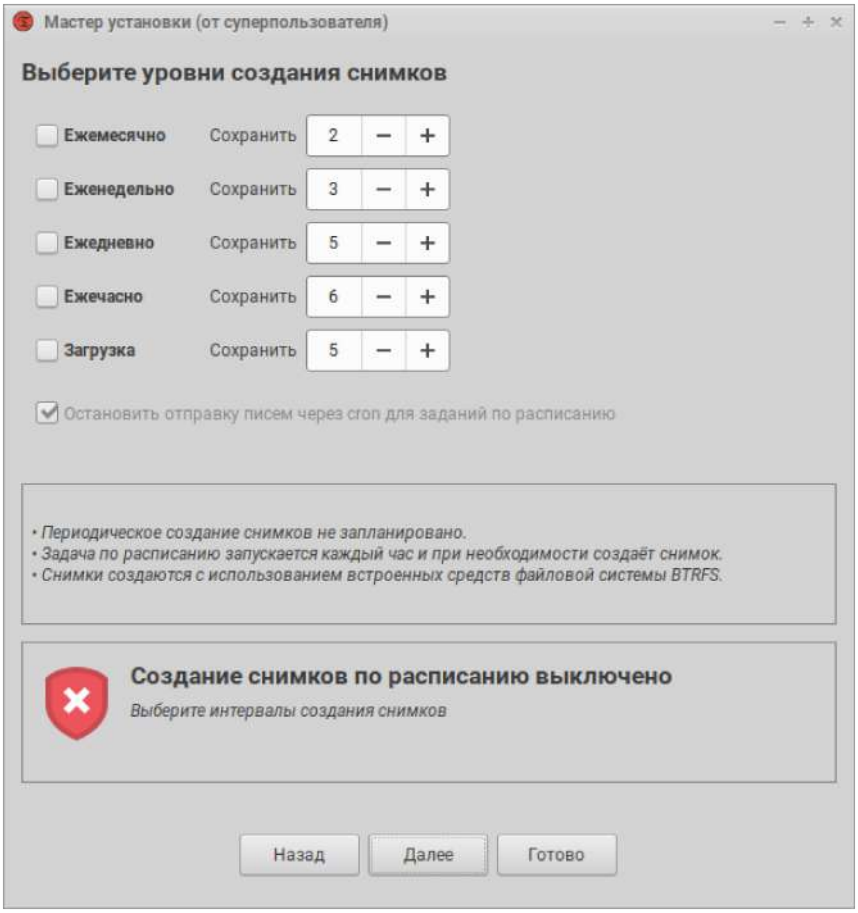
Нажимаем «Далее».

Ждем пока произведется оценка размера операционной системы, после чего необходимо будет указать место для хранения снимков. Им может выступать как диск на котором непосредственно установлена операционная система, или же отдельный диск. Если вы используйте SSD совместно с HDD, то укажите HDD, поскольку снимок системы занимает столько же места, сколько и сама операционная система. Можно завести для этого вообще отдельный диск, главное, чтобы он был отформатирован в файловую систему ext4 или другую, используемую в системах GNU/Linux.

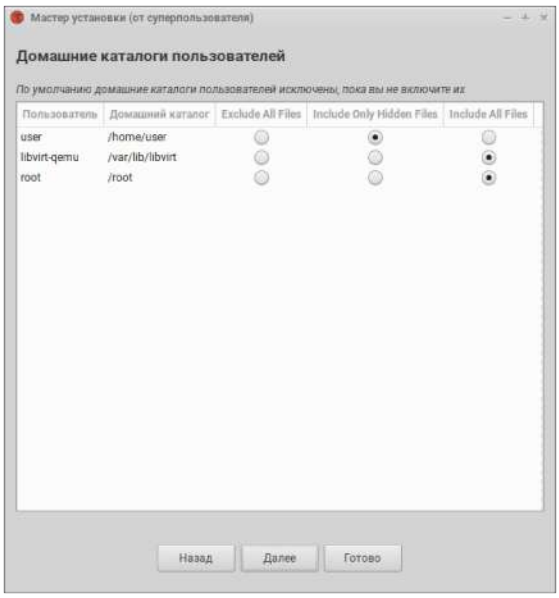


Когда устройство для хранения выбрано, нажимаем «Далее».

Теперь предлагается настроить создание снимков по расписанию. Я рекомендую отключить данную функцию. Мы будем создавать снимки вручную по схеме, которую я освещу далее. Снимаем все галочки и нажимаем «Далее».



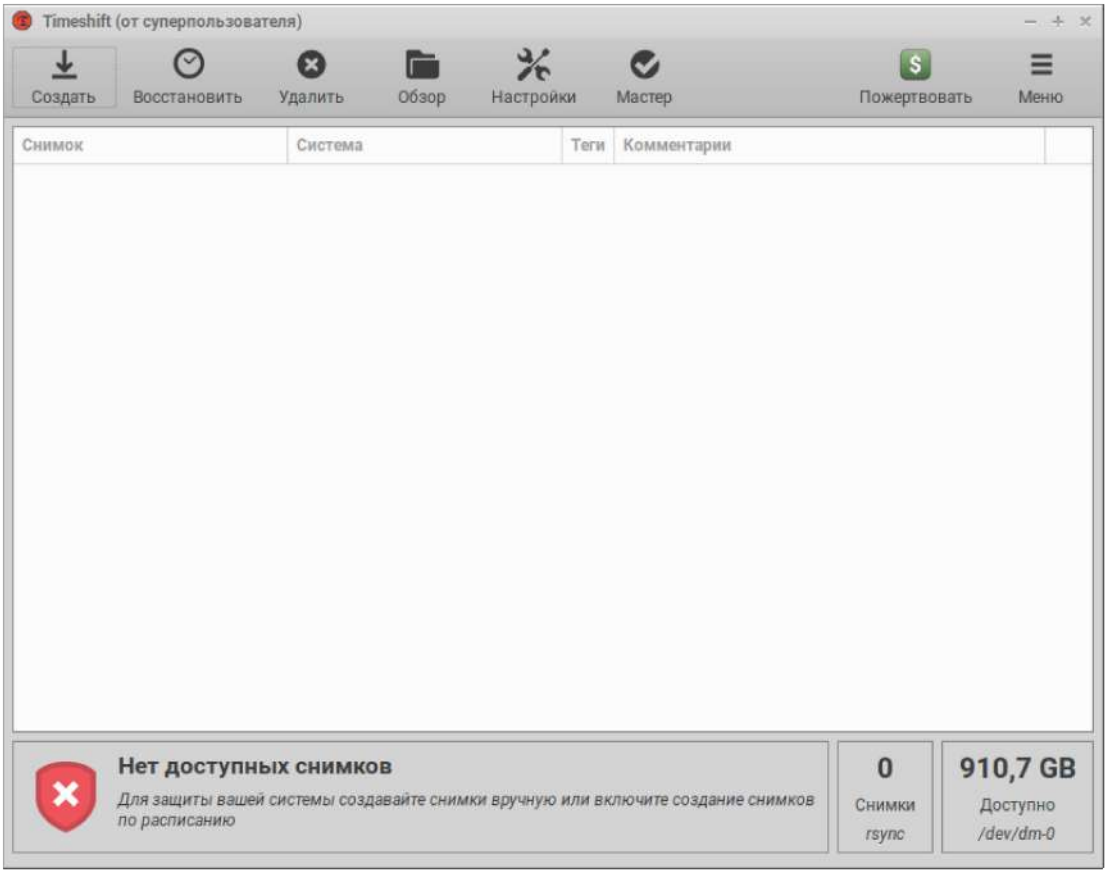
Теперь необходимо указать, стоит ли при создании снимков затрагивать какие-либо пользовательские файлы. Для пользователя root рекомендую указать «Include All Files». Пользователь libvirt-qemu отвечает за файлы виртуальных машин, в том числе за виртуальные жесткие диски (в которых и хранятся системы виртуалок). Вообще для надежности лучше и здесь указать «Include All Files», однако нужно иметь ввиду, что виртуальные жесткие диски могут занимать и 25 и 50 Гб. Соответственно, очень сильно возрастет размер снимка и время, которое будет затрачиваться на его создание. Если у вас нет возможности предоставить большое количество места для снимков или вы не готовы ждать по сорок и более минут, пока снимок будет создан, то указывайте «Exclude All Files». Что касается обычных пользователей, то ваши личные файлы я не рекомендую включать в снимки системы. Однако, как я уже говорил, в каталог /home включаются некоторые системные файлы, и лучше обеспечить их восстановление. Они являются скрытыми, поэтому указываем «Include Only Hidden Files».



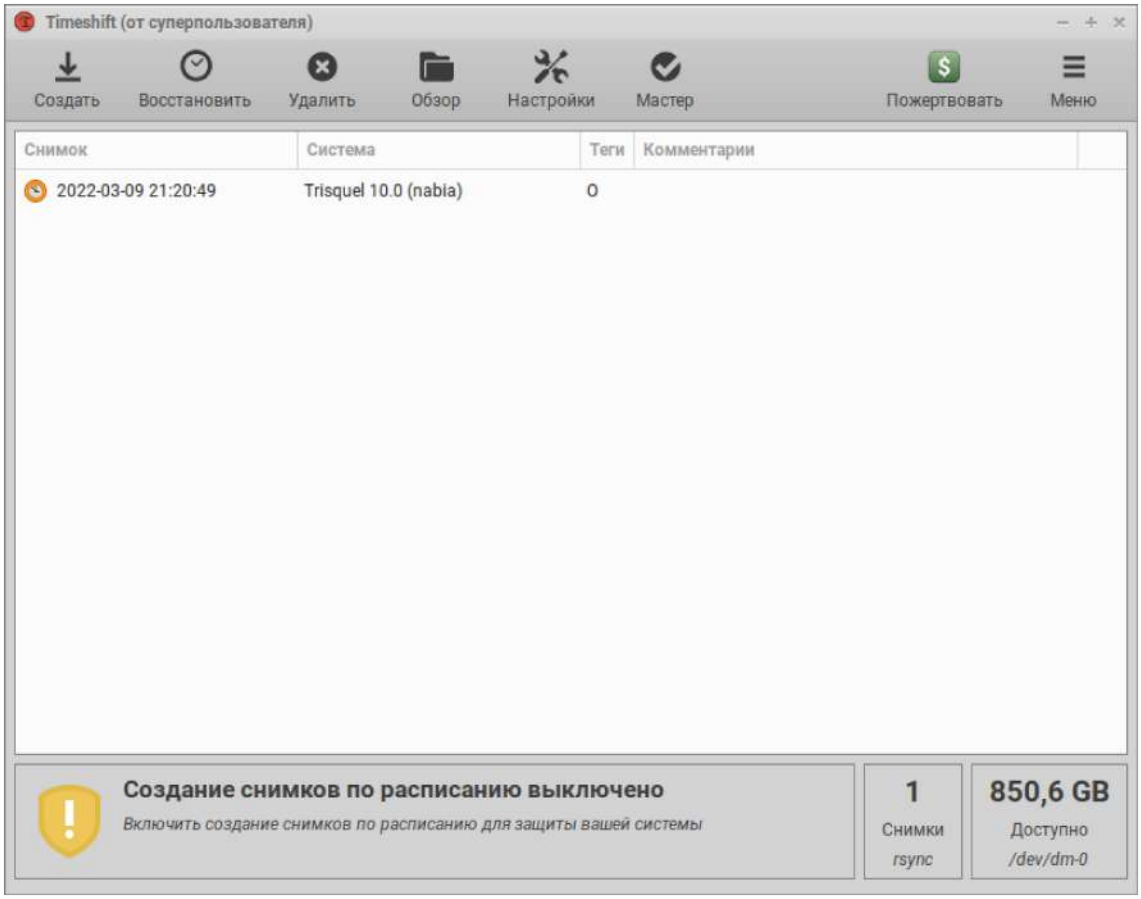
Нажимаем «Далее».

Выскочит сообщение о том, что установка завершена. Нажимаем «Готово».

Откроется основное окно программы. Чтобы создать снимок, нажимаем на кнопку «Создать» вверху слева.



Начнется процесс создания снимка. После окончания процесса, он появится в списке в основном окне. Для восстановления системы, необходимо выделить нужный снимок и нажать на кнопку «Восстановить» вверху.



Я рекомендую создавать точки восстановления после каждого обновления системы. Делать это лучше по такой схеме. Обновились, перезагрузились, почистили систему, сделали точку восстановления. Поскольку может так случиться, что после обновления, что-то начнет работать не корректно, я рекомендую сохранять не менее двух последних точек восстановления. То есть, после того, как вы создали точку восстановления, не удаляйте предыдущую точку. А вот когда в вашем списке появляется более двух точек, наиболее старые можете удалять. Таким образом, у вас будет надежная страховка на случай сбоев.

15 Настройка принтеров и сканеров

В Trisquel для работы с принтерами используется CUPS. В нем изначально присутствуют драйвера для многих устройств. Поэтому часто после подключения принтера/МФУ к компьютеру и его включения, устройство определяется и драйвер к нему подбирается автоматически. Когда это происходит выскакивает уведомление о том, что принтер успешно настроен.

Если такого не произошло, то нужного драйвера в системе нет, но он может быть в репозиториях, поэтому первым делом откроете Synaptic и попробуйте поискать его по сочетанию слова driver и названия производителя принтера/МФУ. Если найдутся драйвера для нужного производителя, установите их, перезагрузите систему и попробуйте подключить принтер. Если это не принесло результатов, то драйвер необходимо скачать отдельно. Как правило, драйвера, в том числе для операционных систем GNU/Linux, можно взять прямо на официальном сайте производителя принтера/МФУ. Если предлагается скачать не просто драйвер для абстрактного «Linux», а указаны названия дистрибутивов, предпочтительно выбирать «Ubuntu» (на ней основан Trisquel), а в случае его отсутствия «Debian» (на нем основана Ubuntu). Если на выбор предлагаются типы файлов, к примеру с расширениями .rpm или .deb, выбирайте .deb, это стандартное расширение пакетов системы Debian и, соответственно, основанных на нем. В этом случае установка будет осуществляться через программу GDebi, которая изначально установлена в Trisquel. Если после установки принтер все равно отказывается печатать, попробуйте поиграться с установкой, производя ее при включенном или отключенном принтере. После каждой неудачной попытки, удаляйте драйвер через все ту же программу GDebi и чистите систему с помощью Bleachbit. Также можете поиграться с добавлением или удалением принтеров в программе «Принтеры». Ее можно открыть если пройти в Меню, затем «Система», потом «Администрирование». Иногда драйвера могут предлагать скачать в виде архива с расширениями .tar.bz2 или .zip. Внутри такого архива, скорее всего будет лежать папка с кучей других папок и файлов. Необходимо эту папку распаковать из архива, как вариант, в домашнюю папку с пользовательскими файлами. После этого, поищите в этой папке файл с названием install.sh и дважды щелкните на него. В выскочившем окне нажмите на кнопку «Запустить». После этого система, как правило, определяет драйвер. Возможно также, что его не удасться так запустить и это придется делать через терминал с

правами суперпользователя с помощью следующей команды

./install.sh

Предварительно необходимо в терминале пройти в папку, где лежит данный файл.

В некоторых случаях может предлагаться скачать помещенный в архив скрипт. Он может иметь расширение .gz. В этом случае необходимо его скачать, затем создать в пользовательском каталоге папку для файлов принтера, переместить туда скачанный файл, подключить принтер к компьютеру и включить его. После этого в терминале перейти в режим суперпользователя, для чего нужно набрать уже знакомую строку

sudo bash

И ввести пароль. Затем перейти в папку с файлом скрипта, набрав строку

cd /home/имя пользователя/название папки с файлом

Затем скрипт нужно разархивировать, для чего набираем

gunzip название файла скрипта

После чего скрипт остается запуститься, просто набрав в терминале название скрипта и нажав «Enter». По ходу установки необходимо будет прописать название модели принтера (оно написано на самом устройстве, на коробке от него, в документации, его же можно посмотреть в программе «Принтеры» в Меню). Также будут задаваться вопросы, на которые нужно указывать «y». Кроме вопроса о подключении принтера по URL (т.е. по сети). Если принтер подключен по сети, то также «y», если нет, то «n». И далее необходимо указать путь до него. Чтобы его узнать, идем в Меню, категория «Система», затем «Администрирование» и там выбираем «Принтеры». Здесь нажимаем «Разблокировать» вверху справа. Набираем пароль. Затем нажимаем «Добавить» и ждем пока в открывшемся окне в списках путей в поле слева не появится строчка со словами «usb» и моделью вашего принтера. Эту строку указываем в терминале. В конце будет предложено протестировать принтер,

после согласия на что, будет напечатана тестовая страница. На этом установка драйвера для принтера закончена.

Со сканерами ситуация аналогичная. Часто драйвера для сканера/МФУ уже есть в системе, и после подключения устройства, они автоматически будут подобраны. Проверить, работает ли сканер можно попробовав что-нибудь просканировать с помощью программы «Простое сканирование». Если сканирует, значит все в порядке, если нет, значит надо устанавливать драйвера отдельно. В этом случае их также ищите на официальном сайте производителя.

Кстати, если принтер требует особой настройки, производится она в той же программе «Принтеры». Для этого, открыв ее, щелкните правой кнопкой мыши по значку принтера и в появившемся поле нажмите «Свойства». Выскочившее окно и будет содержать все необходимые настройки, к примеру, указание, какой тип бумаги используется, обычная или фотобумага.

После того, как в вашу основную систему установлено все необходимое, пришло время, если вы еще этого не сделали, отключить ее от Интернета, убрать автоподключение к сети. Для этого щелкните по значку сети на панели и нажмите «Изменить соединение». В появившемся окне выделите то соединение, через которое осуществляется доступ к Интернету, и щелкните справа на кнопку «Изменить». В выскочившем окне откройте первую вкладку и снимите галочку с «Автоматически подключаться к этой сети». После этого нажмите «Ok». Теперь при запуске системы, при подключенном Интернет-кабеле/модеме/адаптере, при активном Интернет-соединении, ваша система подключаться к этому соединению не будет. При необходимости, например для обновления или установки нового ПО, подключить ее к Интернету можно будет вручную, просто нажав на значок сети на панели и затем нажав на нужное соединение. Остальную же Интернет-активность, как я уже говорил, осуществлять следует из-под виртуальных машин, о настройке которых я и расскажу в дальнейшем.

16 Обновление Trisquel до новой версии

Существует способ обновить уже установленную версию Trisquel до более новой, когда она выпускается. Это значительно проще, чем производить полный процесс установки системы. Однако, такое обновление не всегда осуществляется корректно, и стоит быть готовым к тому, что придется все-таки осуществлять полный процесс установки. Тем не менее, я покажу, как можно

обновлять Trisquel до новой версии, когда она выходит. Для того, чтобы проверить наличие новой версии в терминале от суперпользователя нужно ввести команду.

```
do-release-upgrade -c
```

Отобразится информация о наличии или отсутствии новой версии.
Для обновления системы нужно ввести команду.

```
do-release-upgrade -d
```

Начнется процесс установки, по завершении которого, нужно будет перезагрузить компьютер и можно начинать работать в новой версии операционной системы.

4 Виртуальная машина для публичной Интернет-активности

17 Определение публичной Интернет-активности

Подключение к Интернету без использования средств анонимизации, я называю публичным. В этом случае вы напрямую работайте с Интернет-ресурсами, без использования туннелирования. Интернет-ресурс при этом видит ваш ip-адрес и другие атрибуты. Провайдер и различные следящие системы видят к каким Интернет-ресурсам вы обращайтесь и, в случае не шифрованного соединения, могут видеть содержимое трафика, передаваемого между вами и Интернет-ресурсами.

В каких случаях следует осуществлять Интернет-активность подобным образом? Во-первых, при работе с Интернет-магазинами. Поскольку, как я уже говорил, при работе с ними, вы или закажите курьера до своего дома, или придете в пункт самовывоза, или закажите в ближайшее почтовое отделения, куда также сами придете. Вы так или иначе предоставите Интернет-магазину реальные данные о себе. Засветите свое лицо, настоящие ФИО, или хотя бы просто номер телефона (в большинстве стран привязанный к паспортным данным) с адресом электронной почты (в подавляющем большинстве привязанной к телефону, который привязан к паспортным данным). Конечно,

если вы радикально подходите к приватности, вы можете вовсе отказаться от использования Интернет-магазинов. Но, к примеру, если вам нужно приобрести крупную бытовую технику, а свой автомобиль отсутствует, скорее всего, вам придется заказывать ее доставку. Если вы человек пожилой и вам сложно таскаться по магазинам, то заказ товаров домой с помощью Интернет-магазинов вас очень сильно выручит.

Во-вторых, при использовании публичной электронной почты. Публичной электронной почтой я называю ту, которую вы предоставляете в различные организации для связи с вами, которая известна широкому кругу людей именно в привязке к вам. Переписка по такой почте доступна, как минимум, сотрудникам сервиса почты и тем, с кем они сотрудничают. Почти все почтовые сервисы привязывают аккаунты своих пользователей к номеру мобильного телефона, который привязан к паспортным данным. Конечно, ни о какой приватности здесь говорить не приходится. Тем не менее, как в современном мире едва ли возможна жизнь без мобильного телефона, так и крайне затруднительна она без электронной почты.

В-третьих, при использовании неэтичных социальных сетей. Неэтичными соц. сетями являются те, которые собирают данные о своих пользователях. Их сервера централизованны и базируются на несвободном ПО. Это широко известные ВКонтакте, Facebook, Одноклассники, Instagram и т.д. Безусловно, лучше не пользоваться ими вообще. Тем более, что на сегодняшний день в отличие от электронной почты и тем более мобильного телефона, необходимости использовать их и иметь в них аккаунты нет. Тем не менее, кому-то это может быть необходимо в связи с его деятельностью. К примеру, если вы блогер, использование таких социальных сетей может быть для вас крайне важно. Однако, я все же рекомендую отказываться от них. Как вариант, вы можете поместить на своей странице в такой соц. сети объявление, что решили прекратить свою деятельность в ней и, допустим, через полгода, удалите этот аккаунт. Вместе с тем, укажите, что переходите в этичную социальную сеть (о таких сетях я расскажу в дальнейшем) и дайте ссылку на свой аккаунт в таковой (предварительно, естественно его заведя). Это даст время вашим подписчикам, переключиться на ваш новый аккаунт, и, заодно, приобщит их к этичным сервисам.

В-четвертых, не обязательно, но может быть рационально, при использовании этичных соц. сетей, если вы в них светите какие-то свои

персональные данные. Элементарно — размещаете личные фотографии, на которых ваше лицо. Опять же, если вы блогер, публичная личность.

В-пятых, при работе с государственными, муниципальными, общественными, социальными сервисами. Например при оплате ЖКХ, электроэнергии, передаче показаний счетчиков воды, электричества, оплате штрафов, записи на прием ко врачу, в общем, опять же, там, где вы так или иначе засветите свои реальные данные.

В-шестых, когда вы ищите в Интернете какую-то информацию, которая связана с вами, при том, что различным организациям, в частности гос. организациям, известно, что она связана с вами. Классический пример такой ситуации — поиск информации в ходе написания диплома. У вас есть четко определенная тема диплома. Ваш институт знает ее, знает какую информацию вам нужно по ней искать, и эти данные могут быть доступны организациям, с которыми работает институт. Такую активность в отличие от Интернет-магазинов, публичной почты, гос. сервисов и неэтичных соц. сетей, осуществлять публично нет необходимости. Это просто можно считать приемлемым.

В каких случаях осуществлять Интернет-активность подобным образом не стоит? Во-первых, при общении. Ваша личная жизнь, это ваша личная жизнь и незачем провайдерам, гос. службам, корпорациям и всяким взломщикам ее знать. Конечно, если речь идет о ваших близких или деловых партнерах, т.е. тех, чья связь с вами и так известна, общение без анонимизации можно считать вполне приемлемым. Главное при этом использовать безопасные каналы с надежным шифрованием, о которых будет сказано далее.

Во-вторых, при поиске, чтении, просмотре, скачивании какой-то информации. Сюда относится чтение статей, книг, блогов, новостей, в том числе на государственных сайтах, при условии, что вы не планируйте авторизацию в своем аккаунте, привязанном к вашим настоящим ФИО, номеру телефона и т.д. и иным образом светить свои персональные данные. Также посещение форумов, просмотр изображений, видео, прослушивание музыки и скачивание чего-либо. Ваши личные интересы, проблемы и т.д., это, опять же, ваша личная жизнь и незачем в нее посвящать посторонних.

Вот, в принципе все то, что следует и не следует делать при публичной Интернет-активности. Настало время определиться, какую операционную систему мы будем использовать для этой виртуальной машины.

18 Операционная система для виртуальной машины

Существует рекомендация, чтобы операционная система виртуальной машины отличалась от основной. Это нужно для того, чтобы злоумышленник, взламывающий виртуальную машину, не смог предугадать уязвимости основной операционной системы, на случай если ему выпадет шанс взломать и ее.

Если смотреть с этой позиции, то лучше, чтобы основная и гостевая (т.е. виртуальная машина) операционные системы принадлежали к разным веткам, а еще лучше к разным семействам операционных систем. Однако, за пределами семейства GNU/Linux, достойной операционной системой можно счесть разве что OpenBSD.[20] В ней отсутствуют несвободные компоненты, однако для простого домашнего использования она не подходит, ввиду свой сложности и ограниченного софта. В рамках семейства GNU/Linux есть полностью свободные операционные системы не относящиеся к ветке Debian (к которой, напоминаю, относится Trisquel). Но операционные системы других веток, по сравнению с веткой Debian, выглядят все же менее приглядно.

Чтобы хоть в какой-то мере выполнить выше оговоренное правило, а также в целях расширения кругозора, я решил использовать систему все же отличную от Trisquel. К сожалению, у других полностью свободных операционных систем, относящихся к ветки Debian, проблемы с удобством и функциональностью. Ввиду этого, я рекомендую в качестве гостевой операционной системы использовать систему Devuan.

Как уже говорилось, изъян Devuan по сравнению с полностью свободными дистрибутивами в том, что он лояльно относится к установке несвободного ПО. Однако, изначально несвободных компонентов в этой системе, в том числе в ядре, нет. Также по сравнению с самим Debian, который также свободен от проприетарных элементов, в ней отсутствует неприятный компонент systemd. К тому же она менее забагована. В ней, однако, в отличии от Debian, по-умолчанию включены разделы репозиториев с несвободным ПО. Однако их легко отключить. Ввиду этого, Devuan полностью пригодна для использования.

Скачать последнюю версию системы Devuan можно, пройдя по ссылке.[1] На момент написания пособия, это Devuan 4. После скачивания iso-образа можно запускать программу виртуализации.

19 Программы виртуализации

Прежде чем приступать к изложению методики создания виртуальной машины, расскажу о самих программах виртуализации. О неприемлемости использования проприетарных инструментов, таких как VMware, полагаю, можно не упоминать. Гораздо интереснее обстоит дело с очень популярной и широко распространенной программой VirtualBox. Сама по себе VirtualBox свободна. Но у нее есть проблема, о которой люди, рекомендующие ее, предпочитают не упоминать. Дело в том, что для полноценной работы с данной программой в нее необходимо установить специальный плагин. Без него вы не сможете даже развернуть гостевую ОС на весь экран. Но вот этот вот плагин, без которого полноценно работать с данной программой невозможно, распространяется под проприетарной лицензией.[2] То есть его установка превращает свободную VirtualBox в несвободную. А без него с ней работать, как было сказано, не получится.

Существуют полностью свободные инструменты для виртуализации. KVM,[3] Xen[4] и т.д. В репозиториях Trisquel присутствуют инструменты Qemu/KVM.[5] Они позволяют осуществлять полноценную виртуализацию, программно эмулировать оборудование. Их мы и будем использовать.

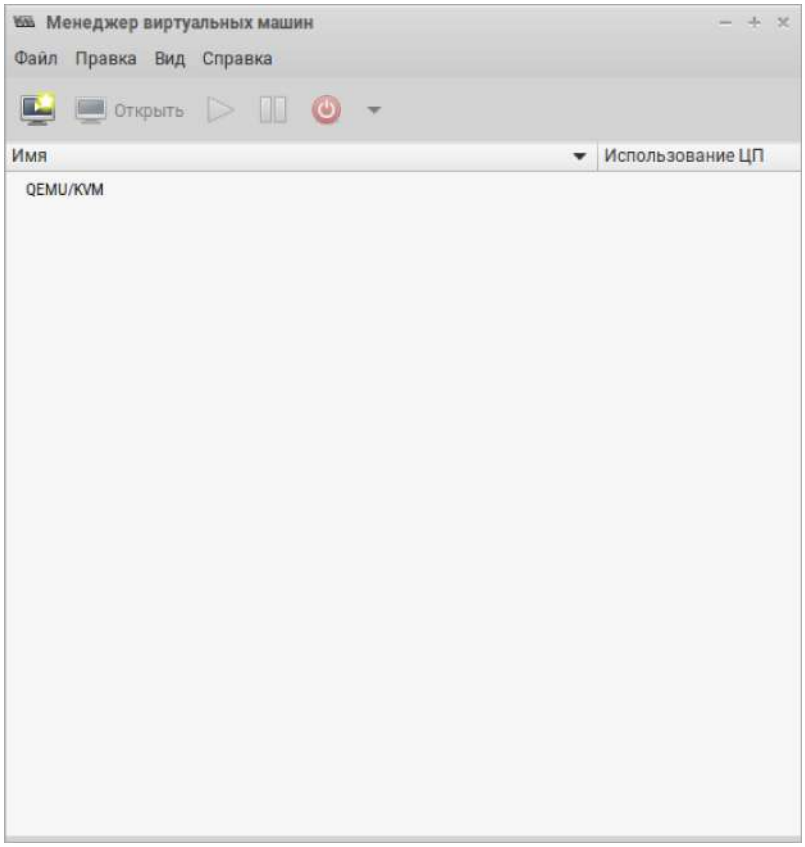
Однако для управления виртуальными машинами также нужен графический интерфейс. Одним из наиболее удобных и функциональных является Virtual Mashine Manager. Существуют и другие, Aqemu, Qtemu, но они недостаточно функциональны и мне показались не слишком удобными. В общем, ввиду вышесказанного, использовать мы будем именно Менеджер

виртуальных машин.

Настало время заняться созданием виртуалки.

20 Установка Devuan на виртуальную машину

Идем в Меню, категория «Прочее» и нажимаем «Менеджер виртуальных машин». Открывается окно, в котором сначала пройдет подключение к инструментам виртуализации. Когда подключение закончится отобразится надпись, о том, что подключено Qemu/KVM. Теперь, в принципе, программа виртуализации полностью готова для начала создания и настройки виртуальных машин.

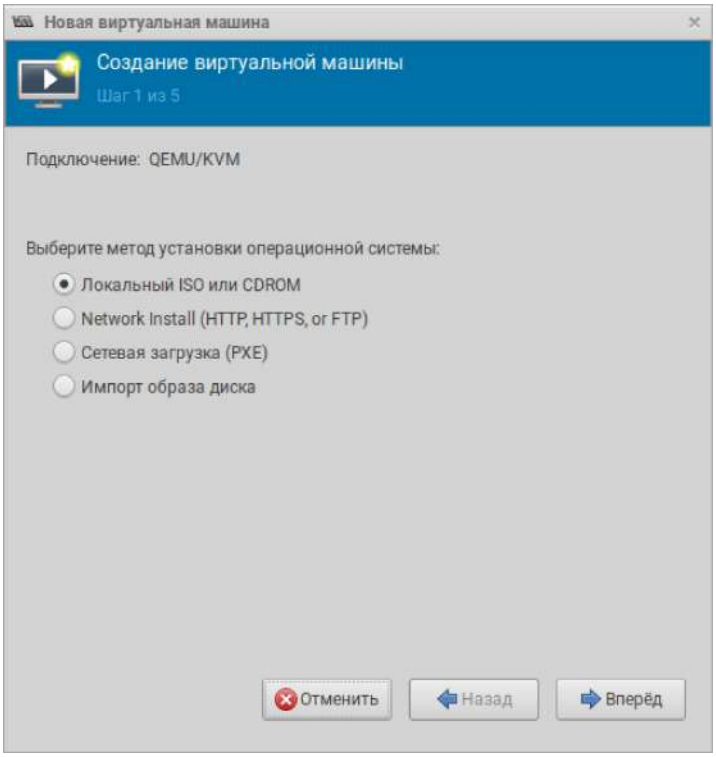


После установки Менеджер виртуальных машин создал сеть NAT. Она позволяет подключать виртуалки к Интернету, транслируя пакеты через хост (основную операционную систему). Поскольку мы держим основную операционную систему отключенной от Интернета, NAT мы использовать не будем и его желательно отключить. Однако есть ситуация, в которой это будет

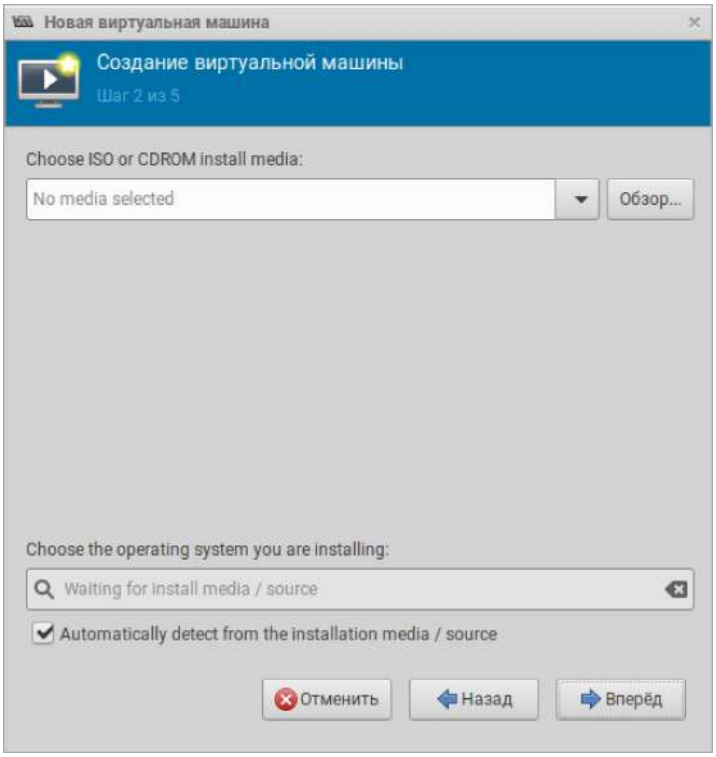
все-таки не целесообразно. Если вам приходится часто менять типы подключений, т.е. сегодня вы дома используйте проводной Интернет, завтра уехали на дачу с ноутбуком и там используйте USB-модем, затем в кафе подключайтесь к сети Wi-Fi с помощью адаптера, — то это может создать проблему. Для виртуальной машины, о которой сейчас идет речь, это не критично, поскольку можно просто указать в ней все эти типы сетевых карт. Однако, когда мы дойдем до виртуальной машины для туннелирования трафика, то там настройка файервола сильно зависит от прописанного сетевого адаптера. И в случае разных подключений, вам придется каждый раз перенастраивать там файервол, что весьма накладно. В этом случае можно использовать NAT. Но при этом обязательно, чтобы в основной операционной системе файервол жестко блокировал трафик. Межсетевой экран, настройка которого была приведена выше, затрагивает только входящий и исходящий трафик. Транзитный же остается не затронутым, ввиду чего виртуалки смогут спокойно получать Интернет по NAT. Единственное правило, которое следует оставить, это разрешение DNS. Других исключений не требуется. Если же вы не используйте регулярно разные сетевые карты, а например, всегда пользуйтесь только Wi-Fi, или у вас компьютер всегда находится дома, подключенный к Интернету через провод, то стоит использовать прямое подключение виртуалок к сети, и NAT нужно отключить.

Нажимаем «Правка» на верхней панели и затем «Свойства подключения». Иногда эта функция неактивна пока не будет создана и выделена в окне виртуалка, в этом случае данное действие придется производить уже после того, как виртуалка будет создана. В выскочившем окне, во вкладке «Виртуальные сети» на сети «default» снимаем галочку с «Автозапуск». После этого закрываем окно. Теперь можно приступать непосредственно к созданию виртуалки.

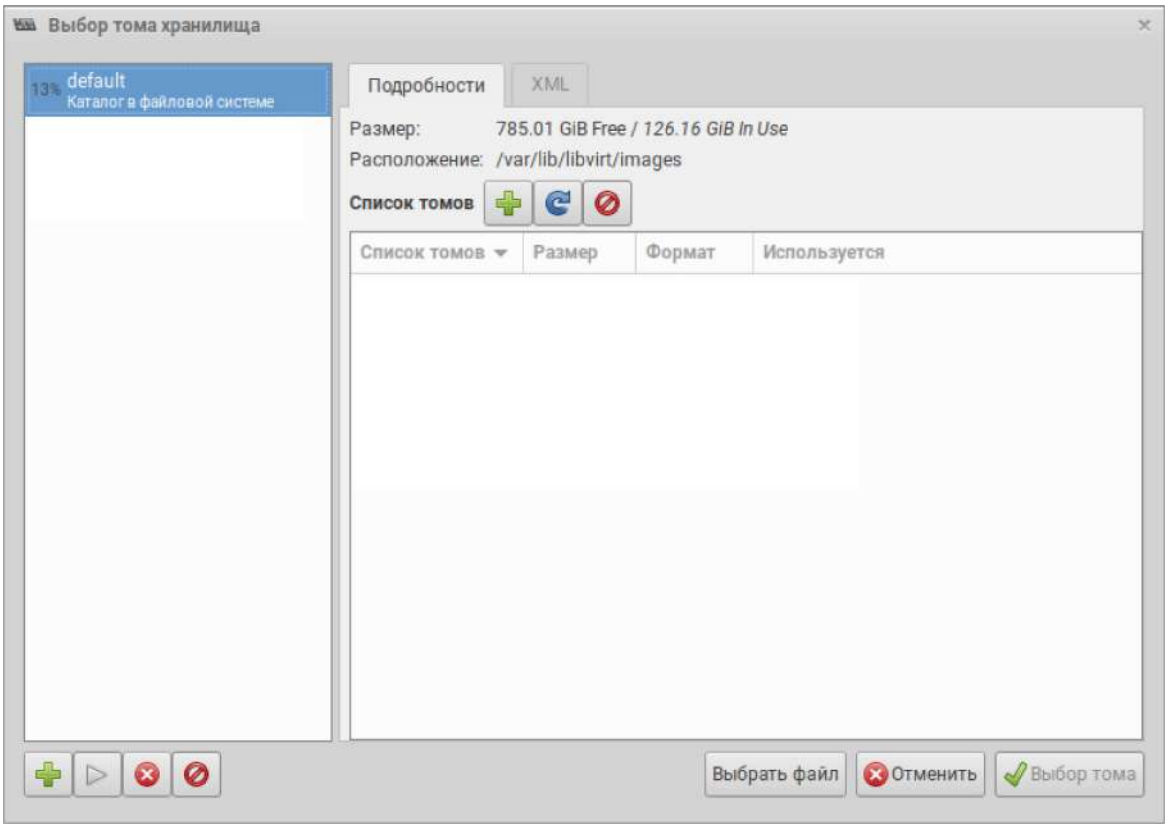
Нажимаем кнопку «Создать». В выскочившем окне должно стоять «Локальный ISO или CDROM». Нажимаем кнопку «Вперед».



Теперь нажимаем кнопку «Обзор».

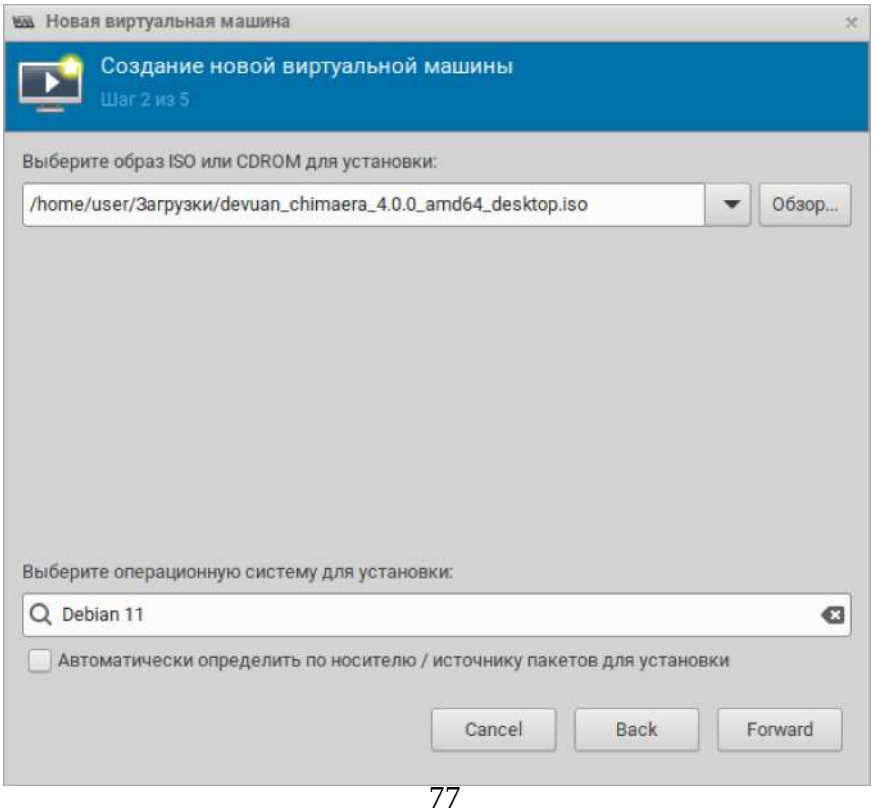


В появившемся окне нажимаем кнопку внизу «Выбрать файл».

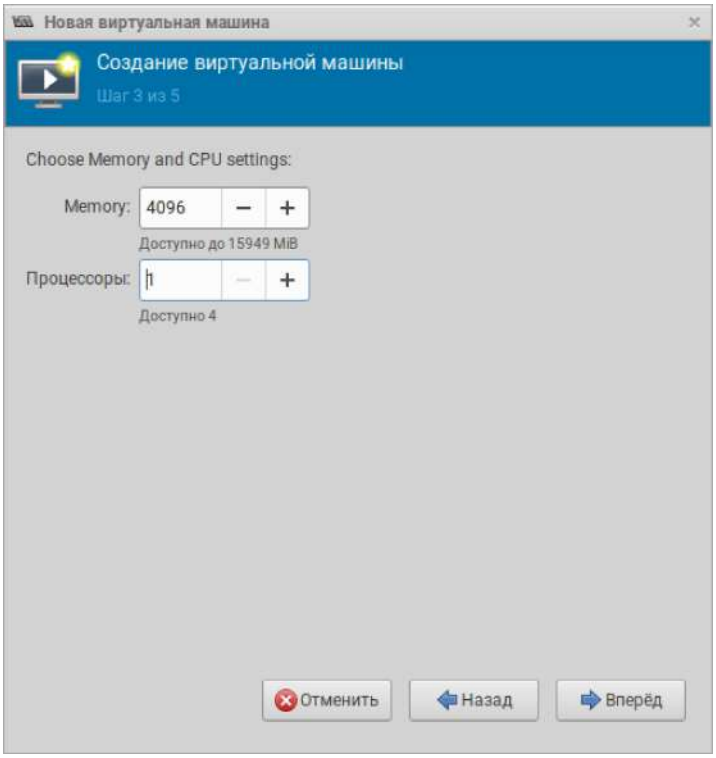


В выскочившем окне идем в ту папку, где лежит скачанный образ Devaun. Отмечаем его, после чего нажимаем «Ok».

Теперь снимаем галочку с «Automatically detect from the installation media / source». В поле ввода набираем «Debian» и среди выскочивших вариантов выбираем «Debian 11».

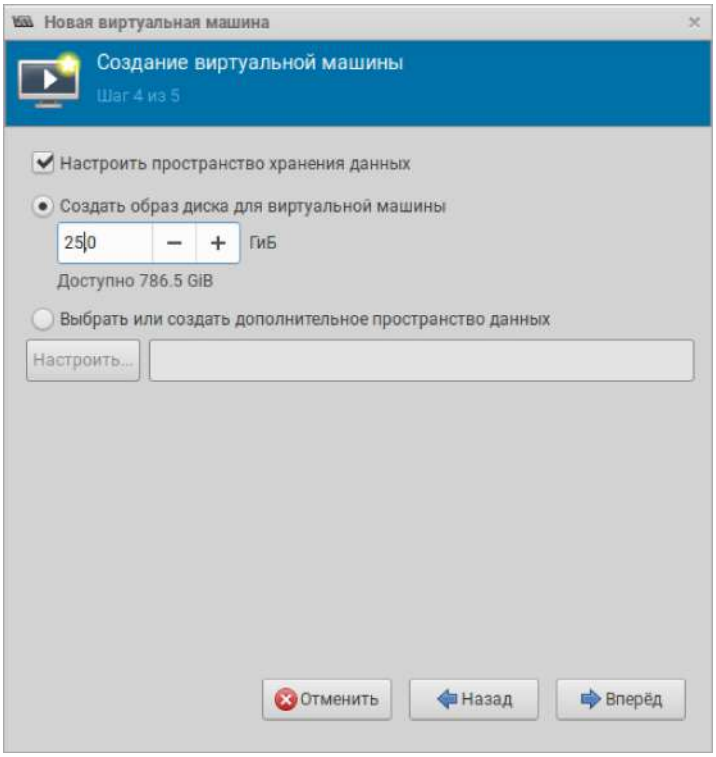


Нажимаем на кнопку «Вперед». Теперь, если у вас всего 4 Гб оперативной памяти то в «Оперативная память (ОЗУ)» введите 2048 Мб. 2 Гб вполне достаточно. Если у вас 8 Гб и более, можете выставить 4096 Мб. В этом случае у вас не будет необходимости устанавливать в виртуальную машину файл подкачки. Выделять виртуалке более 4 Гб нет совершенно никакой необходимости. Если у вас относительно современный процессор с четырьмя и более ядрами, то в «Процессоры» выставьте 2. Пары ядер, если процессор относительно мощный, вполне достаточно. Если у вас процессор относительно слабый, например Pentium, то можете выделить ему все четыре ядра.



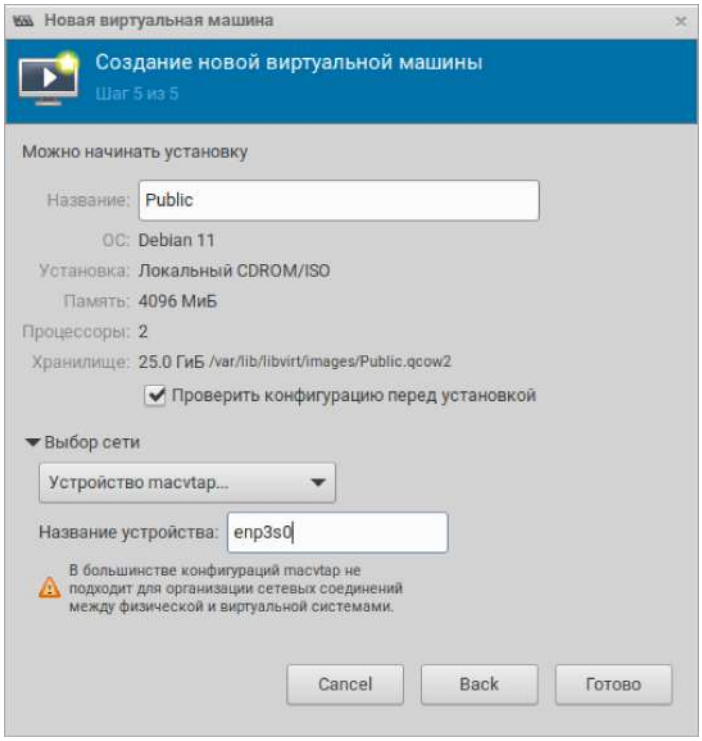
После того, как все выставлено, жмем «Вперед».

Теперь нужно выделить объем дискового пространства для установки виртуалки. Я рекомендую указывать не менее 15 Гб.



Нажимаем «Вперед».

Теперь нужно придумать и забить в поле название виртуальной машины. Ставим галочку на «Проверить конфигурацию перед установкой». После этого раскрываем графу «Выбор сети» и выбираем «Устройство macvtap» (напоминаю, что если используйте для подключения разные сетевые карты, то оставляйте NAT). В графе «Название устройства» указываем то, которое подключено к Интернету. Его название можно посмотреть в настройках соединения, для этого щелкаем по апплету сетевого соединения на панели внизу справа и смотрим в выскочившем окне интерфейс. Там указан тип, а в скобках само название. Его и нужно указать в графе названия устройства.



Нажимаем кнопку «Готово».

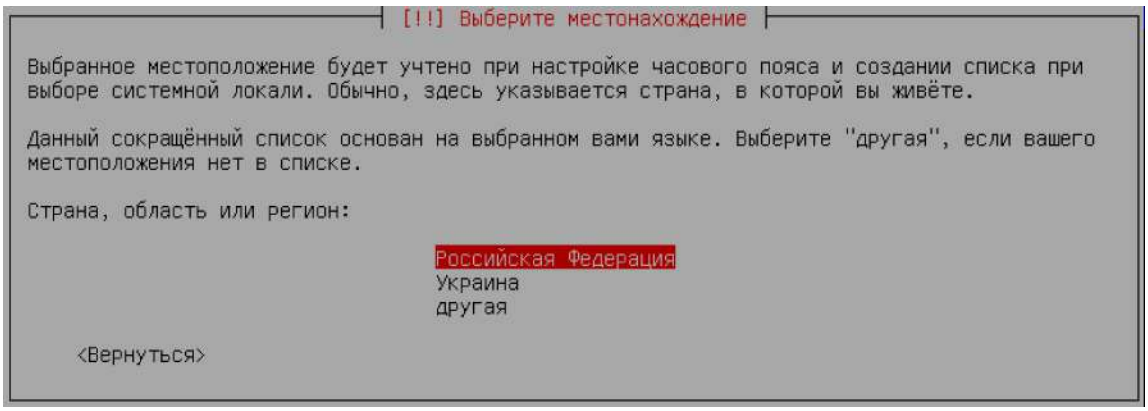
В появившемся окне можно дополнительно настроить некоторые параметры. Если хотите активировать графическое ускорение, то идите во вкладку «Дисплей Spice» и здесь поставьте галочку на «OpenGL». Это необходимо для какой-то тяжелой графической деятельности, например, для онлайн-игр и, возможно, для просмотра видео в разрешении 4K. Я не рекомендую без необходимости использовать данную функцию, поскольку это может стать дополнительным инструментом для идентификации вас. Для обычной деятельности, в том числе просмотра видео в HD-качестве, эта функция не нужна. После того, как все нужное выставлено, нажимаем внизу справа кнопку «Установить систему».

Появится черное окно, в котором через некоторое время возникнет картинка с надписями. Для комфортной работы с системой нажимаем на верхней панели «Вид» и щелкаем на «Под размер ВМ». Окно развернется под размер экрана виртуальной машины. Когда мы установим систему, мы сможем выставить настройки дисплея для разворота во весь экран, а пока работаем так. По умолчанию выделена графа установки. Нажимаем «Enter».

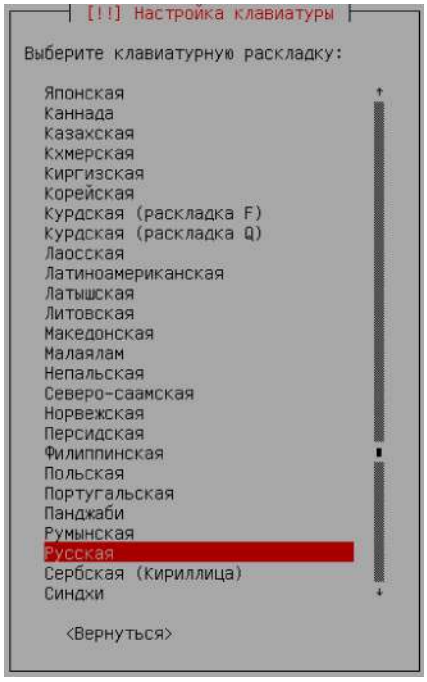
Появляется выбор языка. Выбираем нужный нам с помощью стрелок на клавиатуре.

Нажимаем «Enter».

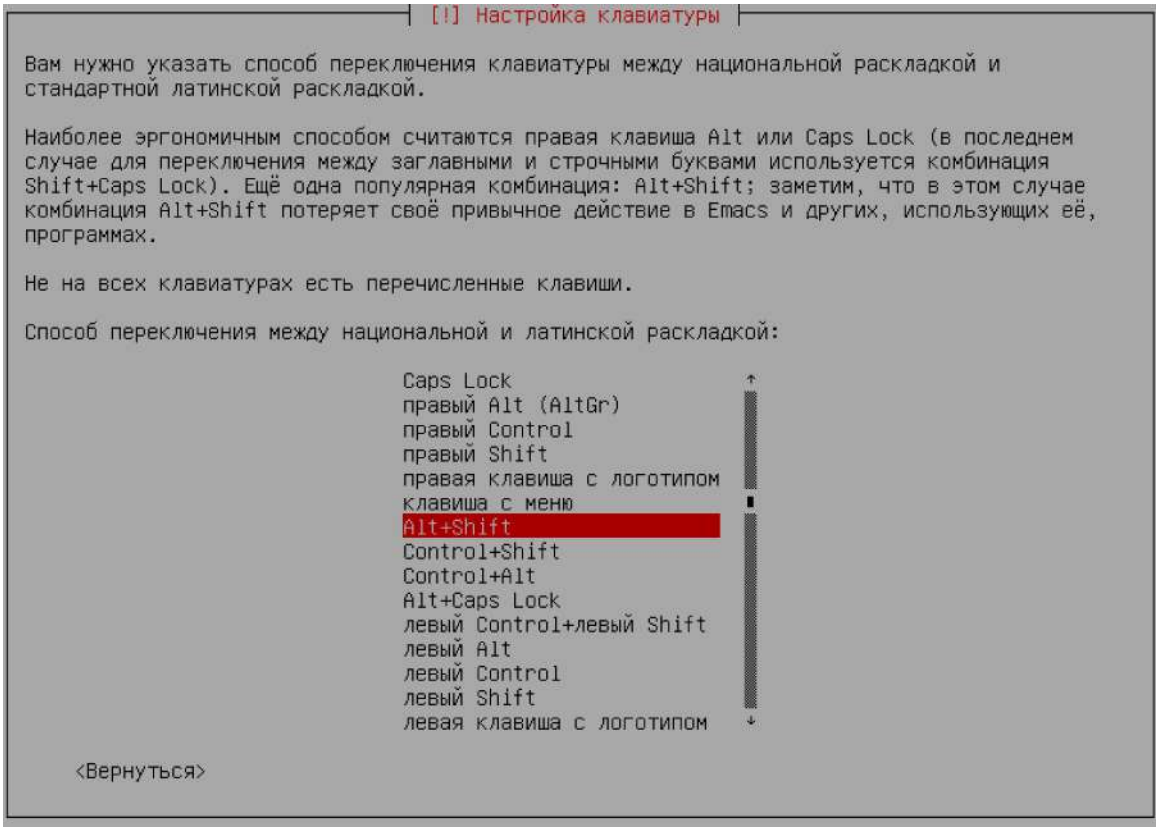
Выбираем страну и нажимаем «Enter».



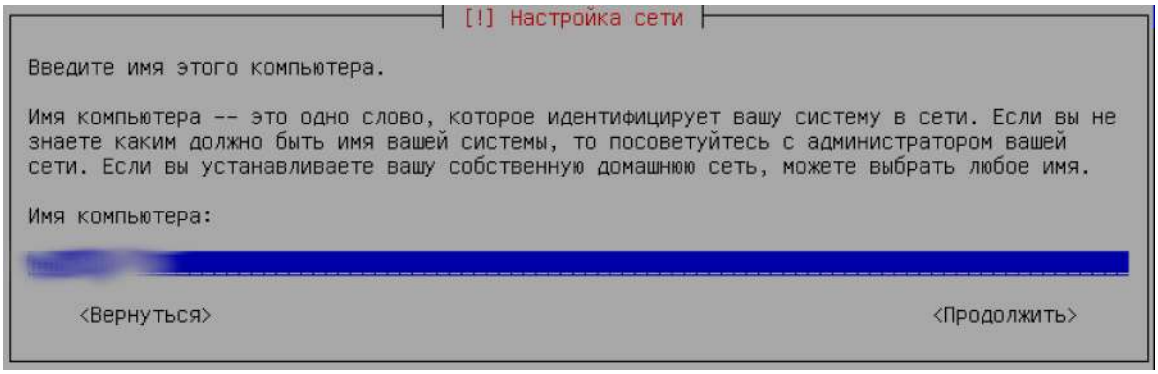
Выбираем раскладку клавиатуры и снова жмем «Enter».



Выбираем способ переключения раскладки клавиатуры. Снова «Enter».

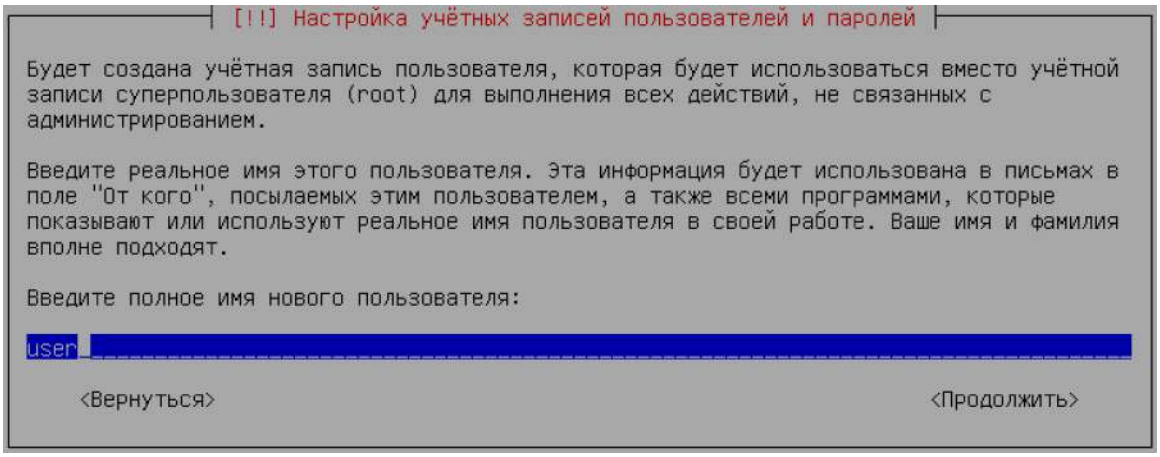


Придумываем и вбиваем название компьютера (виртуальной машины). Желательно, чтобы оно отличалось от названия, которое было выбрано для основной операционной системы.

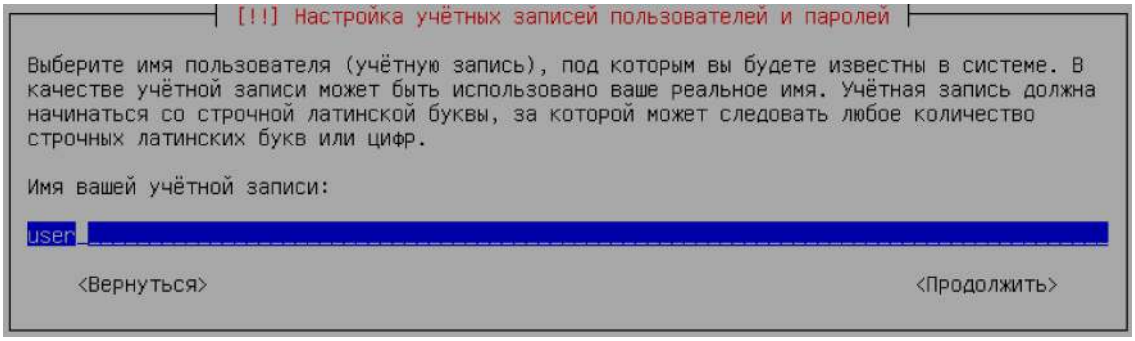


Вбиваем, а затем повторяем пароль суперпользователя. Я рекомендую, чтобы не путаться, вбивать тот же пароль, что и в основной операционной системе. Если у компьютера несколько пользователей, и в основной операционной системе несколько учетных записей, и ваш пароль пользователя отличается от пароля root, то используйте пароль пользователя, а не root.

Вводим имя пользователя. Здесь те же принципы, что и при установке основной операционной системы. Не вбивать настоящее имя. Один из наиболее предпочтительных вариантов, вбивать просто «user».

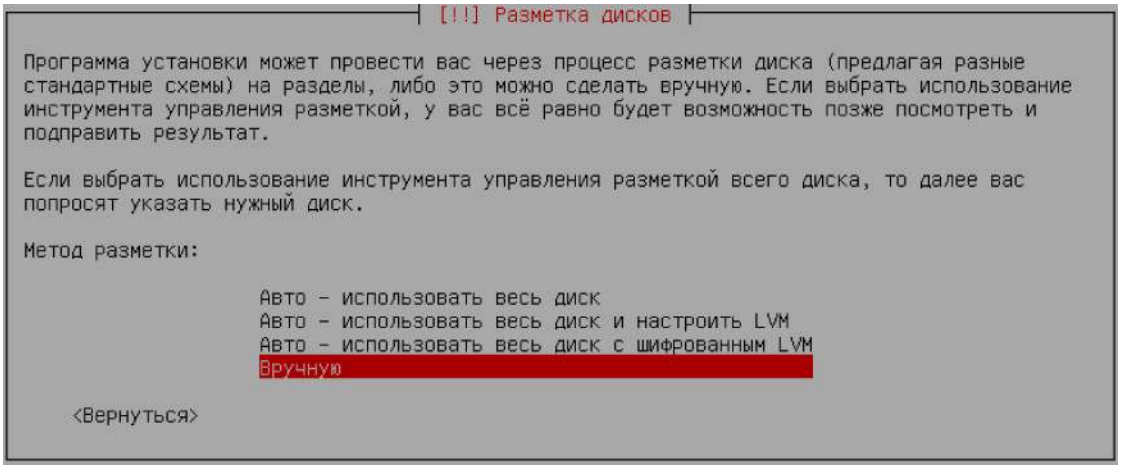


Вводим имя учетной записи. Здесь также придумывайте, что хотите, но чтобы не путаться, лучше, чтобы оно совпадало с именем пользователя.

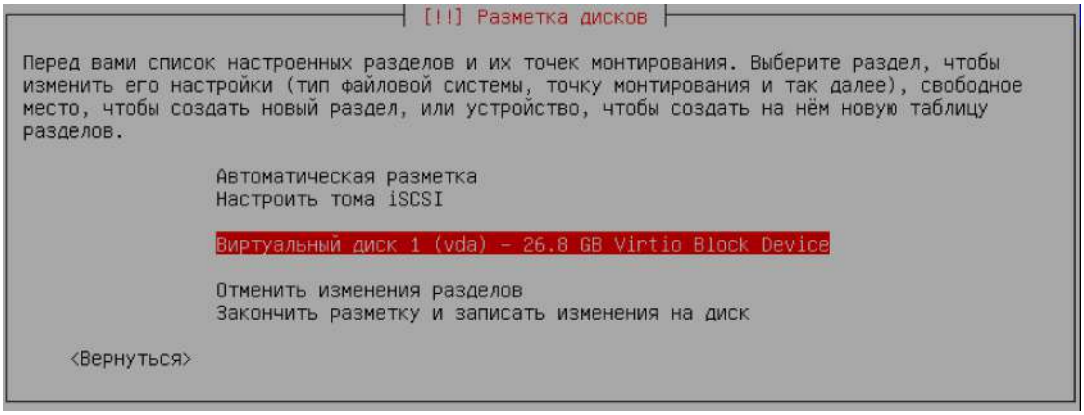


Вводим пароль пользователя. Чтобы не путаться, я рекомендую вводить тот же пароль, что вводили для суперпользователя.

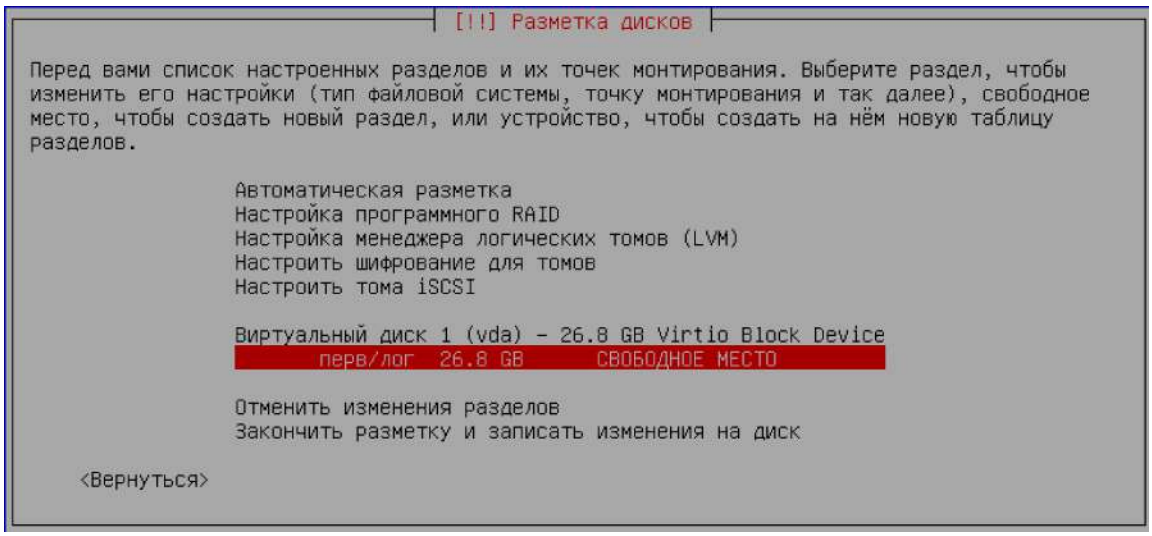
Теперь пришло время разметить диск. Если вы выделили всего 2 Гб оперативной памяти, то можете смело нажимать «Авто — разметить весь диск». В этом случае автоматически будет выделено пространство под установку и раздел подкачки, равный объему выделенной оперативной памяти. Если вы выделили 4 Гб, то раздел подкачки не нужен, и лучше разметить диск вручную. В этом случае выбираем, собственно, «Вручную».



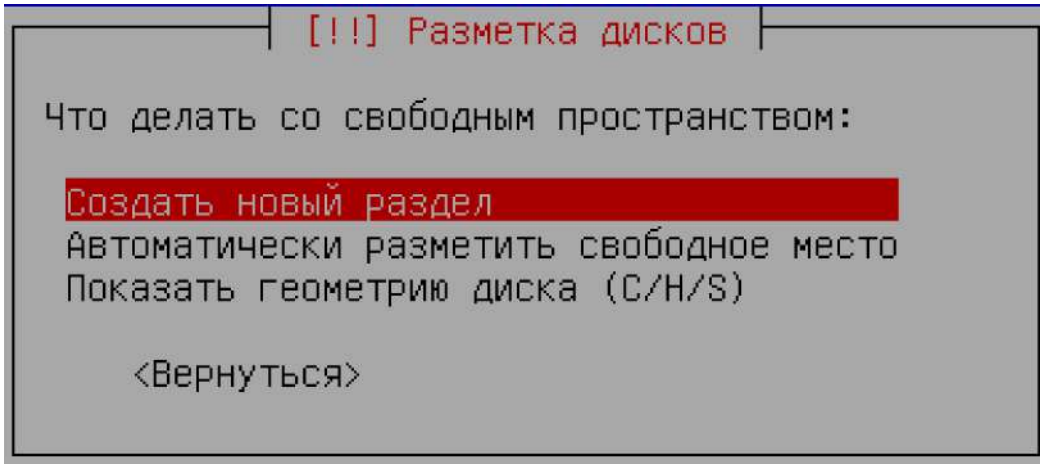
Выбираем там где «Виртуальный диск».



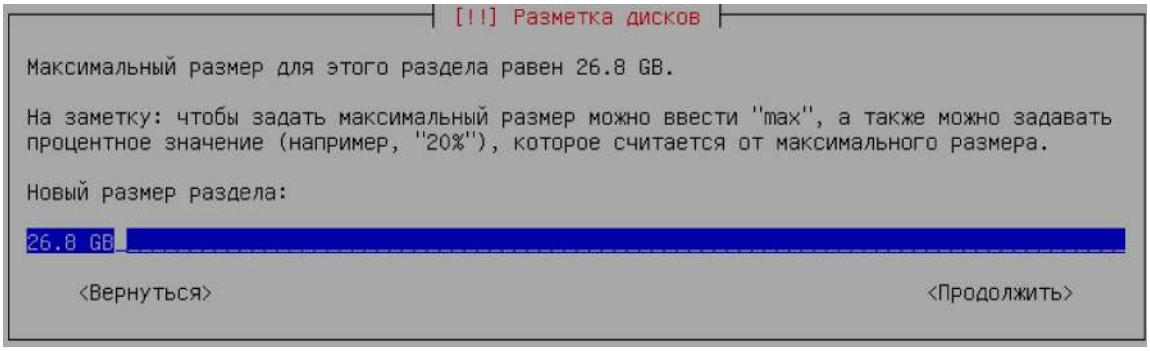
На вопрос создать ли новую пустую таблицу разделов, указываем «Да».
Выбираем там где «СВОБОДНОЕ МЕСТО».



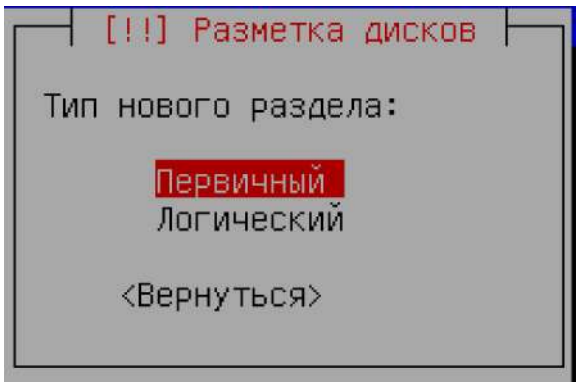
Выбираем «Создать новый раздел».



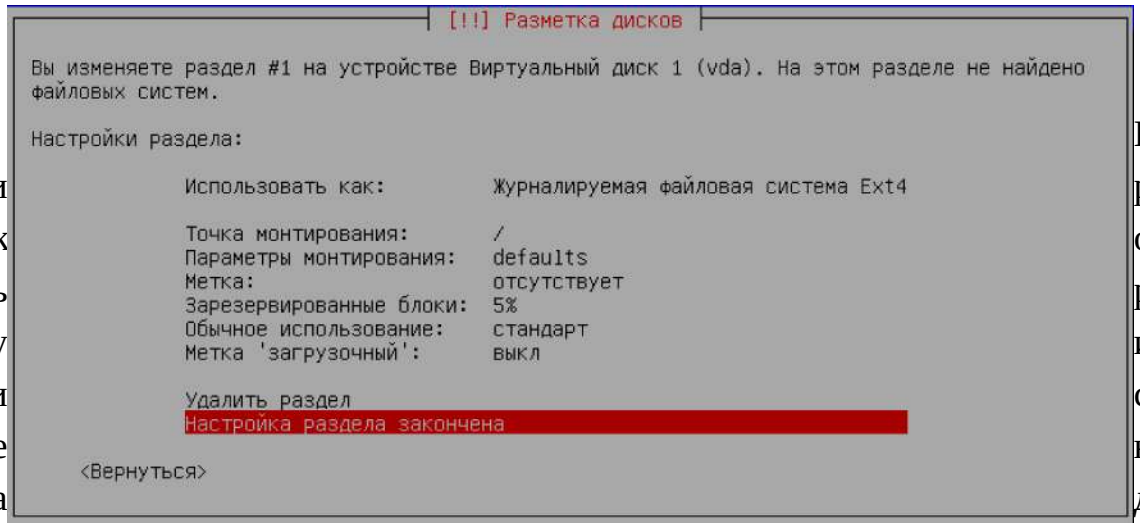
Оставляем весь объем диска.



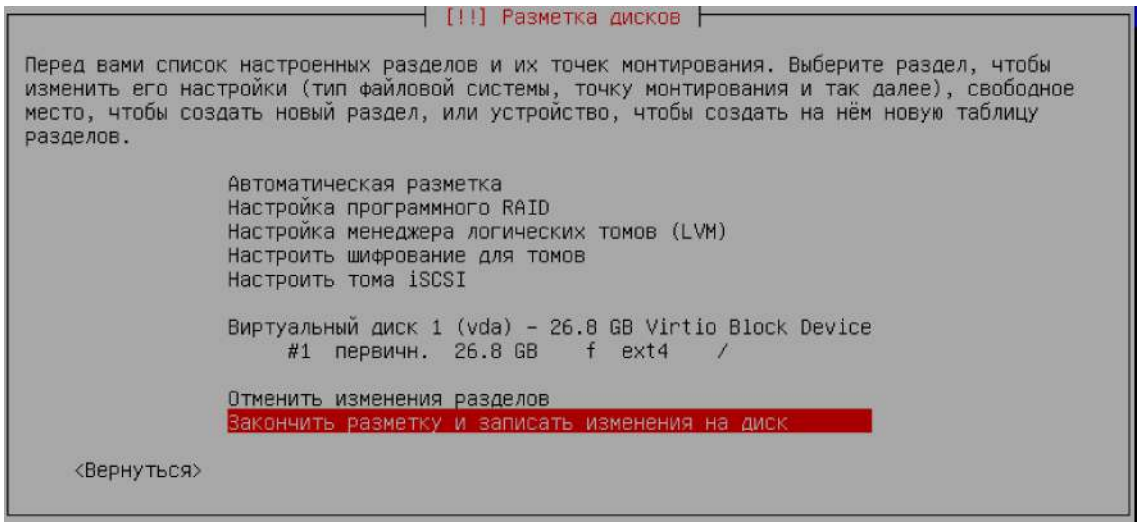
Выбираем «Первичный».



Проверяем, чтобы «Точка монтирования» стоял «/». После чего выбираем «Настройка раздела закончена».



Выбираем «Закончить разметку и записать изменения на диск».



На вопрос, хотим ли мы вернуться в меню разметки, указываем «Нет».

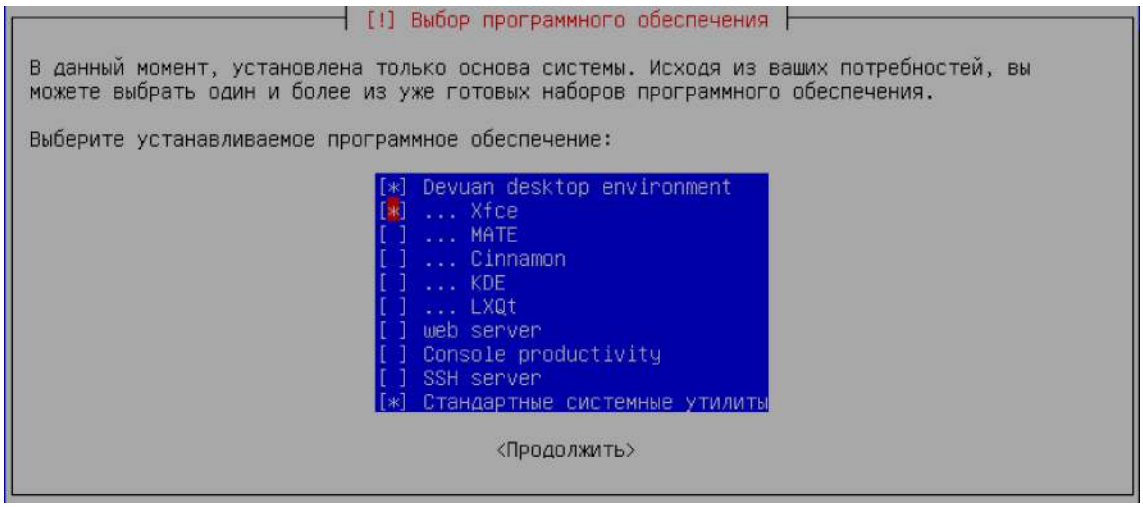
А на вопрос, записать ли изменения на диск, «Да».

Начнется процесс установки. Когда появится окно с вопросом, нужно ли просканировать дополнительный установочный носитель, выбираем «Нет».

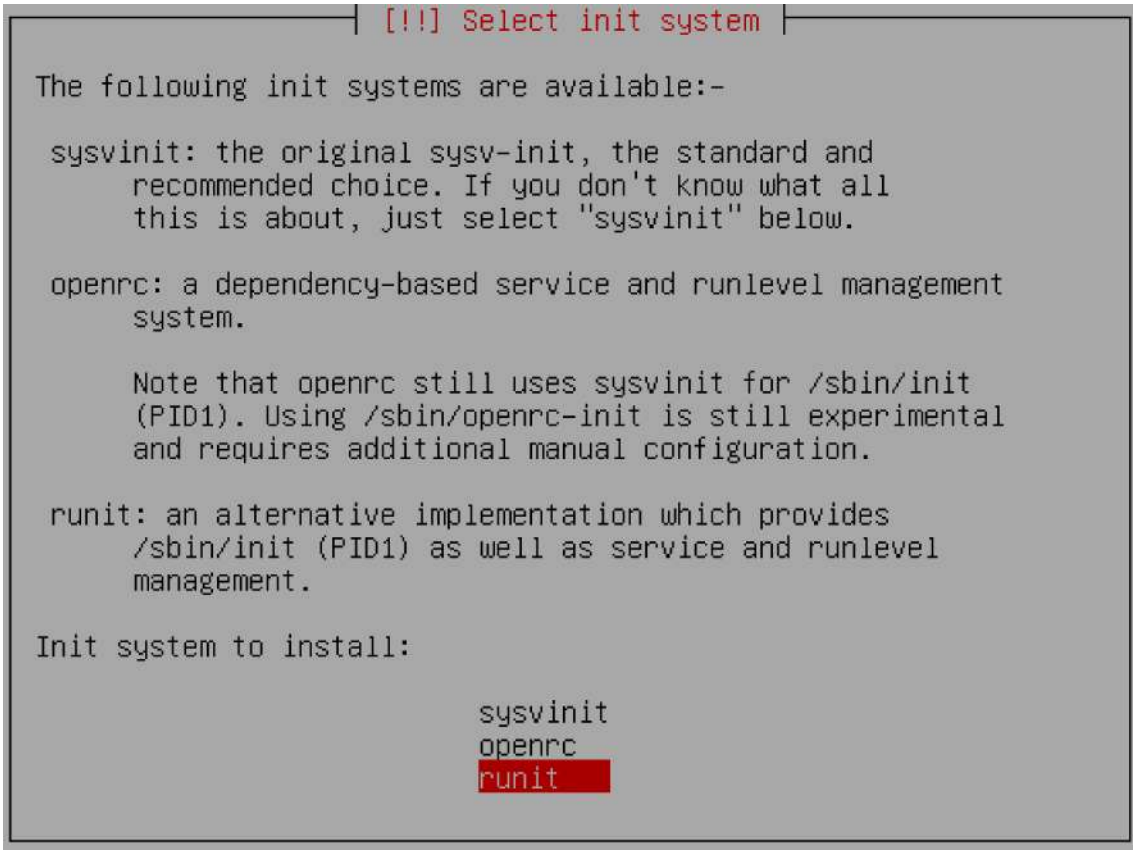
Отказываемся от использования зеркала архива из сети.

Также как и от участия в опросе популярности пакетов.

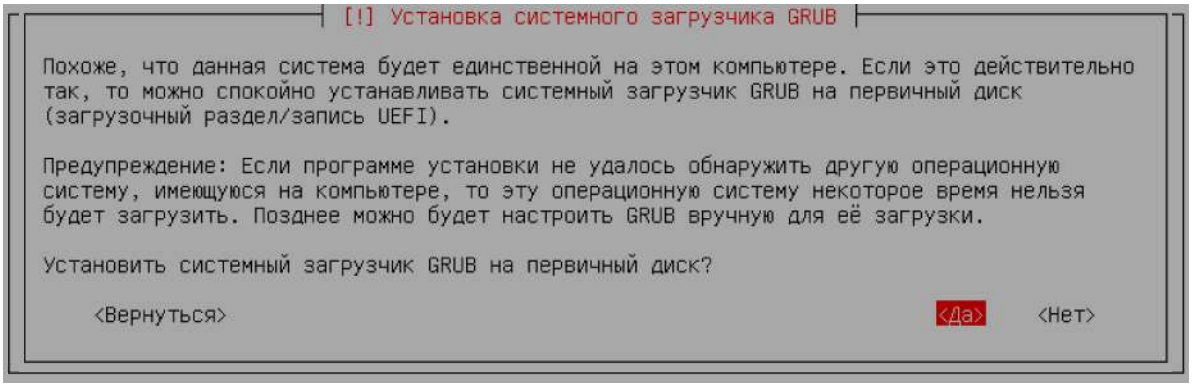
Когда закончится эта стадия установки придет время выбрать компоненты системы, которые нужно установить. Во-первых, нужно определиться с графической оболочкой. От этого зависит, как будет выглядеть операционная система, но и также, насколько она будет производительной и функциональной. Оболочка KDE очень тяжеловесная, и без графического ускорения с ней работать невозможно. Оболочка Cinnamon представляется очень удобной, однако она также крайне тяжеловесная и требует аппаратного ускорения. Активировать его только чтобы использовать определенные графические оболочки, я считаю нерационально. MATE не слишком тяжелая, довольно красивая (в конце концов именно ее использует Trisquel), и в целом ее можно рекомендовать. Однако она проигрывает в гибкости настройки одной из оболочек. Аналогична ситуация с LXQt. Наиболее легковесной из представленных является оболочка XFCE. Она очень гибко настраиваемая. И именно ее я всецело рекомендую. В принципе, ничто не мешает вам установить несколько графических оболочек и самому попробовать каждую. В данном пособии будет использоваться XFCE, как наиболее гибкая и при этом легковесная. Жмем «Enter».



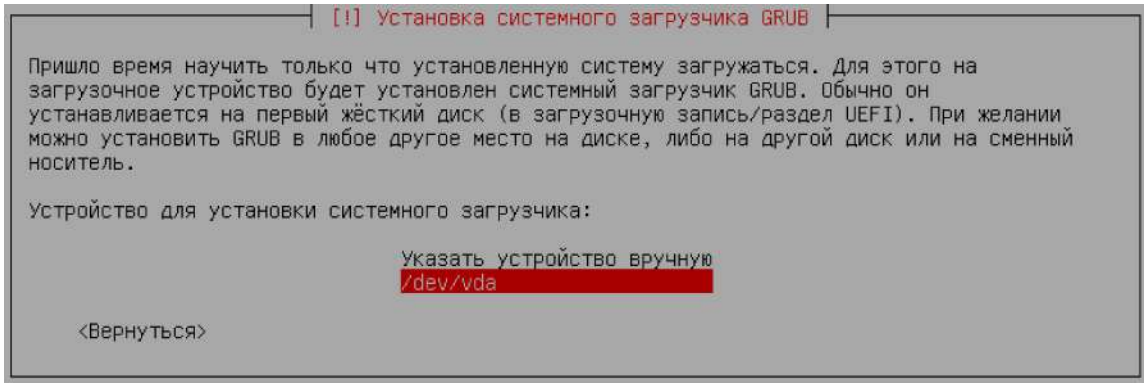
Когда установка закончится, появится вопрос, какой инициализатор установить. Я рекомендую выбирать Runit, поскольку он наиболее современный, и с ним система показывает наилучшую производительность.



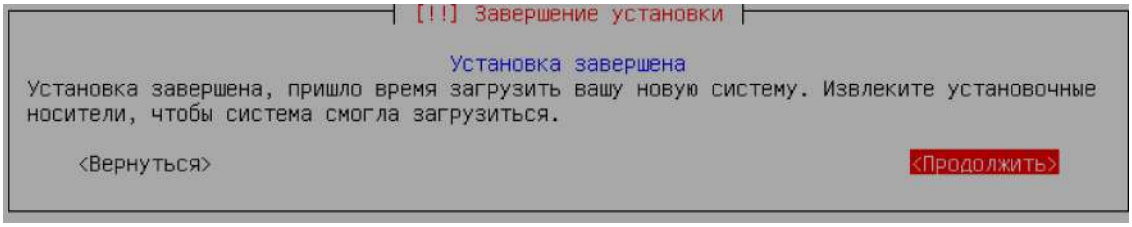
Когда установка инициализатора закончится, появится вопрос, установить ли системный загрузчик GRUB на первичный диск? Выбираем «Да».



Указываем «dev/vda».



Когда установка закончится, появится сообщение, что все завершено успешно и нужно перезагрузить компьютер. Нажимаем «Enter».



После того, как виртуальная машина перезагрузится, iso-образ будет как бы извлечен из виртуального дисковода, и произойдет загрузка операционной системы, установленной на виртуальный жесткий диск.

21 Настройка публичной виртуальной машины

После запуска появится окно в котором нужно будет ввести имя пользователя и пароль. В дальнейшем мы автоматизируем вход в систему.

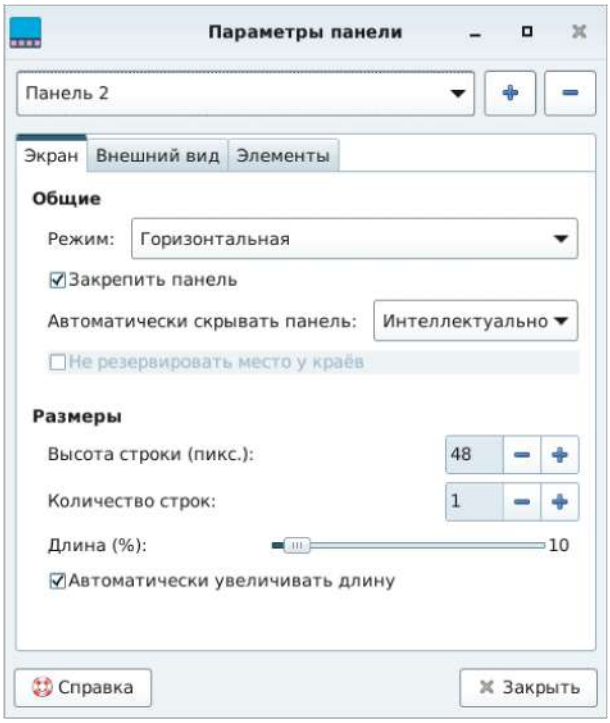
Обращаю внимание, что если вы установили несколько графических оболочек, то выбрать, какую из них загружать, можно нажав колесо справа сверху. В выпавшем поле будут все установленные графические оболочки. Вводим имя пользователя и пароль и нажимаем «Enter».

Открывается рабочий стол, вид которого напоминает вид MacOS. Если вам он нравиться, можете оставить, как есть. Однако, если вы пересели с Windows, вам скорее всего это будет неудобно, и я сейчас покажу, как настроить внешний вид. Но для начала проверьте, работает ли Интернет. Если вверху справа на панели кружится значок, похожий на загрузку, значит нет соединения. Также можете запустить браузер и проверить, грузятся ли сайты. Если нет, то возможно, виртуалка не верно определила драйвер для виртуального сетевого адаптера, который связан с реальным. Чтобы исправить проблему, выключите виртуалку (выключение в Меню на панели вверху слева). Нажмите на синий значок с буквой i «Показать виртуальное оборудование» на окне виртуалки вверху слева и выберите значок двух стрелочек вверх и вниз с надписью, похожей на «NIC :11:11:11» (цифры будут другими). Здесь в графе «Модель устройства» выберите «virtio», а если оно и стоит, то «rtl8139» и нажмите «Применить» внизу справа. После этого перезапустите виртуалку. Если после перезапуска на верхней панели все еще крутится загрузка, нажмите на нее правой кнопкой мыши, выберите «Изменить соединение», нажмите на имеющиеся соединение, а затем на значок колеса внизу слева. После этого в графе «Метод» выберите набор цифр в кавычках, перед которыми есть маркировка, например «eth». После этого нажмите «Сохранить» внизу справа. Если у вас Wi-Fi, и все это не помогает, то необходимо установить в систему драйвер адаптера, как и в основной системе. Если и это не решает проблемы, то остается включить NAT, и подключать виртуалку по нему, при этом настроив в основной системе фаервол, как это было сказано для такого случая. Если все в порядке, можно переходить к настройке внешнего вида.

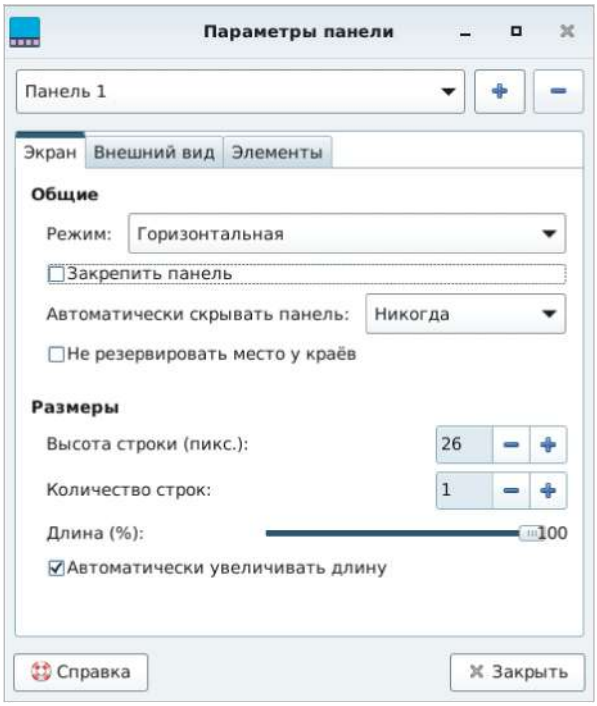
Для начала, если виртуальная машина не разворачивается на весь экран, идем в Меню (оно слева сверху), категория «Настройки» и нажимаем «Дисплеи». В появившемся окне выставляем нужное разрешение и нажимаем применить. После этого, разворачиваем виртуальную машину на весь экран, для этого нажимаем соответствующую кнопку справа на верхней панели окна виртуалки. Теперь, чтобы свернуть виртуальную машину нужно нажать соответствующую клавишу в поле, вылезающем по-середине сверху, когда туда

подводится курсор мыши. Сохраняем настройки экрана.

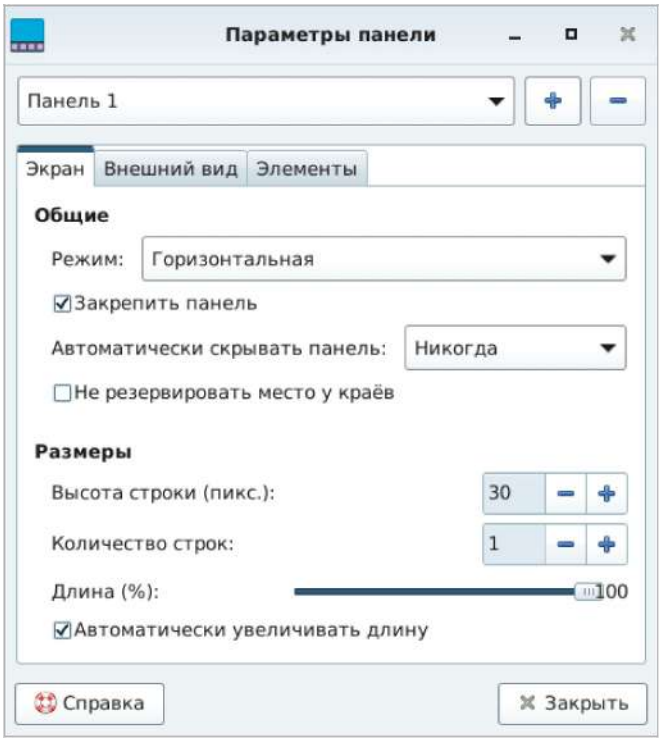
Теперь приступаем непосредственно к настройке внешнего вида. Чтобы убрать нижнюю панель, нажимаем по верхней панели (на нижней может не сработать) правой кнопкой мыши, наводим курсор на «Панель» и выбираем «Параметры панели». В появившемся окне, в верхней графе меняем «Панель 1» на «Панель 2» и нажимаем знак минус (–) слева от графы. Панель будет удалена.



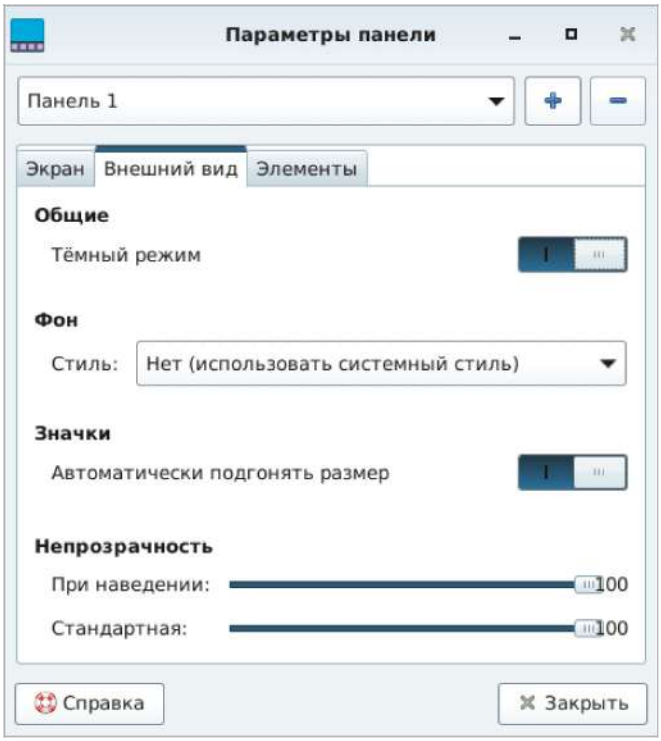
Теперь переместим верхнюю панель вниз. Для этого указываем в той же графе «Панель 1». Затем снимаем галочку с «Закрепить панель». После этого по бокам панели появятся точки. Беремся мышью за одну из них и тащим панель вниз.



Когда панель перетащена, ставим галочку на «Закрепить панель».

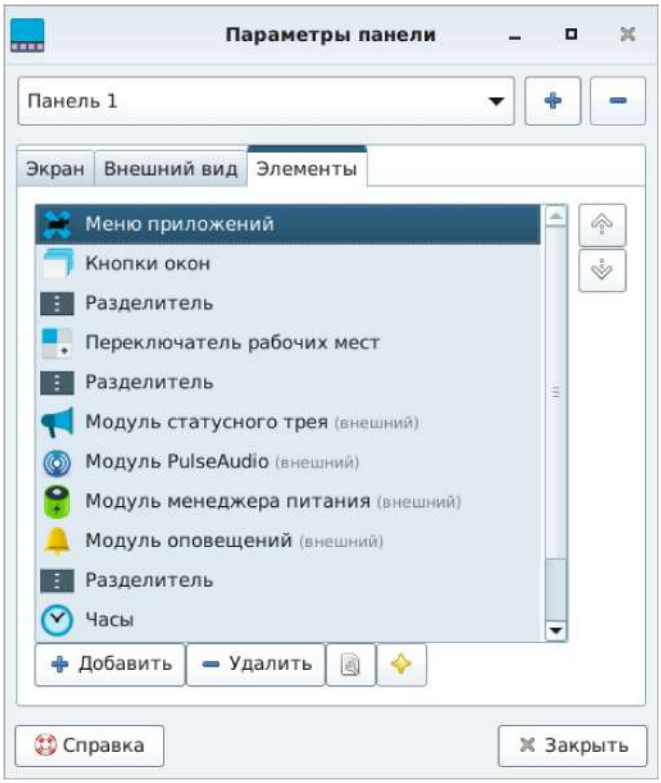


Также можно перейти во вкладку «Внешний вид» и настроить все по своим нуждам.



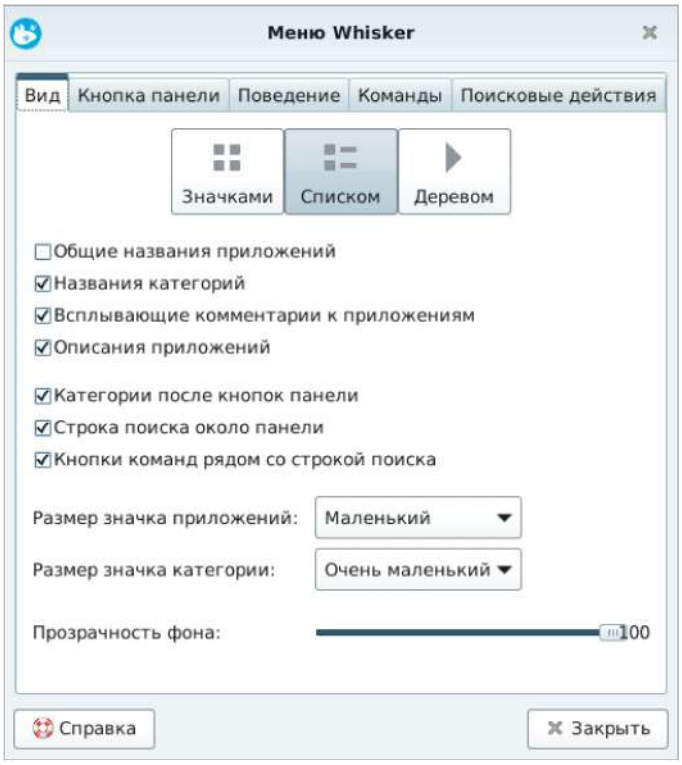
Добавим на панель кое-какие недостающие апплеты. Для этого также щелкаем по ней правой кнопкой мыши, наводим на «Панель» и нажимаем «Добавить новые элементы». В выскочившем окне нажимаем «Добавить».

Находим «Раскладка клавиатуры», отмечаем ее и нажимаем «Добавить». По-умолчанию в XFCE используется достаточно неказистое Меню. Если вы любите минимализм, то можете пользоваться им. Если же хотите что-то более броское, добавьте также «Меню Whisker». Можете добавить также еще какие-нибудь нужные вам апплеты.



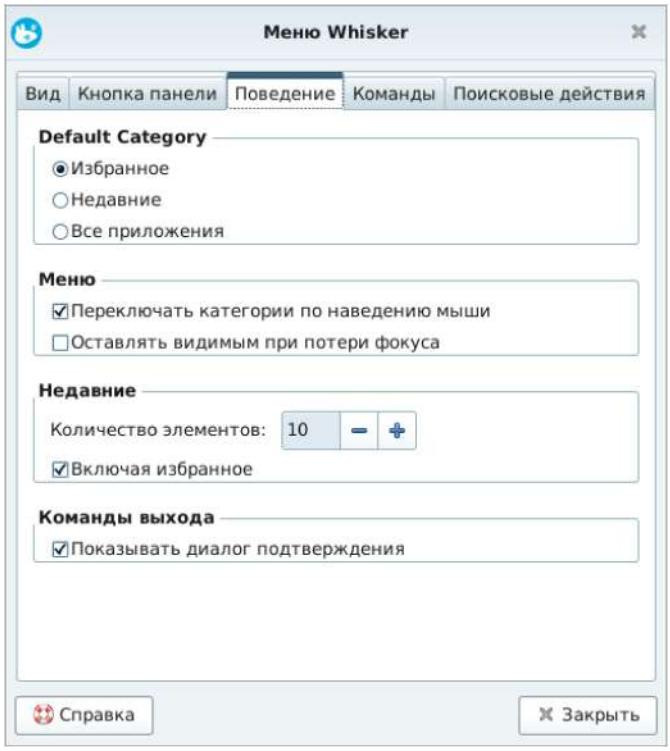
Когда все добавлено, закрываем окно добавления и можем удалить ненужные нам апплеты. Для этого выделяем их и нажимаем «Удалить». Затем закрываем окно. После этого нажимаем на апплет «Меню Whisker» и затем нажимаем «Переместить». После чего перетаскиваем влево до конца, на место Меню. Похожим образом расставляем и другие апплеты, как вам хочется.

После этого можно настроить внешний вид Меню. Для этого нажимаем по значку Меню правой кнопкой мыши и выбираем «Свойства». В появившимся окне во вкладке «Вид», собственно производим настройку вида. Здесь можно изменить, например, отображение описания приложений и комментариев к ним, прозрачность фона. Также выставить расположение строки поиска и кнопок выключения.



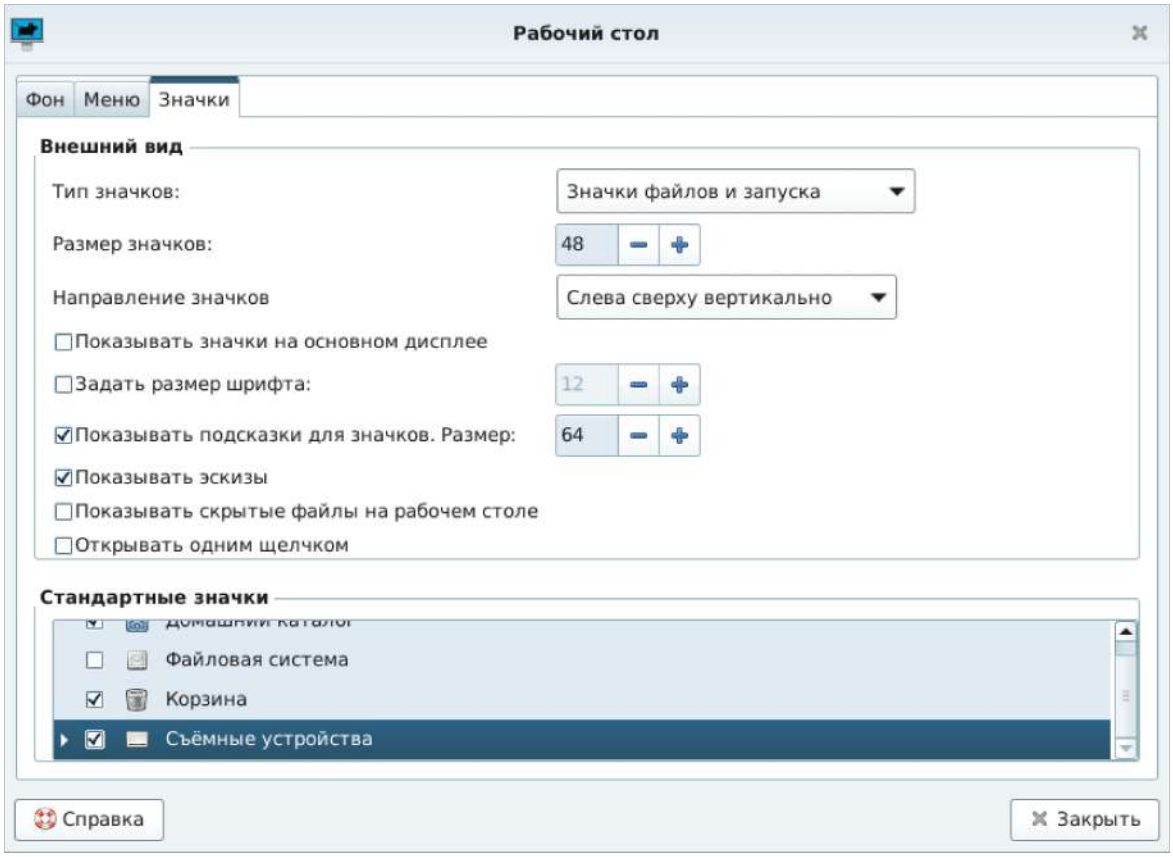
Во вкладке «Кнопка панели», щелкнув на значок, можем выбрать значок, который нам больше нравится. Также здесь настраивается размер панели и значков.

Во вкладке «Поведение» можем выставить переключение категорий по наведению мыши.

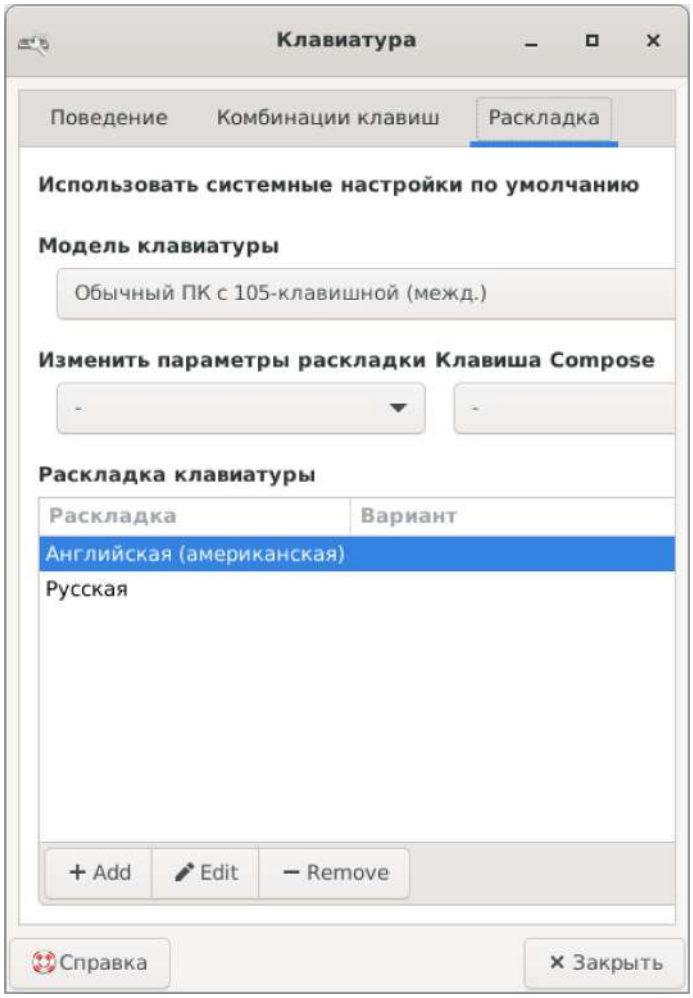


После этого продолжаем настройку внешнего вида. Для этого идем в Меню, категория «Настройки» и выбираем «Внешний вид». В выскочившем окне во вкладке «Стили» можно выбрать темы. Во вкладке «Значки» выбрать темы значков. В других вкладках, можно настроить шрифты и произвести другие настройки.

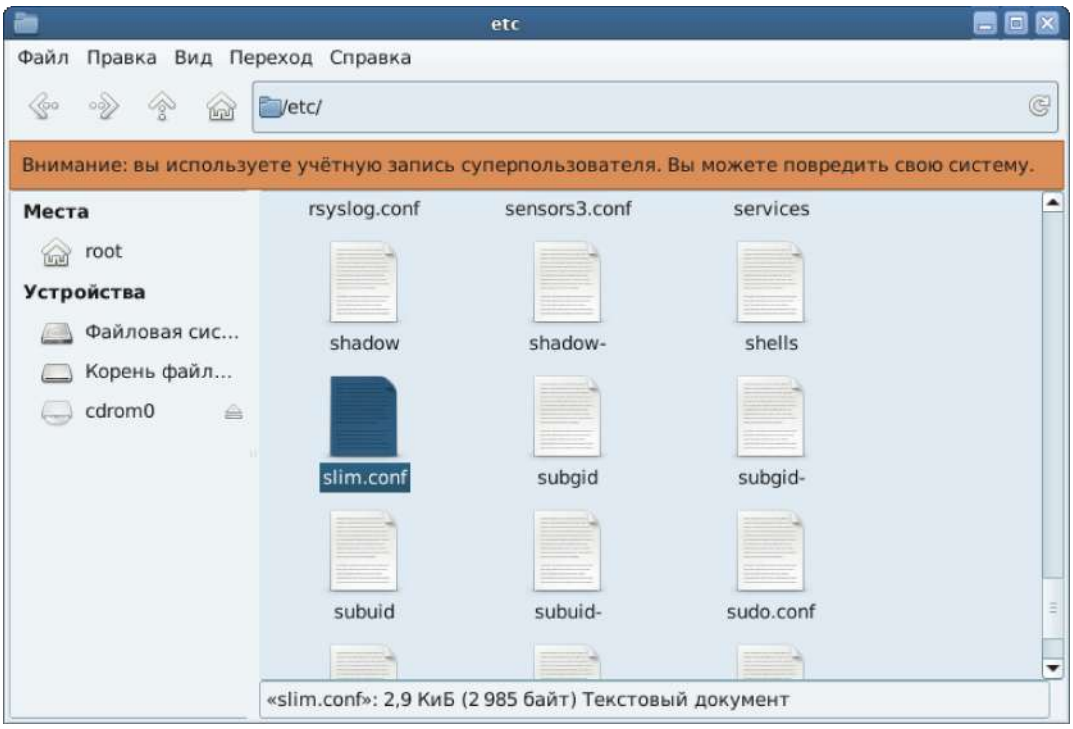
После того, как все нужные настройки произведены, закрываем окно. Нажимаем правой кнопкой мыши по рабочему столу и в появившемся поле выбираем «Настройка вида Рабочего стола». В появившемся окне можно сменить фон, однако выбора обоев почти нет, если хотите какие-то другие, их придется скачать отдельно. Также здесь можно настроить значки рабочего стола, удалить ненужные, изменить размер и т.д.



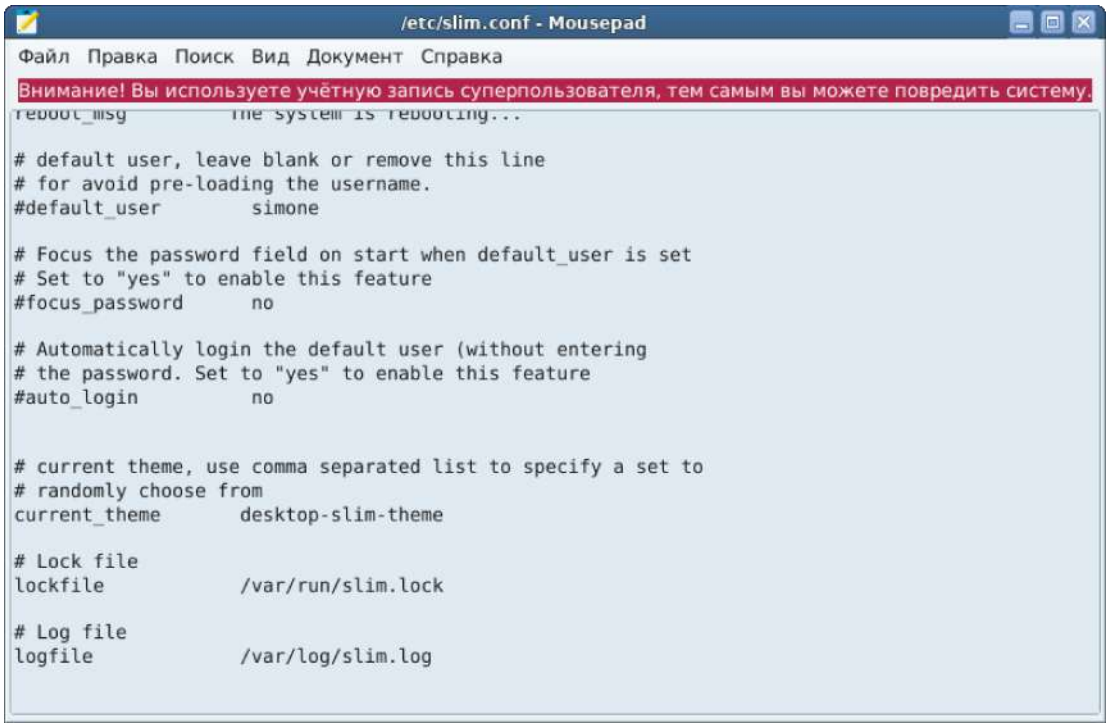
После того, как настройка дизайна закончена, нужно задать раскладку клавиатуры, если она не установилась автоматически. Для этого идем в Меню, категория «Настройки» и нажимаем «Клавиатура». Во вкладке «Раскладка» нажимаем кнопку «Add» внизу, выбираем нужный язык и нажимаем «Ok». Проверяем работу раскладки и закрываем окно.



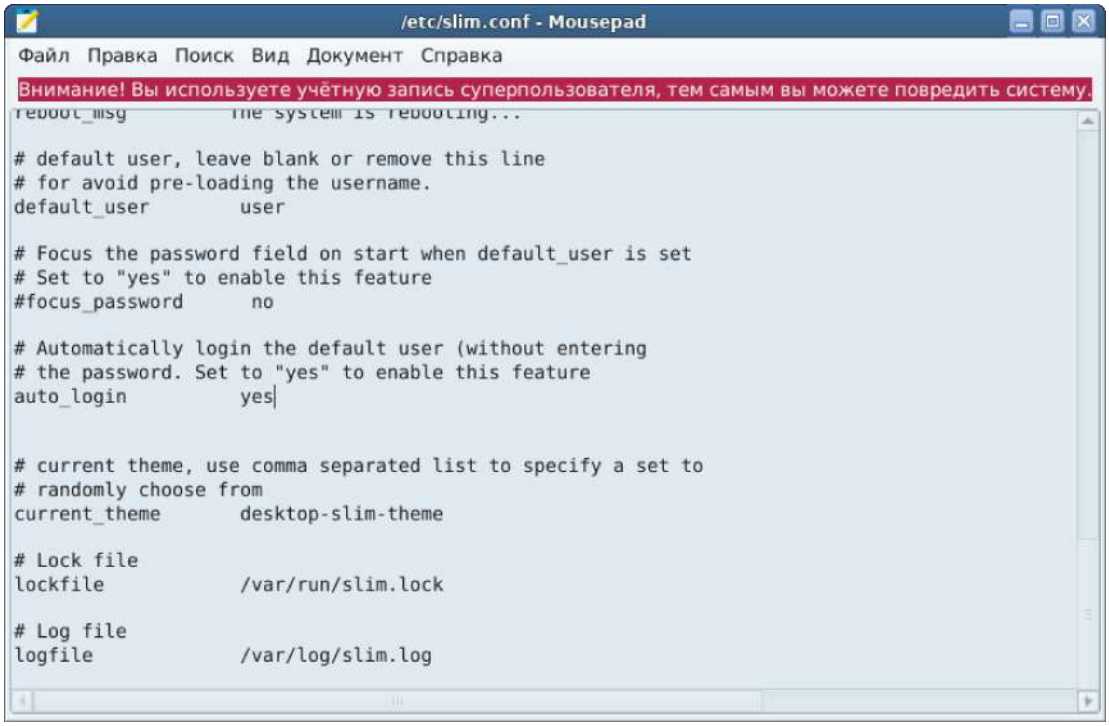
Теперь включим автоматический вход в систему, чтобы каждый раз не вводить имя пользователя и пароль. Для этого открываем терминал сочетанием клавиш Ctrl-Alt-T. Набираем su и нажимаем «Enter». Затем вводим пароль и снова «Enter». Затем sudo bash и «Enter». Теперь thunar. Мы запустили файловый менеджер с правами суперпользователя. Переходим в корневой каталог и идем в папку etc. Здесь находим файл slim.conf и открываем его в редакторе Mousepad, для чего щелкаем по нему правой кнопкой мыши, нажимаем «Открыть с помощью», затем «Открыть в другом приложении». В открывшемся окне выбираем Mousepad и ставим галочку на «Использовать по-умолчанию для этого типа файлов».



В открывшемся окне спускаемся вниз и ищем строчки default_user и auto_login.

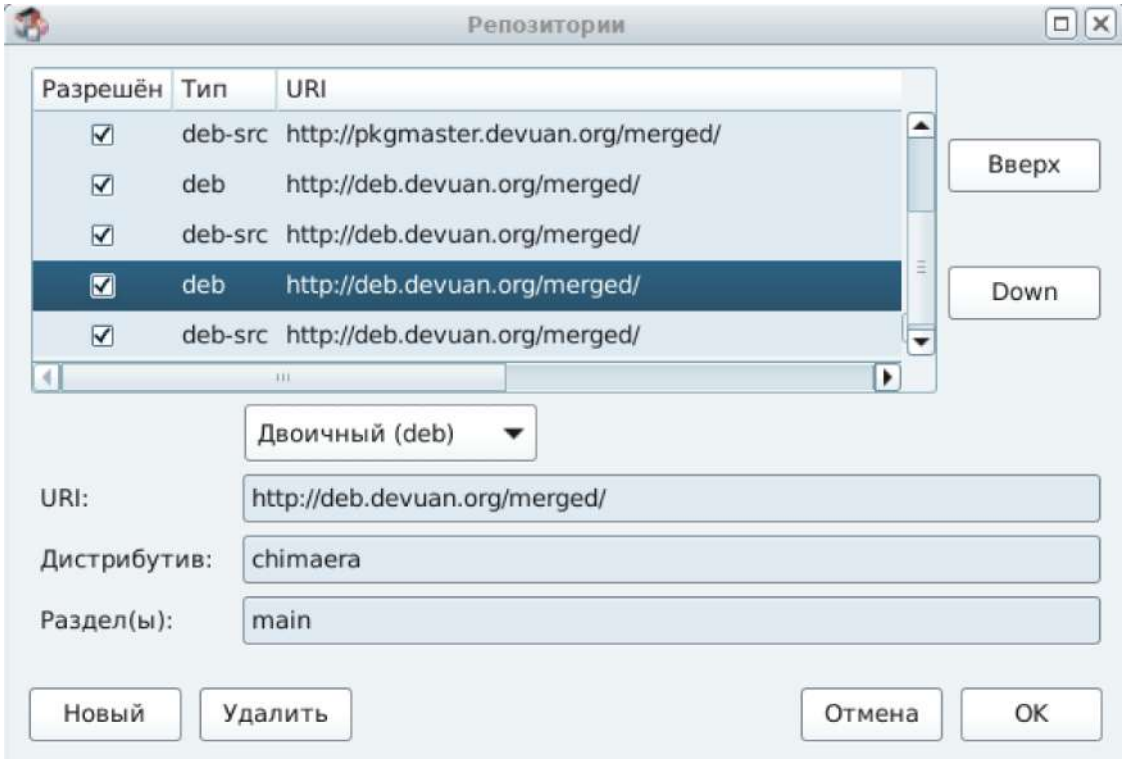


В первой строчке вместо simone нужно вбить имя пользователя, а во второй вместо no указать yes. После чего строчки нужно раскомментировать, т.е. снять перед ними значок решетки (#).



Сохраняем и закрываем все окна.

Теперь пришло время обновить систему. Для этого идем в Меню, категория «Система» и нажимаем «Менеджер пакетов Synaptic». Прежде чем приступать к обновлению, необходимо настроить репозитории. Поэтому нажимаем на верхней панели «Инструменты» и выбираем «Репозитории». В открывшемся окне снимаем галочку со строки в которой указан CD, иначе при попытке обновиться, Synaptic начнет искать диск и, не найдя, выдаст ошибку. Затем ставим галочки на всех других репозиториях. После чего необходимо пройтись по всем ним и в графе «Разделы» убрать слова «contrib» и «non-free», оставив только «main». В разделе main находятся только свободные программ. В разделе contrib программы тоже свободны, но имеют зависимости от несвободных. В принципе их можно использовать, но поскольку такая политика нас не устраивает, мы эти разделы отключаем. В разделе non-free содержатся несвободные программы, их использование противопоказано. Далее необходимо добавить некоторые репозитории. Нажимаем «Новый» и в верхней строке вводим http://deb.devuan.org/merged. В средней вводим chimaera. А в нижней main. Затем снова нажимаем «Новый», вместо «Двоичный (deb)» выбираем «Исходный код (deb-src)» и заполняем строки точно также, как в предыдущем случае. Нажимаем «Ok».



Выскочит окно с предложением обновить список пакетов. Нажимаем «Обновить». После того, как пройдет поиск обновлений, в первую очередь устанавливаем пакет apt-transport-https. Он позволяет скачивать программы и обновления с применением шифрования. После того, как этот пакет будет установлен, идем в «Инструменты» и выбираем «Репозитории». Теперь в репозиториях http://pkgmaster.devuan.org/merged нужно прописать вместо http, https. После чего нажимаем «Ok». Теперь все обновления будут скачиваться с применением шифрования. После этого снова обновляем список пакетов, а затем нажимаем «Отметить все обновления». Выскочит сообщение о том какие пакеты будут обновлены, и какой объем для этого нужно скачать. Нажимаем «Применить». После чего снова нажимаем «Применить».

После того как пройдет обновление, выключаем виртуальную машину. Для этого просто жмем кнопку выключения в Меню.

Когда виртуалка выключиться, нажимаем на верхней панели на кнопку «Снимки». После чего жмем знак плюс (+) внизу слева. В выскочившем окне набираем что хотим или просто щелкаем «Ok». Мы сделали снимок состояния виртуальной машины. Теперь, если мы допустим какую-то ошибку, настроим все неправильно и захотим все вернуть в нынешнее состояние, мы сможем это сделать, просто откатив систему к этому состоянию с помощью снимка. Такие снимки я рекомендую делать после каждого крупного шага настройки, чтобы иметь возможность исправить ошибку, если вы ее допустите на следующем

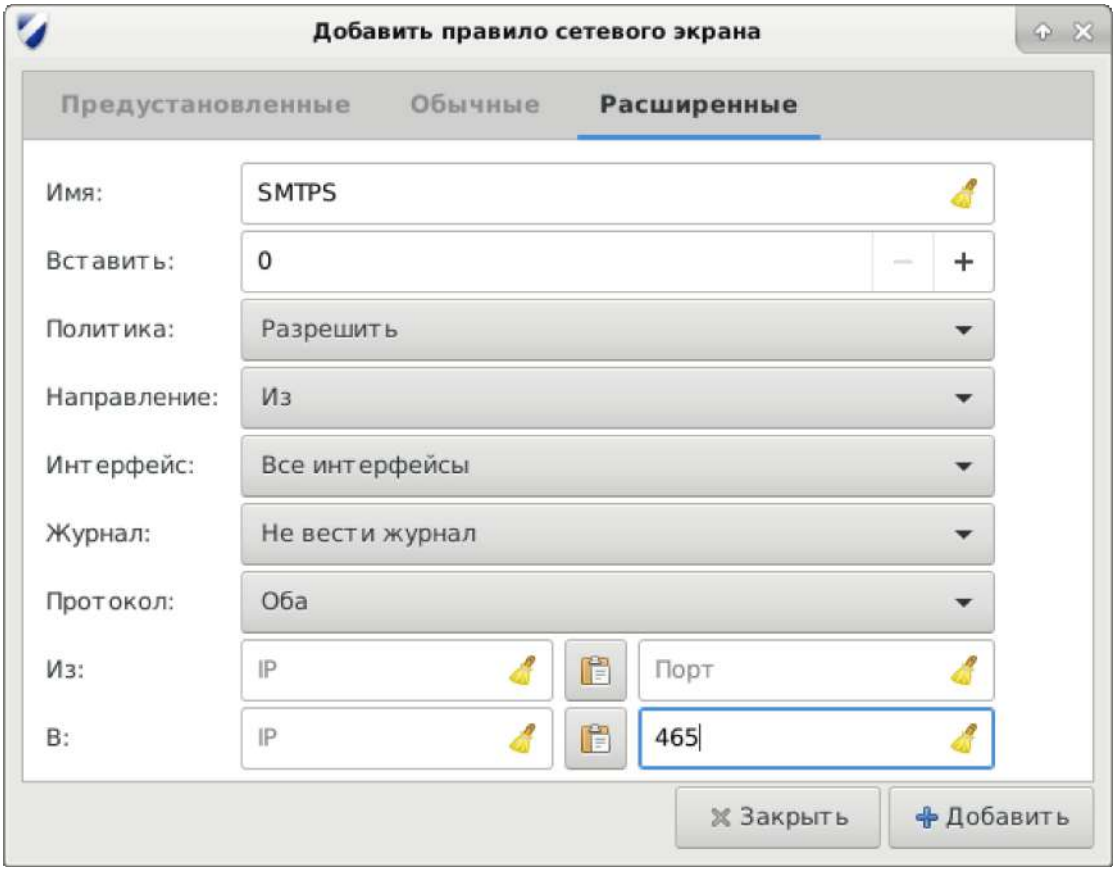
шаге. Также в дальнейшем после каждой Интернет-прогулки я рекомендую откатывать систему к тому состоянию, которое мы настроим. В этом случае, даже если какие-то коварные Интернет-ресурсы оставят в вашей системе нежелательные объекты, помечающие вас, чтобы в дальнейшем идентифицировать, или если в вашу систему попадет вирус, все это будет удалено, после отката системы. Впрочем, до этого этапа еще далеко.

Нажимаем на кнопку «Консоль», после чего запускаем виртуальную машину соответствующей кнопкой. После того, как вход в систему произведен, открываем Synaptic и для начала удалим пакет Telnet. Это инструмент телеметрии, ведущий сбор и отправку разработчикам сведений о производительности системы и возможных ошибках. Таким образом, он является потенциальным средством для слива. Также стоит отметить, что некоторые вирусы, для своей деятельности эксплуатируют именно его.

Теперь можно приступать к установке нового софта. Для начала устанавливаем уже знакомые нам программы Bleachbit и GDebi. В оболочке XFCE изначально недостает некоторых важных функций настройки, таких как настройка времени. Чтобы они появились, нужно установить пакет gnome-system-tools. Также устанавливаем Системный монитор — gnome-system-monitor. Еще необходим файервол — устанавливаем gufw. Еще нам понадобиться Менеджер паролей. Одной из наиболее удобных таких программ является KeePass2. Находим и устанавливаем. Также по-умолчанию нет языковых пакетов для офисных программ и браузера. Поэтому устанавливаем libreoffice-l10n-ru и firefox-esr-l10n-ru. Также устанавливаем curl, поскольку он бывает нужен для подключения новых репозиториев. Еще стоит установить пакет ecj, поскольку некоторые программы для своей работы требуют его. После того, как все нужные программы установлены, необходимо перезагрузить систему, поскольку я замечал, что если этого не сделать после установки программ, система может перестать в дальнейшем корректно запускаться. Также можете установить файловый менеджер caja. Этот файловый менеджер более функциональный чем установленный по-умолчанию Thunar.

После перезагрузки нужно настроить файервол. Настройка полностью аналогична настройке в основной операционной системе. Только здесь для работы с почтой, необходимо добавить еще кое-какие правила. При установке правил, в графе «Направление» указываем «Оба», а в «Приложение», сначала находим и добавляем IMAP, для нешифрованной отправки писем, а затем

IMAPS, для шифрованной. Затем в графе «Направление» ставим «Из», а в «Приложение» находим и добавляем SMTP, для приема писем по нешифрованному каналу. Для того, чтобы добавить правило для получения писем по шифрованному каналу, SMTPS, нажимаем на стрелочку вправо, рядом со строкой поиска. Нас перебрасывает во вкладку «Расширенные». Здесь в «Название» вбиваем «SMTPS», а в самой правой нижней строке «465».



Нажимаем «Добавить». Если пользуетесь какими-то еще отдельными программами, требующими доступ к Интернету, например VoIP, то необходимо указать правила также и для используемых ими портов. Если не знаете, что указывать, то тогда просто не включайте фаервол. Теперь все правила добавлены. Окно можно закрыть.

Теперь пора настроить браузер. В основных настройках все настраиваем также как было показано в основной операционной системе. Но для браузера используемого на постоянной основе для Интернет-серфинга необходимо произвести более глубинные настройки. Эти настройки подразумевают редактирование конфигурации браузера.[6] Ниже будет показана пошаговое

редактирование, чтобы было понятно, какая функция за что отвечает.

В адресной строке вбиваем about:config. В открывшимся сообщении нажимаем «Принять риск и продолжить». Открывается конфигурация браузера. Здесь в строку поиска вбиваем browser.safebrowsing. Под данным маркером находятся функции, которые отвечают за ту самую блокировку опасного и обманывающего содержимого, и как следствие, за слежку Google. Чтобы устранить все потенциальные опасности связанные с этими функциями, везде, где в правой колонке стоит true, его необходимо заменить на false. Для этого, по данной надписи необходимо дважды щелкнуть мышью. Так мы их все отключим.

Затем набираем в строке поиска datareporting.healthreport. Это функции, отвечающие за отправку сообщений о неисправностях и проблемах. Их также следует держать отключенными. Проверяем, чтобы на тамошних пунктах также стояло false.

Следующее devtools.chrome.enabled. Удаленная настройка. Также отключаем.

Также devtools.debugger.remote-enabled. Еще одна функция удаленной настройки. Отключаем.

Следующее toolkit.telemetry. Инструмент телеметрии. Также отключаем все, ставя false.

Проверяем, чтобы отключены были веб-компоненты. Для этого набираем в строке поиска dom.webcomponents.

Следующим проверяем отключен ли DRM-контент media.eme.

Следующее browser.urlbar.merino.enabled. Сервис предоставляющий подсказки при наборе текста.

Следующее browser.startup.homepage_override.mstone. Загружает сведения об изменениях в новой версии браузера. Ставим ignore.

Также отключаем browser.uitor.enabled. Еще один инструмент телеметрии, собирающий информацию о предпочтениях пользователя при работе с браузером.

Следующее dom.event.clipboard. Данная функция позволяет получать доступ к буферу обмена, к примеру с помощью javascript. Отключаем ее.

Далее следует отключить предзагрузку ресурсов network.prefetch-next. Это позволит не загружать ресурсы, которые вам могут быть не нужны, и при этом пытающиеся получить о вас информацию.

В конфигурации могут быть заложены функции взаимодействия (в том числе передачи той или иной информации) с различными ресурсами, с которыми мы, тем не менее, иметь дела не хотим. Именно вычищением ссылок на такие ресурсы мы сейчас и займемся. Эти ссылки находятся также в правой колонке, и выглядят как например https://www.google.com или Google Safe Browsing. Для удаления дважды щелкаем по такой ссылке и очищаем строку в выскочившем окне, затем Enter. Удаляем все ссылки, содержащие слова google, yandex, yahoo, bing, gmail, mail.ru, apple, facebook, youtube, cloudflare.

После этого глубинная настройка браузера закончена. Перезапускаем его.

Браузер стал намного безопаснее, но через него все равно можно получить еще слишком много информации о нас. Для того чтобы закрыть оставшиеся щели, необходимо установить дополнительные расширения.

Если открыть меню и пройти в «Дополнения», то в первой вкладке будет установка новых расширений. Однако, у меня данная функция отказалась корректно работать, поэтому мы будем устанавливать расширения по-другому. Через хранилище дополнений Mozilla.

Вбиваем в адресной строке addons.mozilla.org. На открывшемся сайте в строке поиска набираем http to https. Сайты даже работая по шифрующему протоколу не всегда это шифрование применяют для вашего конкретного соединения. Данное расширение заставляет сайты соединяться именно по шифрующему протоколу, когда это только возможно. Устанавливаем его. Делается это просто по соответствующим кнопкам, поэтому на этом я не буду заострять внимание.

Следующее расширение noscript. Я уже упоминал про javascript. Эта технология позволяющая производить программные сценарии на вашем компьютере. Многие сайты ее используют для повышения своего функционала. Но есть и коварные скрипты, которые стремятся заполучить информацию о вас.[7] С помощью java-скриптов можно узнавать характеристики браузера и операционной системы, а также аппаратного обеспечения. В связи со всем этим java-скрипты следует отключать, когда в них нет необходимости. Данное расширение предназначено именно для этого. Кроме того, с его помощью можно блокировать XSS-атаки.[8] Устанавливаем его.

Затем ищем и устанавливаем ublock. Это блокировщик рекламы. Проблема рекламы не только в том, что она раздражает, через нее также может осуществляться слежка. Многие слышали про adblock. Однако я рекомендую

именно ublock, поскольку, во-первых, он более суров к рекламе, а во-вторых, в нем есть дополнительные полезные функции.

Следующее расширение Privacy Badger. Данное расширение позволяет блокировать жучки, присутствующие на различных сайтах. Довольно гибкое в настройке. Позволяет или вовсе блокировать нежелательные трекеры или запрещать им только оставлять куки, что позволяет достичь баланса между безопасностью и функциональностью сайтов.

Следующее, что ищем Canvas Defender Fingerprinting. Существует такая вещь, как графический отпечаток. Он складывается из многих характеристик вашей системы и железа. Данный отпечаток может быть использован для идентификации вас. Для получения этого отпечатка применяются скрипты. Их блокирует noscript, однако иногда бывает необходимо разрешить какой-то скрипт для повышения функциональности сайта, поскольку многие сайты без включения javascript отображаются некорректно. В этом случае графический отпечаток может стать доступным. Чтобы этого не произошло, отпечаток можно зашумить. Данное расширение как раз и создает шум, который скрывает реальный отпечаток, не позволяя его идентифицировать.

Следующим устанавливаем User Agent Switcher. То, какой браузер и систему вы используйте, тоже может стать идентификатором вас в совокупности с другими средствами меченья. Поэтому данные сведения тоже лучше скрывать. Данное расширение позволяет подменять тип браузера и операционной системы и даже устройство.

Когда расширения установлены, их еще необходимо настроить. Закрываем сайт и нажимаем на значок http to https. В открывшемся поле проверяем, чтобы стояла галочка на «Требовать шифрованные соединения». Можно также поставить галочку на «Блокировать все нешифрованные соединения», но имейте ввиду, что в этом случае, сайты, которые работают без применения шифрования, не будут открываться вовсе.

Нажимаем на значок noscript. В выпавшем поле нажимаем на иконку noscript с перекрещенными инструментами. Открывается окно настроек. Здесь на малой вкладке default убираем все галочки. В этом случае по умолчанию скрипты будут полностью заблокированы. В малой вкладке trusted снимаем галочки с «webgl», «ping», «unrestricted CSS» и «LAN». Данные функции едва ли могут понадобится для какого-то полезного функционала сайтов, зато дадут им больше возможностей собирать о вас информацию, а также облегчат

эксплуатацию уязвимостей, позволяющих осуществлять слежку.[9] Во второй вкладке удаляем все сайты из списка, помечая их как default. Можно оставить только addons.mozilla.org, mozilla.org и noscript.org. Закрываем окно настройки. Подчеркиваю, что при заблокированных скриптах многие сайты могут отображаться некорректно. При необходимости их можно включить целенаправленно, нажав на значок расширения и указав временное или постоянное разрешение на нужном скрипте (обычно, это первый скрипт в списке). Старайтесь не разрешать скрипты, тусующиеся на многих сайтах и собирающих информацию, в частности скрипты от Google и Яндекс. Их можно определить по наличию в названии слов google и yandex, соответственно.

Нажимаем на значок Canvas Defender Fingerprinting. Здесь можно сгенерировать новый шум, нажав на кнопку «Generate new noise». Или отключить зашумление для текущего сайта.

Нажимаем на значок User Agent Switcher. Здесь можно выбрать, на что подменить ваш браузер и операционную систему. В верхней строке можно выбрать устройства, к примеру iphone или смартфон на базе Android. Для удобства я рекомендую подменять устройства только в отдельных случаях. В средней строчке можно выбрать браузер. В нижней строчке, операционную систему. Я рекомендую выбирать Windows, т.к. именно она наиболее популярная, и вам будет проще раствориться, стать неразличимым для Интернет-шпионов. Имейте ввиду, что некоторые сайты, например YouTube, могут не отображаться корректно, если указан тип браузера не соответствующий вашему. Однако, операционную систему, стоит подменять в любом случае.

Также стоит сказать о настройке DNS. Обычно используются DNS-сервера провайдера, и через них запросы идут в незашифрованном виде. Это создает возможности для сторонних наблюдателей подсмотреть эти запросы, а значит узнать, какие ресурсы вы посещаете. А также позволяет подменять передаваемые данные, в результате чего вы можете попасть на поддельный ресурс. Ввиду этого целесообразно использовать шифрованные DNS. В Firefox можно включить функцию использования шифрующего DNS. Для этого в настройках браузера во вкладке «Основные» спускаемся в самый низ и в «Настройки сети» нажимаем «Настроить». В выскочившем окне спускаемся вниз и ставим галочку на «Включить DNS через HTTPS». По-умолчанию, Firefox предлагает использовать серверы от Cloudflare. Но это очередная

крупная компания, пытающаяся собрать сведения о как можно большем количестве пользователей. Поэтому лучше вместо этого сервиса использовать иные. В графе «Используемый провайдер» указываем «Другой». В поле «Другой URL» необходимо указать адрес DNS сервера, поддерживающего технологию шифрования DNS-запросов. Такие сервисы можно посмотреть на странице проекта DNSCrypt.[10] Из представленных сервисов можно выбрать любой, у которого указан протокол DoH. Главное, чтобы это не была крупная корпорация, вроде Google и Cloudflare. Также желательно, чтобы он не вел логирование и цензуру (был помечен как non-logging и т.п.), а также, чтобы поддерживал технологию DNSSEC. Она предназначена для проверки подлинности DNS-запросов, что предотвращает их подмену. Нажимаете на название сервера в левом столбце, выскакивает окно с его данными. Здесь в графе «Addresses» указаны его адрес (прописывается как адрес сайта) и ip (последовательность цифр). Адрес необходимо ввести в поле «Другой URL». Нажимаем «Ok».

После того, как настройка браузера будет произведена, его нужно перезагрузить. Затем можно настроить закладки. Добавить в них те сайты, которые вам нужны. А также добавить в исключения noscript, те скрипты, которые нужно выполнять для корректной работы нужных вам сайтов.

Обращаю внимание, что можно делать резервные копии закладок. С ними вам не придется добавлять их вручную при переустановке браузера или системы.

Также существует возможность сохранить настройки внешнего вида системы и конфигурации программ, чтобы при переустановке не пришлось вручную заново все настраивать. Для этого, в первую очередь, необходимо в файловом менеджере включить отображение скрытых файлов. Обычно эта функция присутствует в разделе «Вид» вверху. После этого в пользовательском каталоге отобразится много папок, названия которых начинаются на точку. Это папки, в которых как раз и хранятся настройки тех или иных программ. Настройки внешнего вида хранятся в папке xfce, которая, в свою очередь, находится в папке config. Ее можно скопировать и в дальнейшем просто перенести ее содержание в аналогичную папку в новой системе. Это сразу настроит панель, апплеты, фон, меню и все остальное, как вы настроили в этой системе. Имейте ввиду, что поскольку она настраивает также и меню с апплетами, необходимо, чтобы при переносе настроек соответствующие

программы уже были установлены в системе. То есть при установке системы сначала, настраиваете репозитории, автовход, обновляетесь и устанавливаете все необходимые программы. И только потом переносите настройки в соответствующую папку. Аналогично можно копировать настройки и различных программ. Например настройки браузера Firefox можно найти также среди скрытых папок в папке mozilla. Перенеся ее содержимое в аналогичную папку в новой системе, вы сразу получите браузер со всеми нужными настройками, в том числе настройками конфигурации, закладками и расширениями. Имейте ввиду, что прежде чем копировать содержимое папки необходимо, чтобы аналогичная папка уже присутствовала, то есть браузер должен быть предварительно хотя бы один раз запущен. Папки с настройками иных программ также имеют названия этих программ. Таким образом в дальнейшем можно настраивать систему.

Еще необходимо сделать замечание относительно звука в виртуальной машине. Громкость звука в виртуалке связана с громкостью в основной операционной системе. Если уровень громкости слишком низкий на высоких показателях или наоборот высокий на низких, просто отрегулируйте громкость в основной системе. Я рекомендую ставить в ней среднюю громкость. Для большинства случаев, это оказывается оптимальным для виртуалки.

Сейчас я хотел бы отдельно остановиться на вопросе о том, каких поисковиков следует избегать, а какими пользоваться.

22 Использование поисковых систем

Ни для кого не секрет, что такие популярные поисковики, как Google, Yandex, Yahoo, Rambler, Mail.ru, Bing и т.д. шпионят за пользователями. Они сохраняют поисковые запросы, привязывают их к ip и другим атрибутам. Ввиду этого, даже в рамках публичной Интернет-активности, пользоваться такими поисковиками не стоит. Чем же воспользоваться заместо этого?

Одним из наиболее развитых и известных на сегодняшний день этичных поисковиков является DuckDuckGo.[11] Он не хранит запросы, не запоминает ваши атрибуты, такие как ip-адрес, не пытается вас пометить при помощи cookie-файлов. Его сервера работают на свободном ПО. Живет он за счет пожертвований и размещения рекламы. Поскольку он не собирает данные пользователей, реклама не является контекстной.[12] Для улучшения релевантности ответов, он использует поисковые базы Bing, Yahoo и Яндекс. С

данными компаниями он партнерствует на условиях предоставления им статистической информации о запросах. То есть, информации о количестве обращений к тем или иным сайтам. При этом, поскольку, как уже не раз было сказано, он не запоминает сами запросы и не собирает данные пользователей, эта информация имеет обезличенный вид. Ввиду партнерства с Яндекс, данный поисковик, среди всех этичных поисковиков, выдает наиболее релевантные ответы для запросов на русском языке. И также его интерфейс имеет русскоязычную версию. В общем, данный поисковик я рекомендую в первую очередь.

Следующий поисковик, который я хочу порекомендовать, StartPage. Это поисковый инструмент от проекта Ixqueck.[13] Существует и поисковик, собственно, Ixqueck. Но всякий раз как я пытался на него зайти, меня неизменно перекидывало на StartPage. Данный поисковик по исполнению очень похож на DuckDuckGo, не запоминает запросы, не собирает данные пользователей, живет за счет пожертвований и рекламы, которая, понятное дело, не контекстная. Отличительной особенностью является то, что он использует поисковую базу Google. Если вы до этого пользовались Google и считайте, что его ответы наиболее релевантные, можете использовать StartPage в качестве основного своего поисковика. Из минусов можно отметить отсутствие русского интерфейса. Но, мне кажется, что для поисковика это не критично. В общем, данный поисковик, также всецело рекомендую.

Еще при разговоре об этичных поисковиках часто упоминают Disconnect Search. Однако при моих попытках, что-либо найти через него, хоть с использованием онлайн-версии, хоть расширения для Firefox, он неизменно перебрасывал меня на DuckDuckGo.

Существуют и другие этичные поисковики, однако на сегодняшний день они недостаточно развиты.

В статьях, размещенных в Интернете, где рассказывается об этичных поисковиках, часто упоминается, что их ответы на запросы не такие релевантные, как у обычных, шпионящих и торгующих информацией. Мои личные эксперименты показали, что ответы выдаваемые Яндекс ничуть не релевантнее ответов, выдаваемых DuckDuckGo, а ответы Google, не релевантнее ответов StartPage. Картина ответов у Яндекс и DuckDuckGo практически идентична, что не удивительно, поскольку, как уже упоминалось, DuckDuckGo сотрудничает с Яндекс. Такая же ситуация с Google и StartPage.

Так что не видитесь на клевету.

С поисковиками разобрались.

Нужно еще обеспечить безопасность паролей для наших аккаунтов.

23 Работа с KeePass2

Сложные пароли и разные для разных аккаунтов, это гарантия безопасности. Однако даже один по-настоящему сложный пароль запомнить крайне трудно, что уж говорить о ситуации, когда у вас десятки аккаунтов. Именно для решения этой проблемы были придуманы менеджеры паролей. Они позволяют создавать зашифрованную базу паролей прямо в операционной системе, где эти пароли привязаны к логинам и сайтам, чтобы легко было ориентироваться. Благодаря тому, что хранится эта база паролей, как было сказано, в зашифрованном виде, она надежно защищена даже в случае проникновения в систему злоумышленника.

Программа KeePass2 имеет все необходимые инструменты для работы с паролями. С помощью нее можно создавать базы данных, где будут храниться, разбитые по категориям сведения об аккаунтах. Эти сведения могут включать название Интернет-ресурса, на котором заведен аккаунт, логин, пароль и комментарии к ним. С помощью данной программы можно генерировать сложные пароли.

Переходим непосредственно к работе с программой. Идем в Меню, категория «Инструменты» и нажимаем KeePass2. Открывается окно программы. Первым делом нужно создать файл базы данных. Для этого щелкаем по значку файла слева сверху, придумываем и забиваем название и пароль для входа в эту базу. Этот пароль, соответственно, придется вводить каждый раз, когда этот файл нужно будет открыть. Я рекомендую, чтобы не путаться, использовать тот же пароль, что и для root и пользователя. Напоминаю, что в рамках одной системы использовать один пароль для разных инструментов приемлемо.

Когда файл создан, можно приступать к созданию категорий для аккаунтов. Они располагаются в левом поле. К примеру, можно создать одну категорию для сайтов гос. услуг, другую для электронных почт, третью для соц. сетей, четвертую для Интернет-магазинов, в которой можно создать несколько подкатегорий для магазинов разных товаров, допустим, если вы пользуйтесь несколькими книжными Интернет-магазинами, парой электронных, и парой магазинов одежды. Чтобы создать категорию, нужно нажать правой кнопкой

мыши по полю и выбрать «Добавить». После чего вбить название категории, можно выбрать значок. Чтобы добавить подкатегорию, щелкаем правой кнопкой мыши по категории и нажимаем «Добавить». Удалить категорию можно щелкнув по ней также правой кнопкой мыши и нажав «Удалить». После этого категория переместиться в отдельную категорию «Корзина». Эту категорию также можно удалить.

В правом поле, создаются записи аккаунтов. Чтобы добавить запись, нужно нажать правой кнопкой мыши по полю и затем нажать «Добавить». Появится окно, в котором наверху можно забить название аккаунта, например имя Интернет-ресурса, на котором он создан. Под ним поле для логина. Следующие два поля для пароля. Вы можете придумать и забить пароль сами, а можете воспользоваться генератором паролей. Для этого щелкните по кнопке справа от ввода пароля. В выскочившем поле можно выбрать вес пароля. Сила пароля зависит не только от его длинны, но и от сложности подбора, понятное дело, что если пароль состоит из словарных слов, подобрать его легко, сложнее всего подбираются пароли, состоящие из рандомного набора символов. Именно такие пароли и генерирует эта функция, случайный набор маленьких и заглавных букв, цифр, в настройках можно добавить пунктуационные знаки. Пароли в 40 бит небольшие и не слишком сильные. 128 бит, весьма стойкие, и именно их я рекомендую использовать для большинства случаев. 256 бит, неимоверно стойкие, но вместе с тем и непомерно длинные. Также следует отметить, что объем пароля не всегда точно соответствует заданному, обычно имеет место погрешность в пределах 10 бит. Кнопка рядом с повтором пароля позволяет посмотреть, что собой задаваемый пароль представляет. Также можете добавить комментарии к записи. Когда все забито, нажимаем «Ok». Запись создана.

Подобным образом создаем записи для всех своих аккаунтов. Теперь для того, чтобы войти в какой-то аккаунт, открывайте эту базу паролей, находите запись с нужным аккаунтом, щелкайте по этой записи правой кнопкой мыши и нажимайте «Copy Login» для копирования логина в буфер обмена, после чего вставляйте логин в поле, собственно, логина на нужном Интернет-ресурсе. Затем щелкайте еще раз правой кнопкой мыши по записи и нажимайте «Copy Password», и вставляйте пароль в нужное поле. Важно, после того, как логин или пароль будут скопированы в буфер обмена, они удаляться из него через пятнадцать секунд. Это сделано для того, чтобы снизить риск их перехвата, в случае получения злоумышленником доступа к вашему буферу обмена.

Теперь во всех аккаунтах у нас разные сложные пароли, при этом запоминать нужно только один, для входа в базу паролей. Безопасность соблюдена и на этом уровне.

24 Выбор и установка дополнительного браузера

Иногда может возникнуть необходимость иметь под рукой несколько браузеров. К примеру может сложиться ситуация, что из-за обилия функций блокирования слежения может не открываться какой-то сайт. Редко, но случается, что невозможно определить, что именно в браузере не дает сайту нормально отображаться. Разрешение всех скриптов, трекеров, рекламы, сторонних cookie-файлов, отключение принудительного шифрования и подмены типа браузера и ОС, не дают эффекта, сайт или некоторые его компоненты, все равно не отображаются (такое наблюдается, например, с одним из видов капчи — reCapcha). Конечно, лучше такие сайты просто не посещать, но иногда это может быть необходимо. В этом случае, выходом может стать использование браузера, не имеющего столь радикального блокирующего функционала.

В репозиториях Devuan немало браузеров, однако почти все они достаточно блеклые и не поддерживающие весь массив современного функционала сайтов, поэтому нормально работать через них невозможно. Помимо Firefox, одним из немногих полнофункциональных, по современным меркам, браузеров в репозиториях Devuan является Chromium.[1] В отличие от своего проприетарного собрата — Google Chrome — Chromium распространяется под свободной лицензией и в целом соответствует критериям свободного ПО. Однако, с ним существуют проблемы. Несмотря на то, что в нем вы можете отключить большую часть неприятных настроек, некоторые предустановки вы не сможете исправить. К примеру, в качестве поисковой системы по-умолчанию на выбор предлагается только четыре поисковика, Google, Yahoo, Bing и Яндекс. Никакие другие поисковики, например DuckDuckGo, вы в качестве поисковой системы по-умолчанию установить не сможете. Кстати, поисковик Google нельзя также удалить из браузера.

Некоторым известен в качестве якобы свободной альтернативы Google Chrome браузер SRWare Iron.[2] Данный браузер основан на Chromium. По заявлению разработчика, помимо отсутствия следящего функционала, он имеет настройки, заточенные на приватность, которых нет в Chromium. Однако, этот

браузер рекомендовать также не приходится. Во-первых, свободный он только на словах разработчика, поскольку исходный код выставлялся только для первых версий. Исходников же последних нет ни на официальном сайте, ни где бы то ни было еще. Во-вторых, в настройках, хоть и можно, в отличии от Chromium, указать в качестве поисковой системы по умолчанию ту, которую вы сами хотите и удалить предустановленные, в том числе и Google, однако, при попытке осуществить поиск, он будет произведен в Яндекс, даже если его плагин удалить. Это происходит в русскоязычном варианте браузера, скачанного с официального сайта. Мне не известно, как обстоят дела с этим браузером на других языках. Как это происходит и почему, непонятно. Эта проблема кочует из версии в версию, и похоже, никто не собирается ее устранять.[3] В общем, браузер еще менее приглядный для использования чем Chromium.

Существует еще один браузер, основанный на Chromium из которого выпилена интеграция с Google. И в отличии от упомянутого выше браузера, он действительно свободный. Это браузер Ungoogled Chromium.[4] К сожалению, он не всегда работает корректно, в него невозможно установить расширения. Сейчас существует тенденция создавать Интернет-ресурсы, открывающиеся только в определенном браузере, поэтому может возникнуть необходимость воспользоваться чем-то, основанном именно на Chromium. Увы, Ungoogled Chromium часто также такие сайты не открывает, потому может возникнуть необходимость воспользоваться именно браузером Chromium.

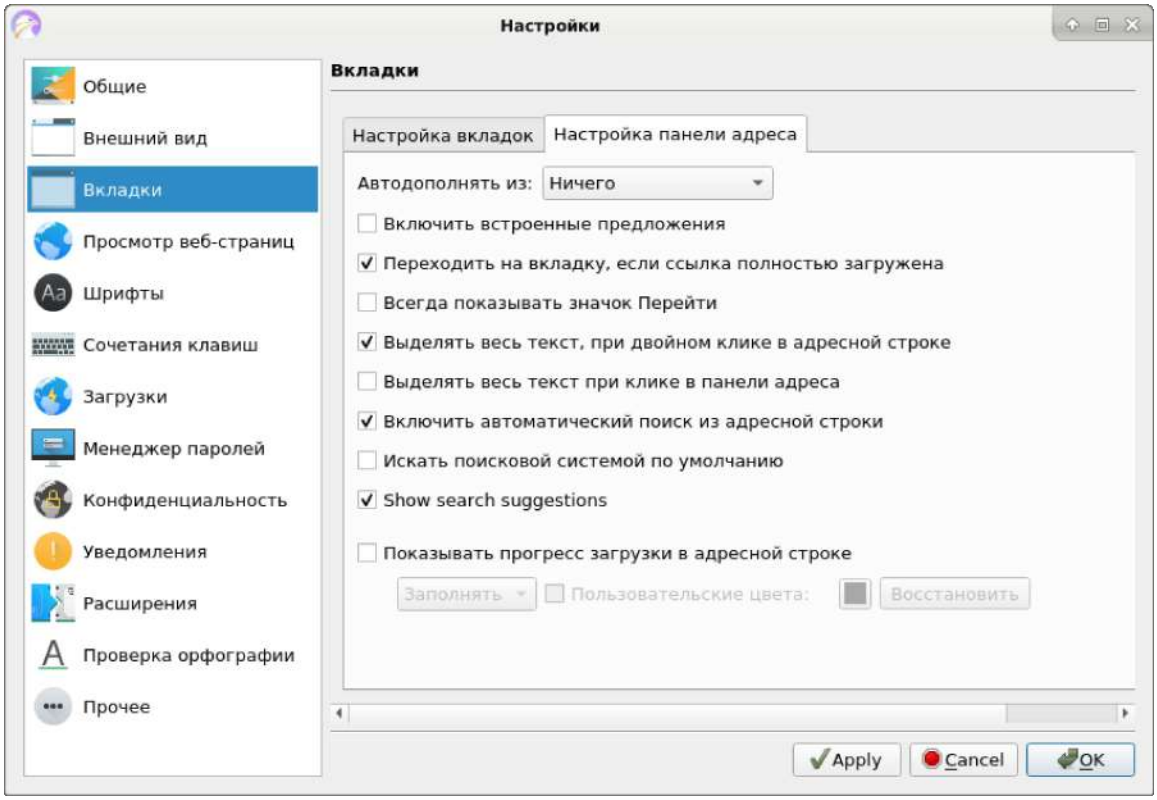
Необходимо предупредить, что при его запуске порой вылезает сообщение с предложением задать пароль. Его осуществляет программа gnome-keyring. Ее можно удалить, но она может быть необходима для некоторых других программ, например для почтового клиента. Чтобы не вводить пароль при каждом запуске необходимо при первом выскакивании такого предложения, ничего не вводя в поля ввода нажать «Продолжить». Именно «Продолжить», а не «Отмена», поскольку в этом случае сообщение будет вылезать постоянно. Далее выскочит предупреждение, что пароли будут храниться в незашифрованном виде. Нажимаем «Продолжить». После этого данное окно больше выскакивать не будет.

Впрочем, более приглядной альтернативой может стать браузер Vivaldi.[5] Его дизайн заметно отличается от классического Chromium. Основная функциональная часть браузера во многом идентична Chromium, хотя некоторые отличия имеются.[6] Стоит отметить, что разработчики предприняли

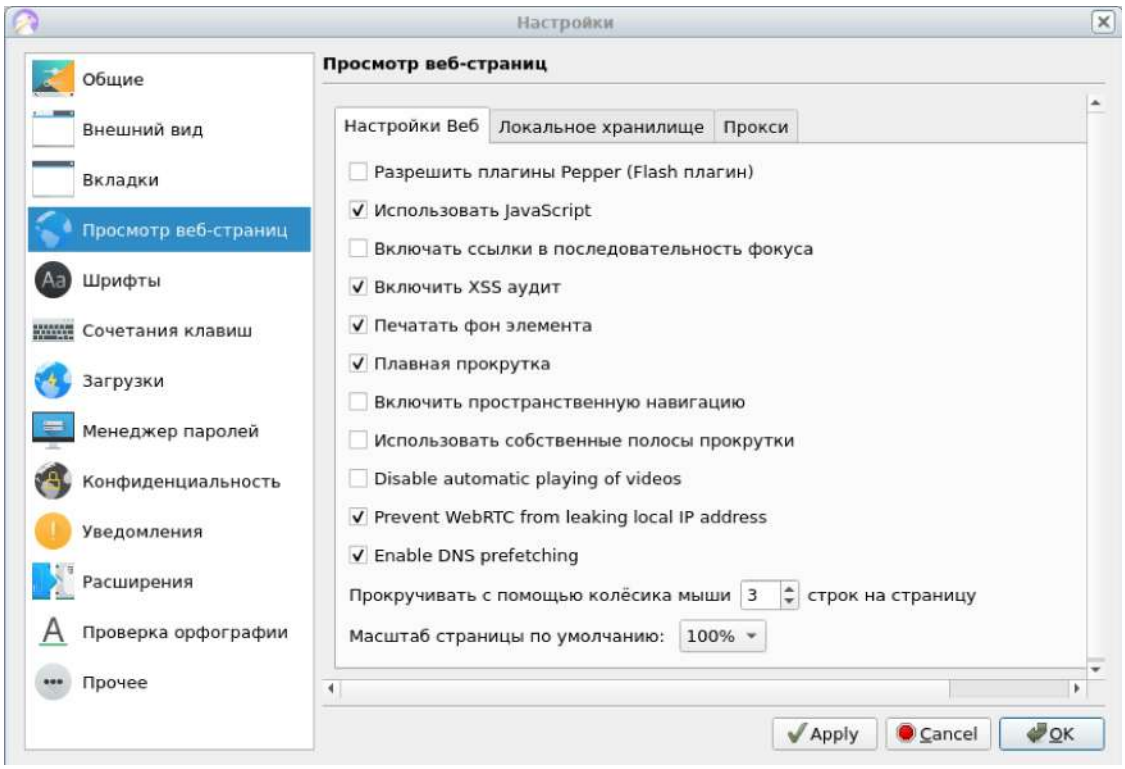
некоторые меры по противодействию слежки Google,[7] из-за чего эта корпорация пыталась даже препятствовать распространению Vivaldi.[8] Функциональная часть браузера, как и Chromium, с которого она взята, находится под свободной лицензией. А вот оформление не является свободным. Таким образом, Vivaldi не является полноценно свободным браузером. Однако, при этом все оформление написано на обычном HTML и CSS, и к его тексту можно получить доступ. То есть, хотя вы не имеете права копаться в исходном коде данных компонентов браузера, вы фактически можете это делать. Сами разработчики Vivaldi заявляют, что не осуществляют преследование пользователей за такие действия. Единственное против чего они выступают категорически против, это чтобы данный их код использовался в коммерческих целях. Если свести всю их аргументацию к одной фразе — они так борются с конкуренцией.[9] Этот момент не очень понятный, — если они не хотели только чтобы их код использовали в коммерческих целях, то почему использовали лицензию, запрещающую вообще какой-либо доступ к исходному коду? Почему не взяли ту, которая просто налагает ограничения на коммерческое использование? Этот момент совершенно не понятный. Также необходимо отметить, что Vivaldi собирает некоторые пользовательские данные. При его установке создается id конкретной установленной копии, и каждые сутки на сервера разработчиков отсылается информация, помеченная этим id, об архитектуре системы, времени последнего сообщения с сервером и ip-адрес. У ip удаляется последний октет, что не позволяет установить, кому конкретно он принадлежит, а можно узнать лишь страну, в которой пользователь производит подключение. Никакая другая информация не собирается.[10] Потому он выглядит более предпочтительно, чем классический Chromium. Тем не менее, данный браузер я рекомендую устанавливать только при крайней необходимости.

К счастью, в репозиториях Devuan есть еще один полнофункциональный браузер. Это браузер Falkon.[11] Он удобен и прост в настройке, и именно его я рекомендую в качестве дополнительного браузера.

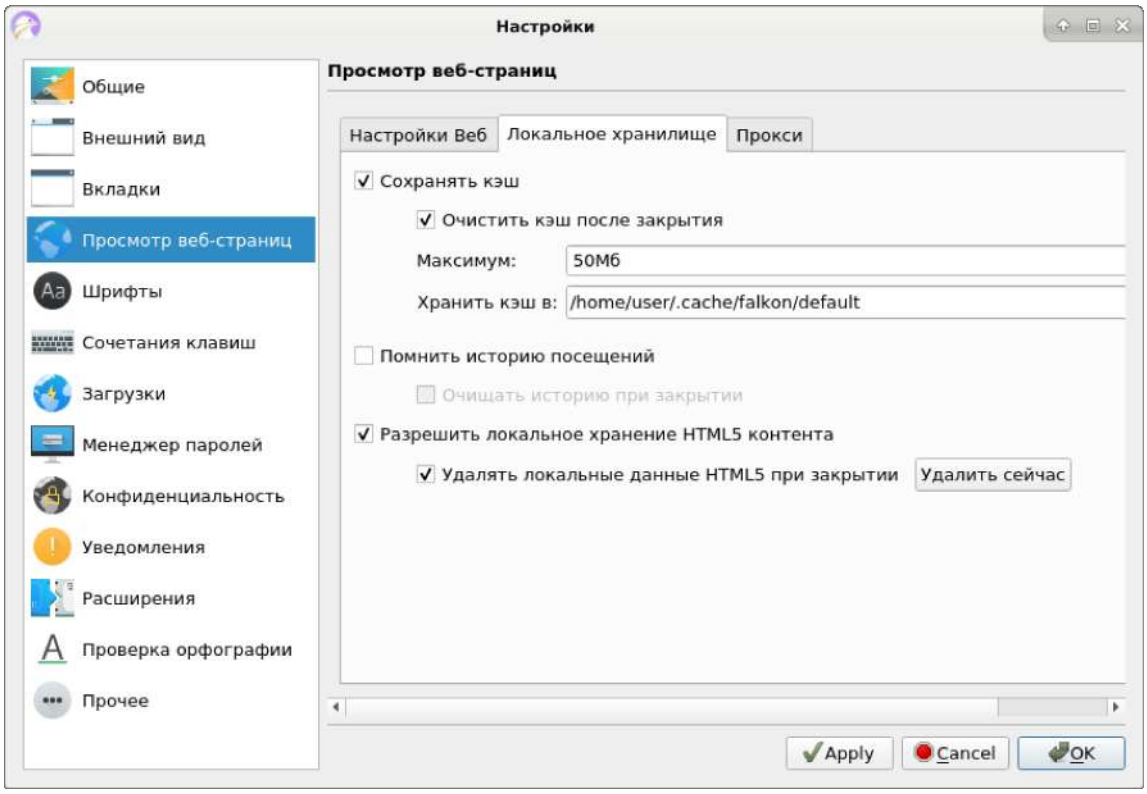
После установки Falkon, открываем его, нажимаем кнопку справа сверху и идем в «Настройки». Идем во «Вкладки» и там в «Настройка панели адреса». Здесь в графе «Автодополнять из» ставим «Ничего». Снимаем галочку с «Включить встроенные предложения».



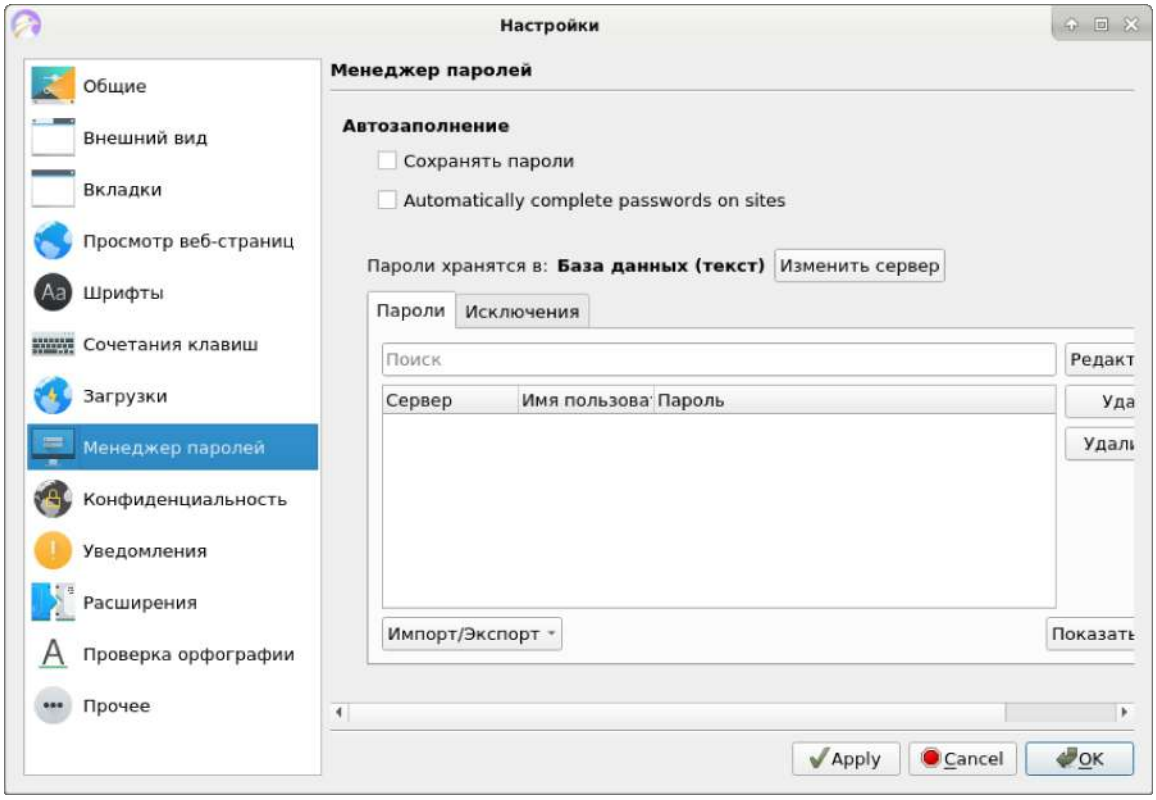
Затем идем в «Просмотр веб-страниц». Здесь во вкладке «Настройка Веб» снимаем галочку с «Разрешать плагины Pepper (Flash плагин)». И ставим галочку на «Включить XSS аудит».



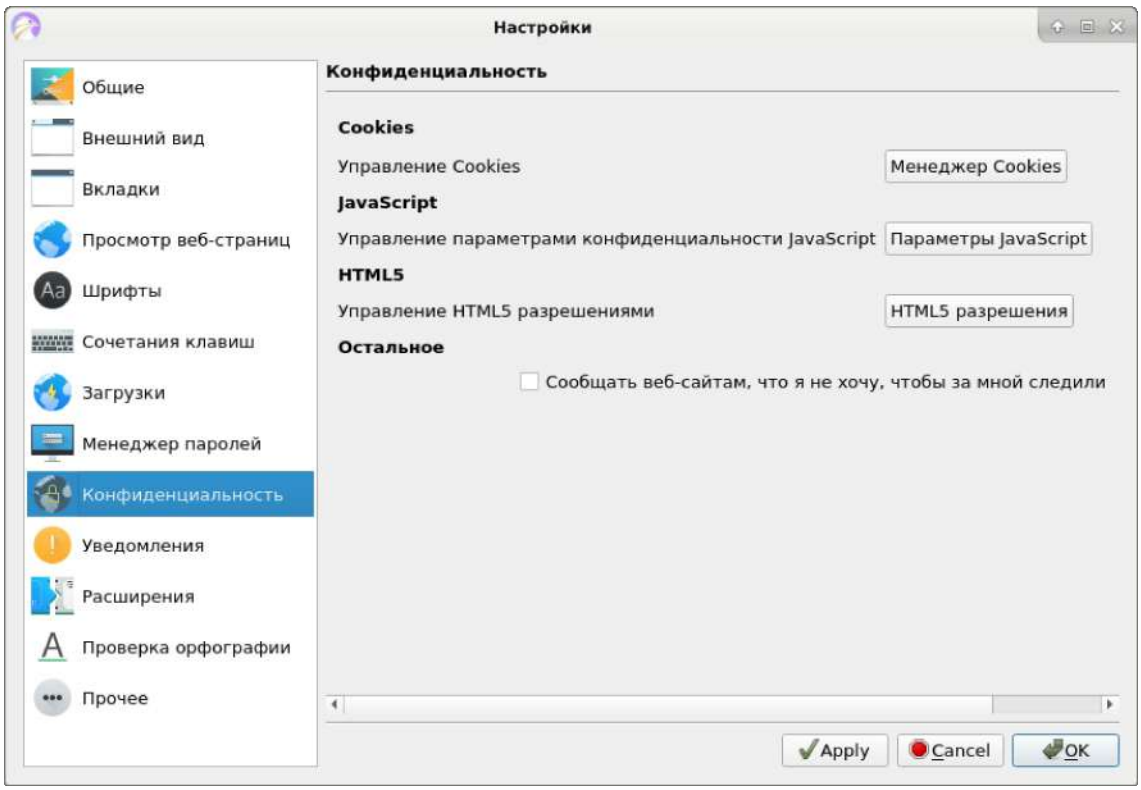
Переходим во вкладку «Локальное хранилище». Ставим галочки на «Сохранять кэш» и «Очищать кэш после закрытия». Снимаем галочку с «Помнить историю посещений». Локальное хранение HTML5 контента можно оставить разрешенным, но нужно поставить галочку на «Удалять локальные данные HTML5 при закрытии».



Идем в «Менеджер паролей» и снимаем галочки с функций сохранения паролей.

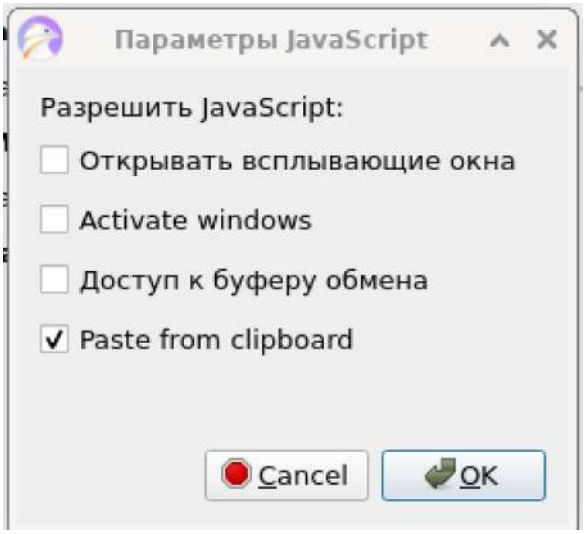


Идем в «Конфиденциальность» и нажимаем на кнопку «Менеджер cookie».



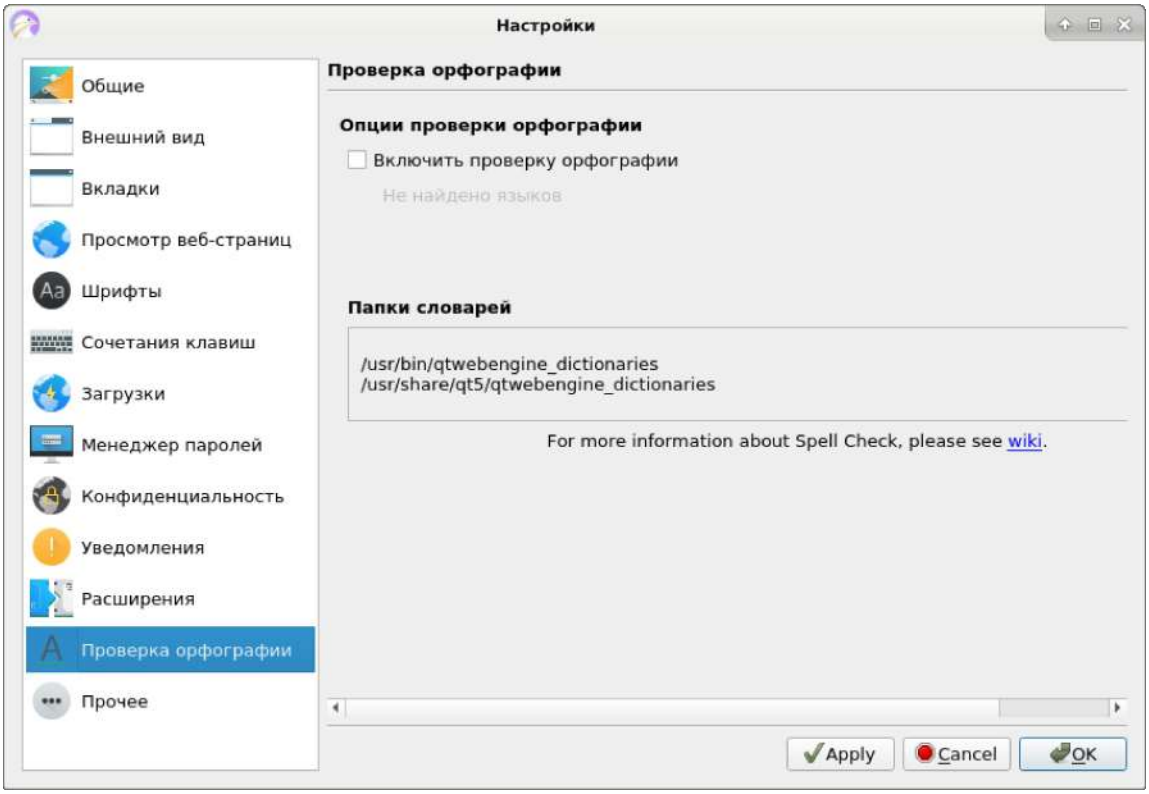
В открывшемся окне идем во вкладку «Настройки» и ставим галочки на «Сохранять cookie» и «Удалять cookie после закрытия». Нажимаем «Close».

Во вкладке «JavaScript» снимаем галочку с пункта «Доступ к буферу обмена».

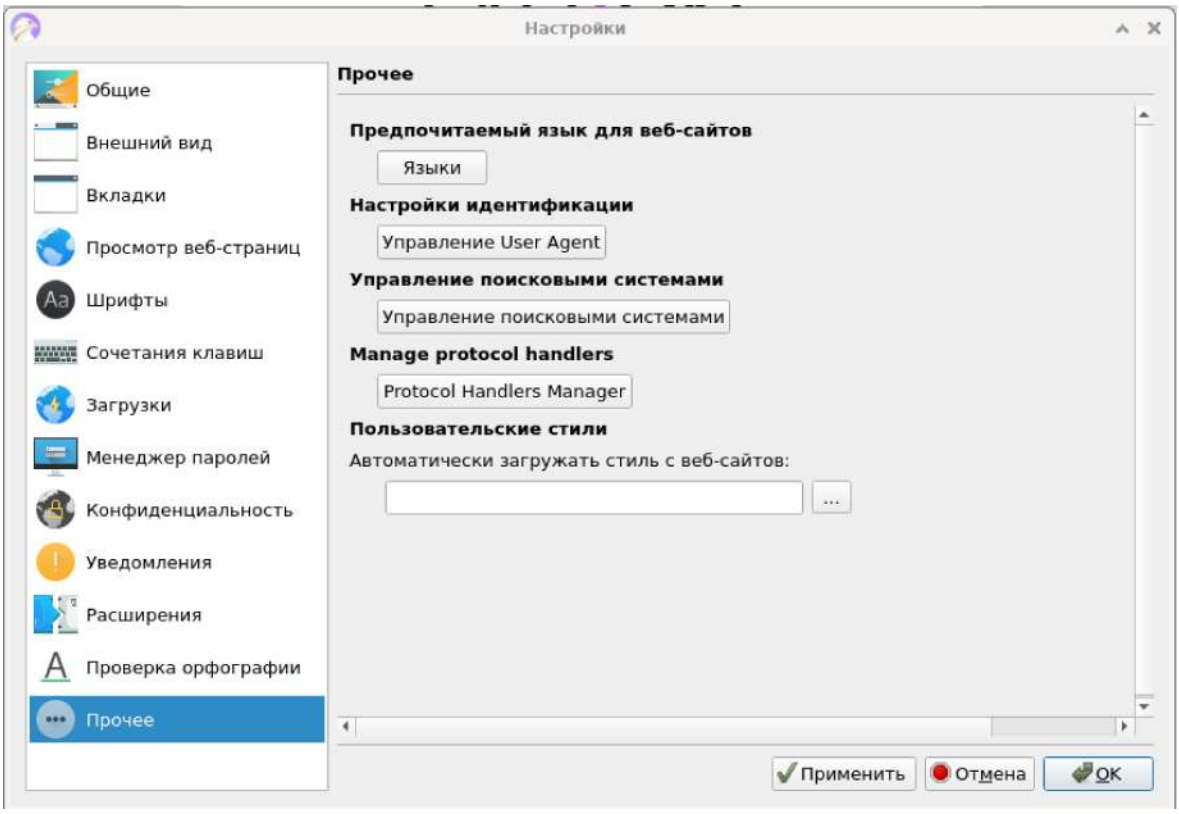


В «Расширения» можно оставить включенным Adblock. По моим наблюдениям, это не препятствует функционалу сайтов.

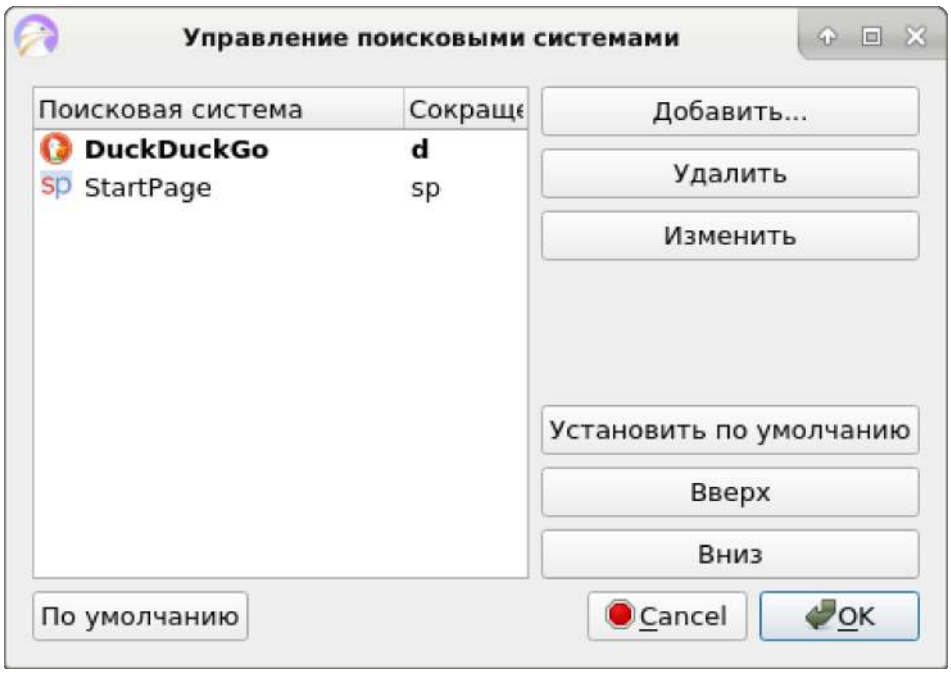
В «Проверка орфографии» проверяем, чтобы эта проверка была отключена.



В «Прочее» есть «Управление User Agent» для подмены типа браузера и операционной системы. Однако, я не рекомендую его использовать, поскольку некоторые сайты могут начать работать некорректно, а мы устанавливаем данный браузер именно для открытия сайтов с их полным функционалом. При этом поисковые системы лучше все-таки настроить. Нажимаем на кнопку «Управление поисковыми системами».



В выскочившем окне удаляем Google. Для этого выделяем его и нажимаем на кнопку «Удалить» справа. Также можно удалить Википедию, поскольку все равно здесь установлена английская версия. Нажимаем «Ok».



Теперь нажимаем внизу справа кнопку «Apply», а затем там же кнопку «Ok».

На этом настройка браузера Falkon закончена. Теперь можете установить необходимые вам вкладки и произвести другие косметические настройки.

25 Клиенты электронной почты

При использовании веб-версии электронной почты существует несколько проблем. Во-первых, в абсолютном большинстве случаев необходима активация java-скриптов, чтобы почта функционировала. Я уже писал о том, какие проблемы для безопасности создают java-скрипты. В случае электронной почты, с помощью них можно детализировать профиль, который создает на вас ее поставщик. Например, узнать ваш конкретный уровень грамотности, анализируя частоту и систематику орфографических и пунктуационных ошибок, а также время затраченное на их исправление. Выявить стилистические закономерности, а также время затрачиваемое на формулировку предложений, анализируя процесс написания писем и т.д. Также существуют маяки электронной почты, представляющие собой крошечные изображения, встроенные в письма с уникальными идентификаторами в URL, сообщающие серверу почты, с которой было отправлено письмо, время, когда оно было прочитано, даже если оно было отправлено на сервис другого поставщика, а также другую информацию, такую, как ip-адрес получателя.[12] Некоторые проблемы связаны с удобством. Например уже полученные и отправленные

письма нельзя просматривать без подключения к Интернету. Затруднено резервное копирование писем. А также почти невозможно или крайне затруднительно управлять сразу несколькими учетными записями.

Эти проблемы помогают решить клиенты электронной почты. При использовании их, на вашем компьютере не выполняются вредоносные java-скрипты, а при грамотной настройке можно защититься от маячков. Нет объявлений из Интернета, таких как реклама. Электронные письма могут храниться непосредственно на компьютере, что позволяет просматривать, составлять и изменять их без подключения к Интернету. Это также облегчает их резервное копирование. Можно работать одновременно с несколькими учетными записями электронной почты. А также имеются другие преимущества.

Из существующих клиентов электронной почты весьма приглядным выглядит Sylpheed.[13] Но, к сожалению, в нем отсутствует некоторый функционал, например HTML. Поэтому многим он может не подойти. К счастью, существуют более функциональные решения.

Для начала хотелось бы сказать об уже упоминавшемся клиенте Icedove, по-умолчанию установленном в Trisquel. Это будет скорее отступление, нежели рекомендация для использования. Клиент, установленный в основной операционной системе, можно использовать для выше оговоренных задач — оффлайн работы с письмами. Однако вариантом для полноценной работы с почтой он вряд ли станет. Дело в том, что репозитории Trisquel одно из очень немногих мест, где данный клиент еще можно достать.

История Icedove такова. Когда-то проекту Debian нужны были браузер и почтовый клиент, для включения в свой дистрибутив. Были выбраны браузер Firefox и почтовый клиент Thunderbird, которые разрабатывались компанией Mozilla. Однако возникла проблема. Политика Mozilla в отношении товарных знаков ограничивала свободу распространения их программ. Оно позволялось лишь на безвозмездных условиях, что делало их программное обеспечение в целом несвободным.[14] Выходом для проекта Debian стало создание своих браузера, на основе Firefox, и почтового клиента, на основе Thunderbird. Так появились браузер Iceweasel и клиент электронной почты Icedove. Помимо того, что эти программы имели свои товарные знаки, в них также были слегка изменены некоторые настройки безопасности. В остальном же это были все те же Firefox и Thunderbird. Однако, с выходом девятой версии Debian, его

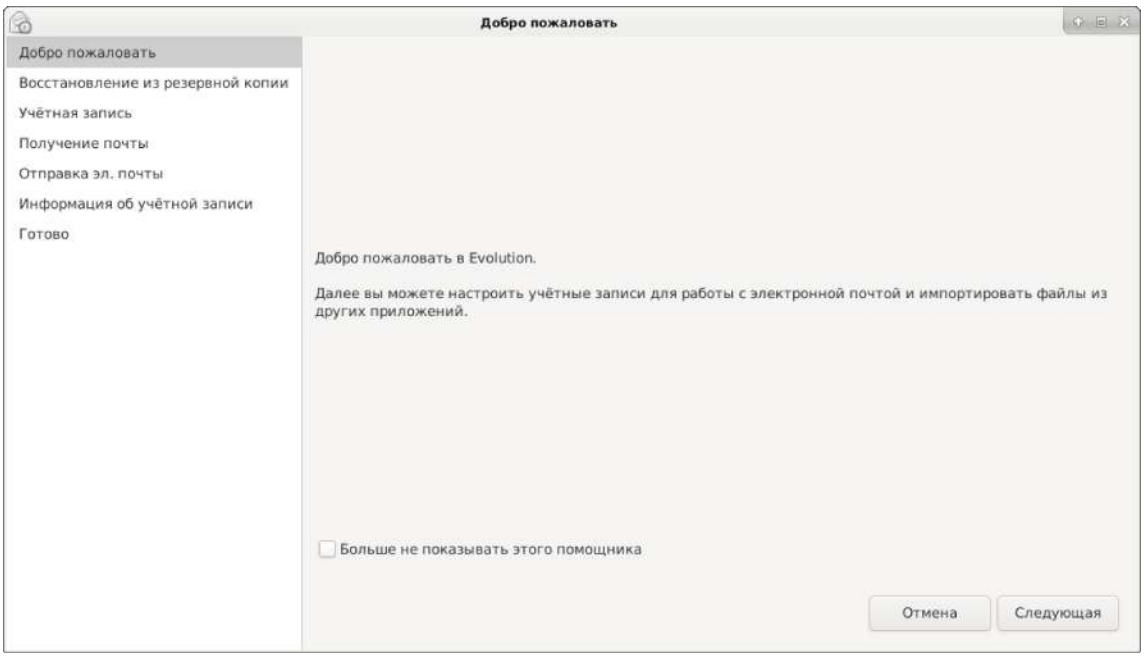
разработчики все-таки договорились с компанией Mozilla. После этого браузер Firefox и клиент электронный почты Thunderbird появились в репозиториях Debian, а Iceweasel и Icedove из них исчезли.[15] А вместе с этим и из репозиториев дистрибутивов, основанных на Debian. Прекратилась и их поддержка. Однако с выходом восьмой версии Trisquel, клиент Icedove появился в его репозиториях и даже был установлен в нем по-умолчанию. И обновления этого клиента продолжают приходить, а значит, ведется его поддержка.

Если говорить о самом клиенте, то он, как и Thunderbird, на котором он основан, имеет широчайший набор функций, крайне приятный и удобный интерфейс. Кроме того Icedove, в отличии от Thunderbird не предлагает включать в себя несвободные дополнения, что выгодно отличает его от последнего. Видимо именно ввиду наличия функциональности и удобства Thunderbird и при этом отсутствия поддержки несвободных дополнений, команда Trisquel решила включить его в свой дистрибутив. Однако как я и сказал, рекомендовать его в качестве клиента для работы с почтой не приходится. В репозиториях Devuan он отсутствует, и вам вряд ли удастся найти его в виде отдельного пакета в Интернете.

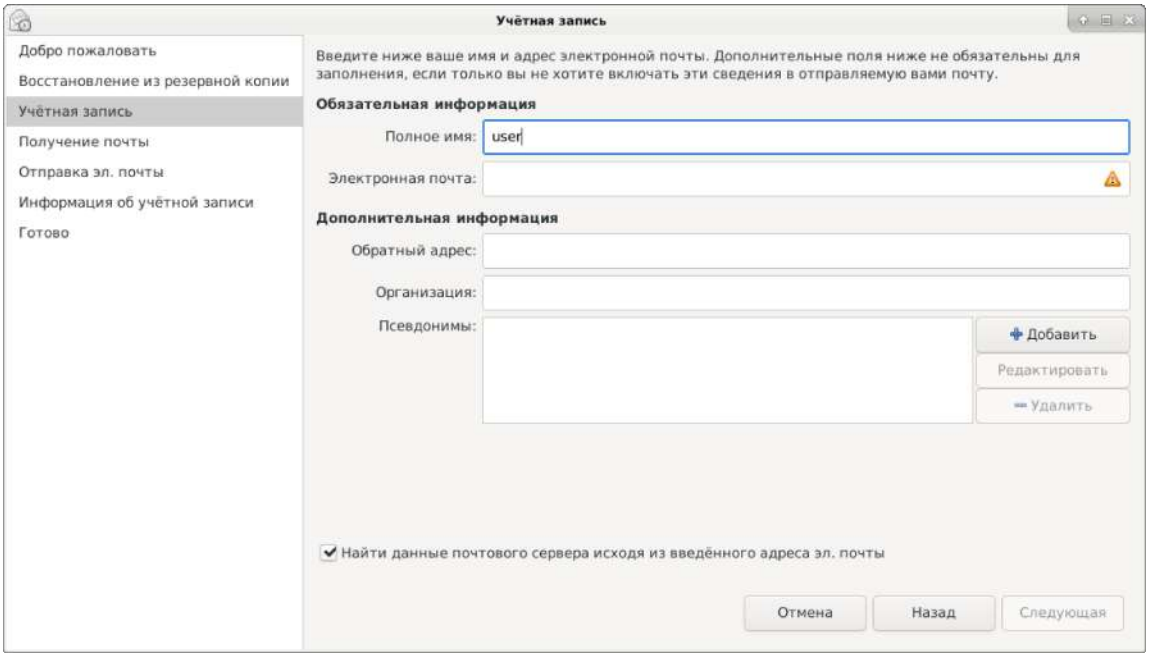
Необходимо сказать о, собственно, клиенте Thunderbird,[16] поскольку он невероятно популярен, и многие склонны вообще считать его лучшим клиентом электронной почты. Он действительно необычайно функционален и удобен, его легко установить из репозиториев Devuan. Но я его не рекомендую. Как было сказано, он включает в себя поддержку несвободных дополнений. Конечно, если вы не будите целенаправленно их устанавливать, несвободных компонентов в нем и не будет, и он останется полностью свободным. С учетом этого, а также отсутствия других минусов, его можно было бы порекомендовать, однако существует полностью свободная альтернатива.

Если вам нужен мощный инструмент с обилием функций, могу порекомендовать клиент Evolution.[17] Он не уступает по функционалу Thunderbird и отличается от него только дизайном и, в некоторых моментах, исполнением этого самого функционала.

После установки идем в Меню, категория «Офис», и нажимаем «Evolution». Выскочит окно с приветствием. Нажимаем внизу справа кнопку «Следующая».

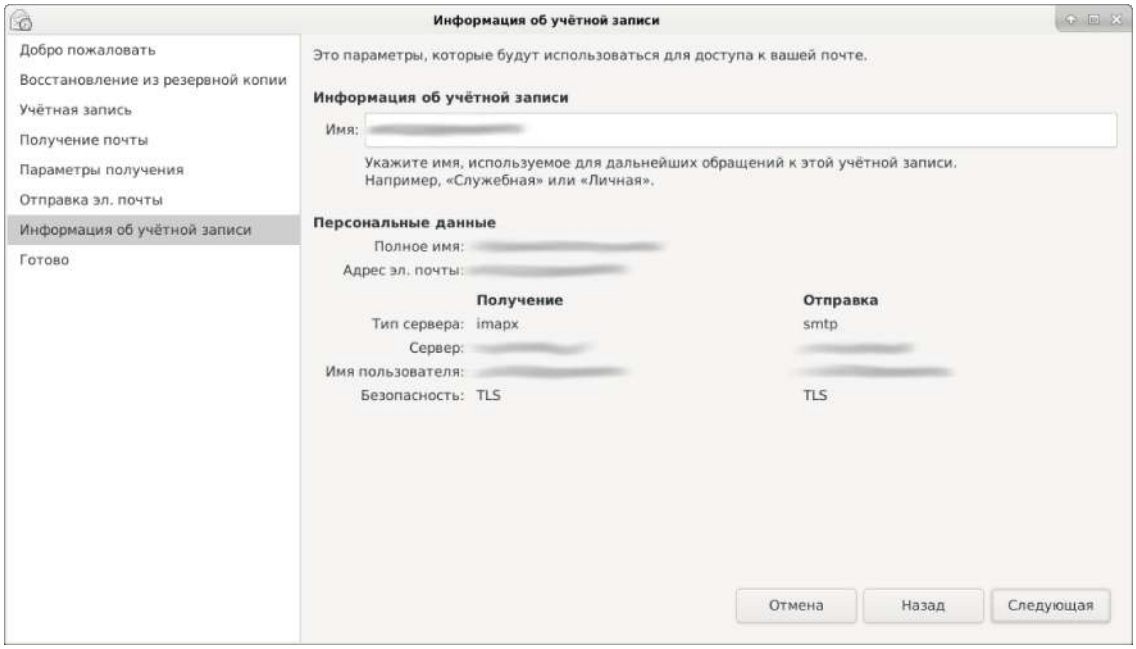


Теперь в графе «Полное имя» набирайте то имя, под которым вы регистрировали почту. В графе «Электронная почта» набираем свой электронный адрес. Если хотите, можете заполнить дополнительную информацию. Проверяем, чтобы внизу стояла галочка на «Найти данные почтового сервера исходя из введенного адреса эл. почты» и нажимаем кнопку «Следующая».



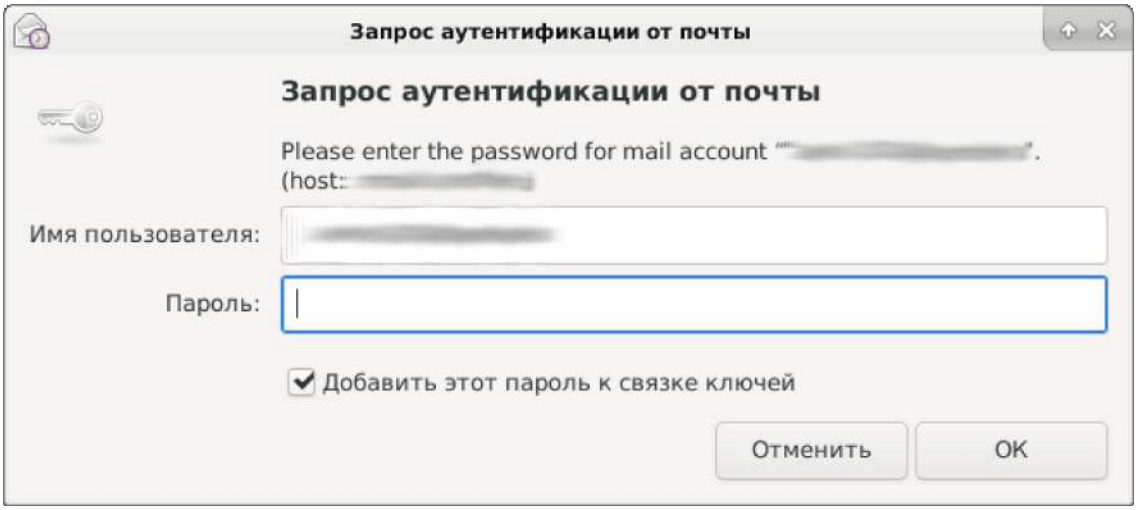
Если все верно, то данные сервера автоматически импортируются в клиент, и появится страница, где будут указаны данные получения и отправки

электронных писем с типом и именем сервера, вашим адресом электронной почты и типом шифрования (обычно TLS).



Нажимаем «Следующая». Теперь «Готово».

Выскочит окно с запросом аутентификации от почты. В графе «Имя пользователя» вводим свой адрес электронной почты, а в «Пароль», соответственно пароль. Проверяем, чтобы стояла галочка на «Добавить этот пароль к связке ключей» и нажимаем «Ok».



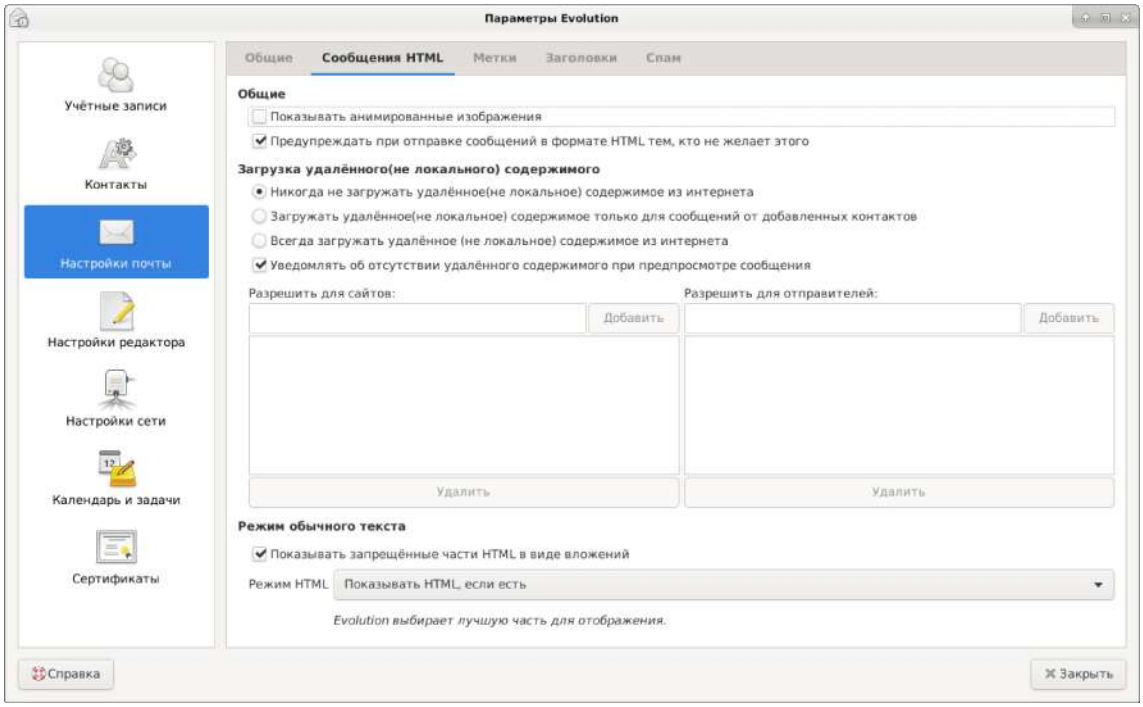
После этого выскочит окно в котором будет предложено создать второй пароль для связки ключей. Если его указать, то это дополнительным образом

зашифрует пароли от почты, хранящиеся на устройстве. Но его необходимо будет вводить каждый раз при запуске клиента. Если хотите дополнительно обезопаситься, то можете его указать. Если же не хотите каждый раз вводить пароль, то тогда, ничего не вводя в поля ввода, нажмите «Продолжить». Выскочит предупреждение, что пароли будут храниться в незашифрованном виде. Нажимаем «Продолжить». Теперь не придется вводить пароль при каждом запуске клиента.

После того, как Evolution развернется, нажимаем вверху справа кнопку «Правка» и выбираем «Параметры». Evolution не только клиент электронной почты, это еще и мощная программа календаря, в котором можно создавать заметки и отмечать события. Управление всеми этими функциями осуществляется во вкладке «Календарь и задачи». Здесь все настраивайте под свои потребности.

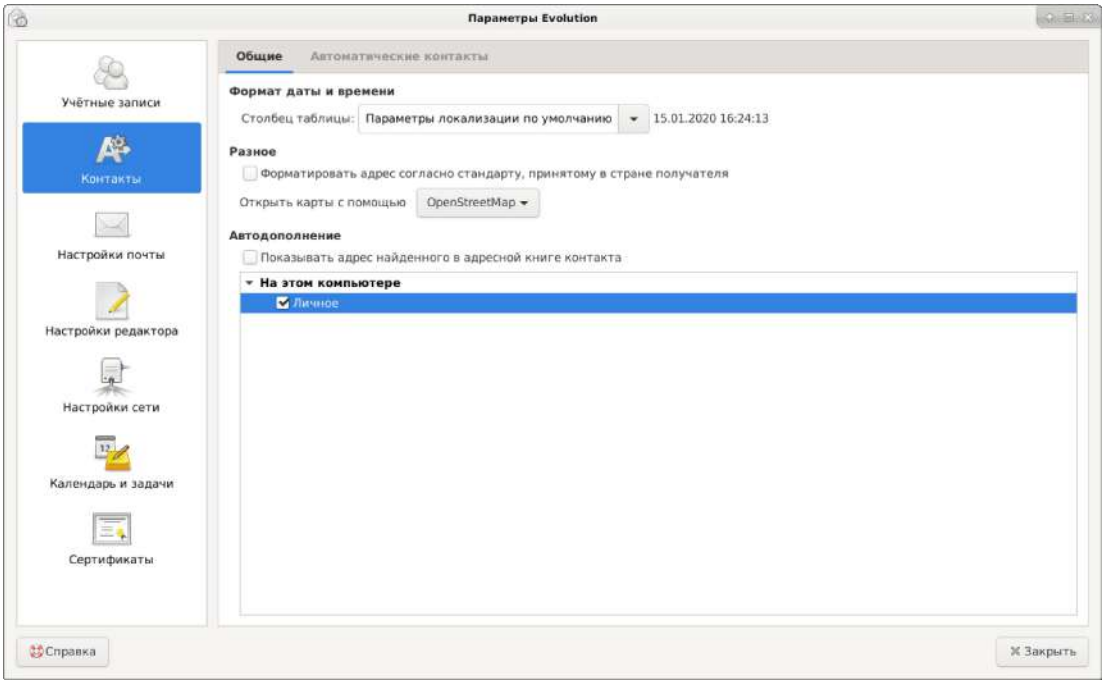
Во вкладке «Настройка редактора» производится настройка средств редактирования писем. В ней все настраивайте на свое усмотрение.

Во вкладке «Настройка почты» производится общая настройка работы почтового клиента. Здесь в графе «Сообщения HTML» я рекомендую указать «Никогда не загружать удаленное (не локальное) содержимое из Интернета» или хотя бы «Загружать удаленное (не локальное) содержимое только для сообщений от добавленных контактов» если вы полностью доверяйте тем, чьи адреса добавили в адресную книгу. Это позволит защититься от тех самых маячков.



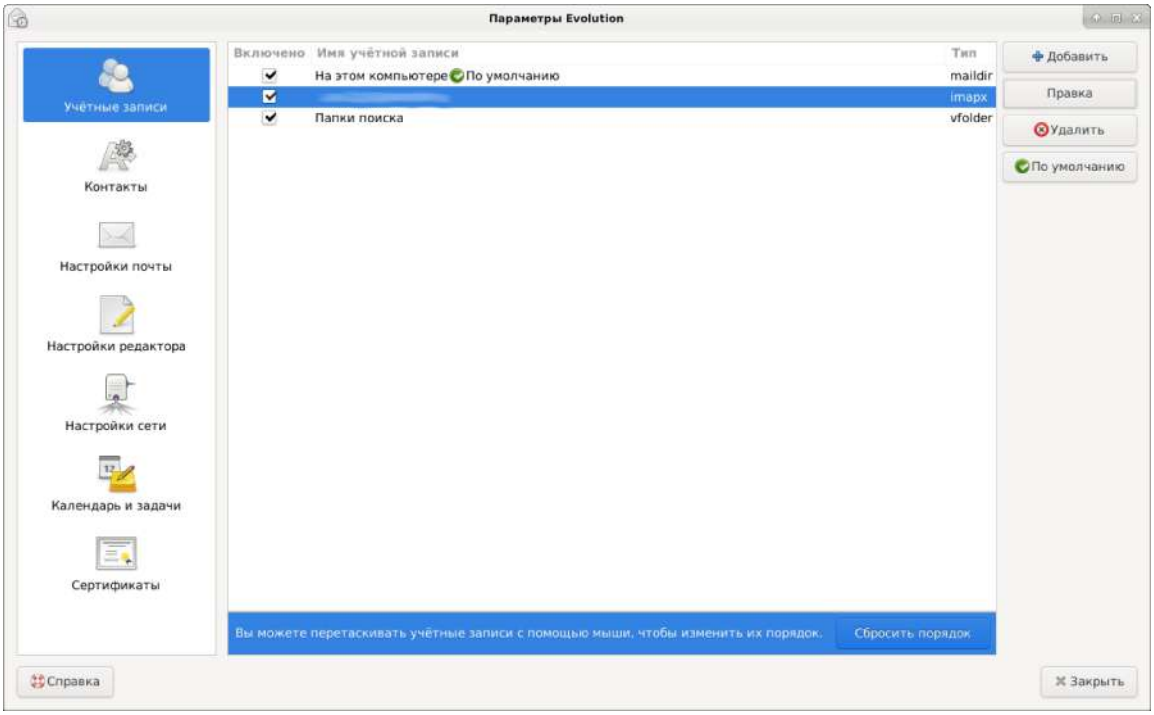
В остальных графах данной вкладки настройки делайте по своему усмотрению.

Во вкладке «Контакты», в графе «Общие» проверьте, чтобы у «Открыть карты с помощью» стояло «OpenStreetMap». Это свободный сервис карт, создаваемый энтузиастами по всему миру и не принадлежащий никакой корпорации. Он не ведет слежку за пользователями, как сервисы карт от того же Google. Об OpenStreetMap я еще расскажу в дальнейшем.

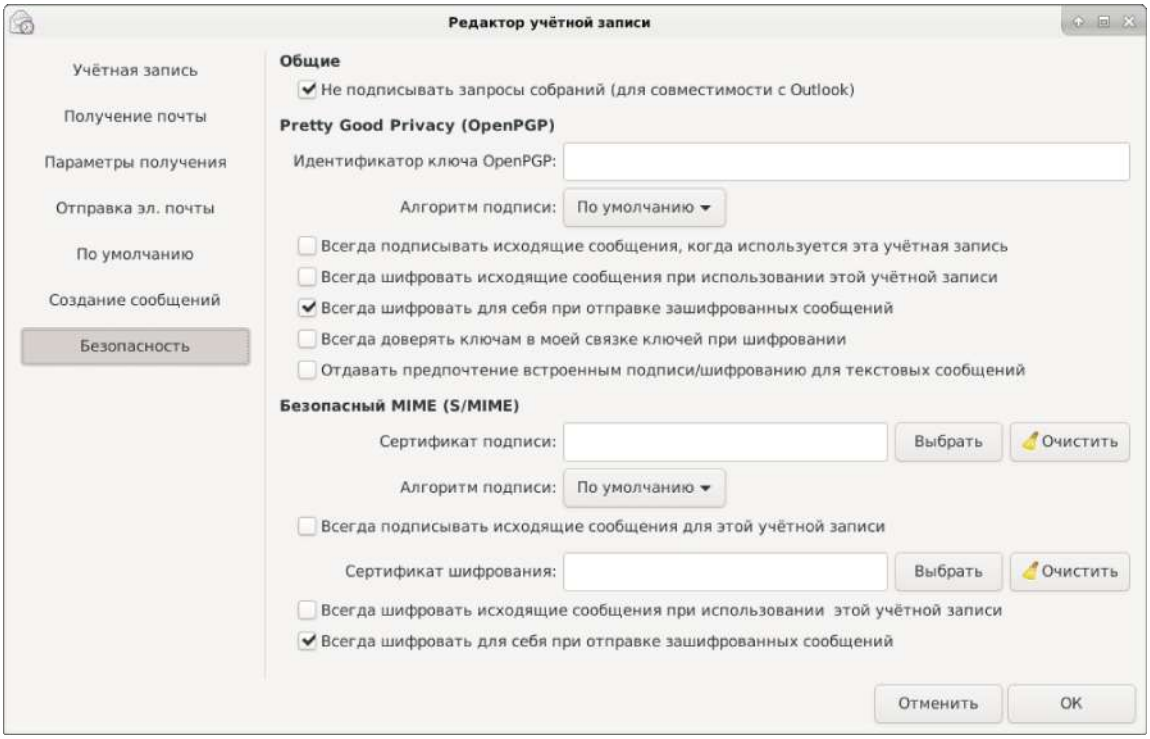


Остальные настройки в этой вкладке также на ваше усмотрение.

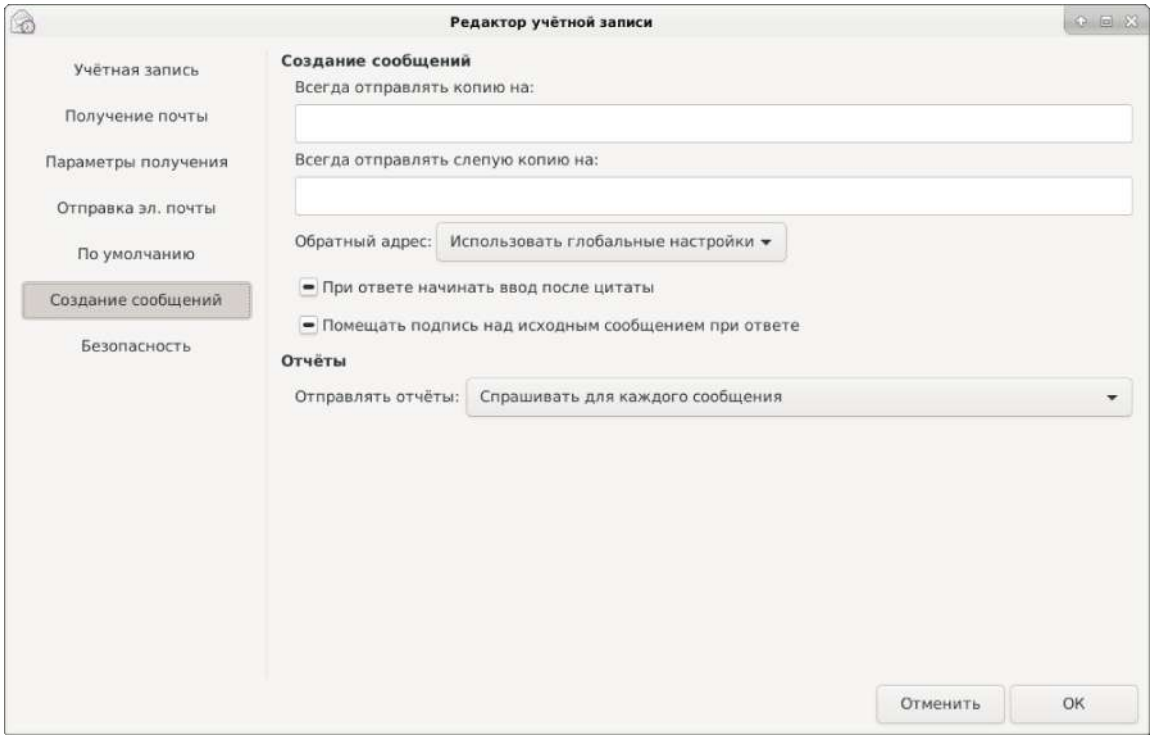
Во вкладке «Учетные записи» выделяем строку в которой указан ваш адрес электронной почты и нажимаем справа кнопку «Правка».



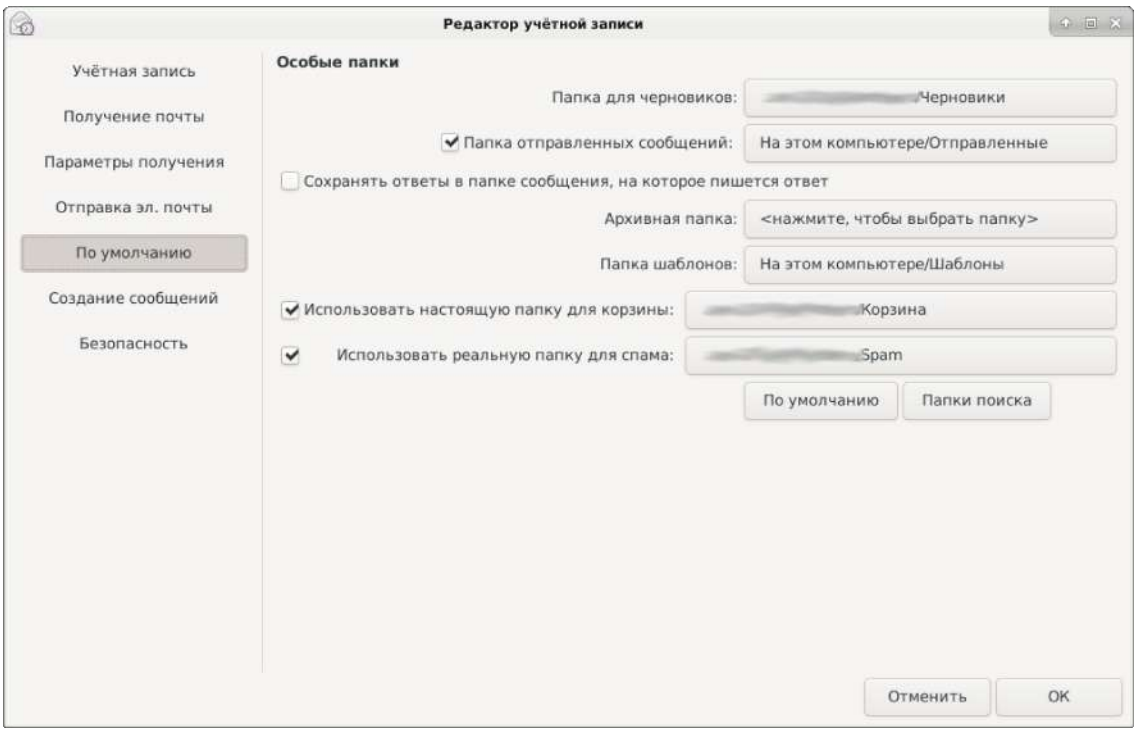
В появившемся окне во вкладке «Безопасность» настраивается шифрование писем. Как я уже сказал, для публичной почты смысла в этой функции не вижу.



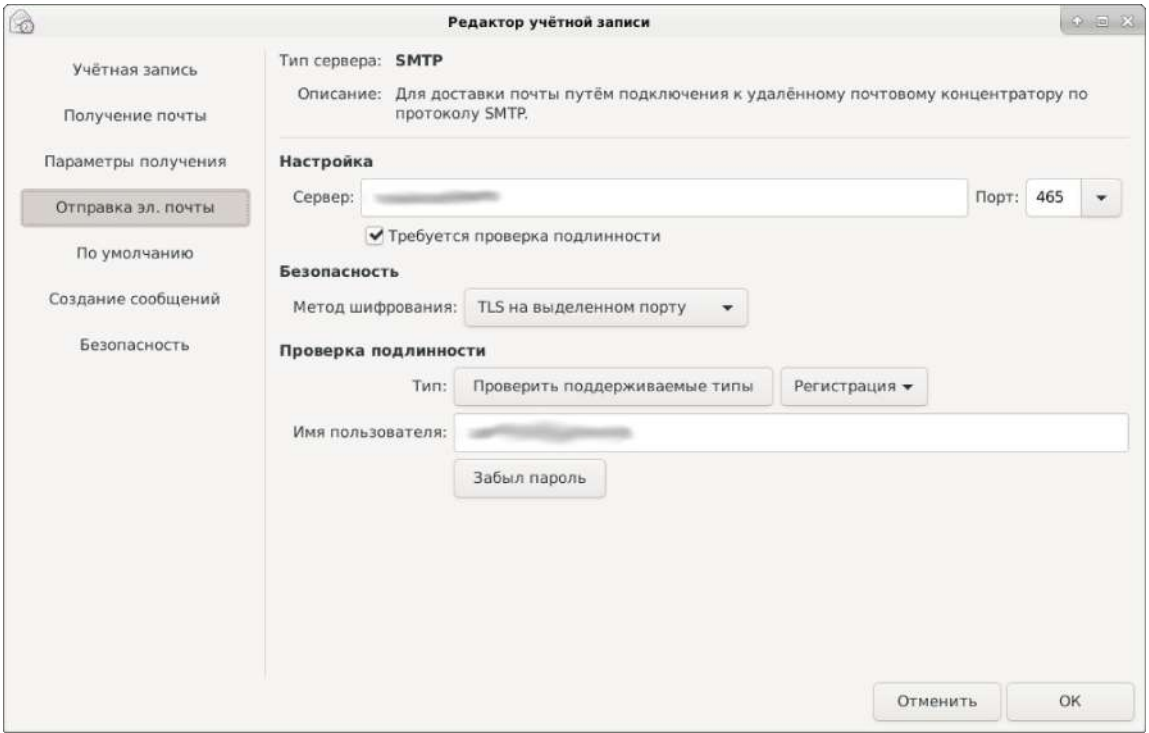
Во вкладке «Создание сообщений» выставляйте настройки в соответствии со своими предпочтениями.



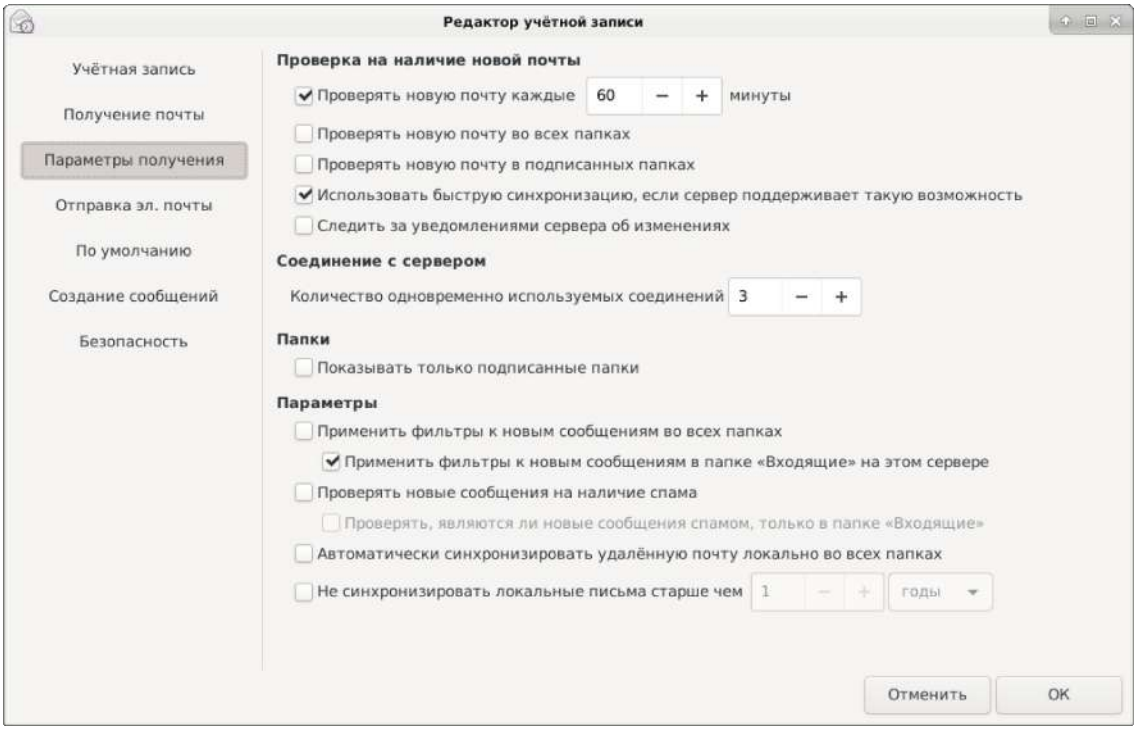
Во вкладке «По умолчанию» настраивается то, какие папки будут использоваться для сохранения тех или иных категорий писем. Я рекомендую оставлять в настройках сохранение писем на сервере почты, чтобы они не потерялись при откате виртуалки. Для этого проверьте, чтобы в графах был указан ваш адрес почты и название соответствующей папки. Выглядеть это будет как «test@test.ru/Черновики». С папкой «Отправленные» существует нюанс. Иногда возникает ошибка при попытке сохранить отправленное с помощью клиента письмо на сервер почты. Если это происходит, то можете указать в качестве папки для отправленных писем локальную. Выглядеть это будет как «На этом компьютере/Отправленные». Если письмо важно сохранить, то можете его потом скопировать в папку на сервере. Как это делать, а также как создавать резервные копии, я расскажу дальше.



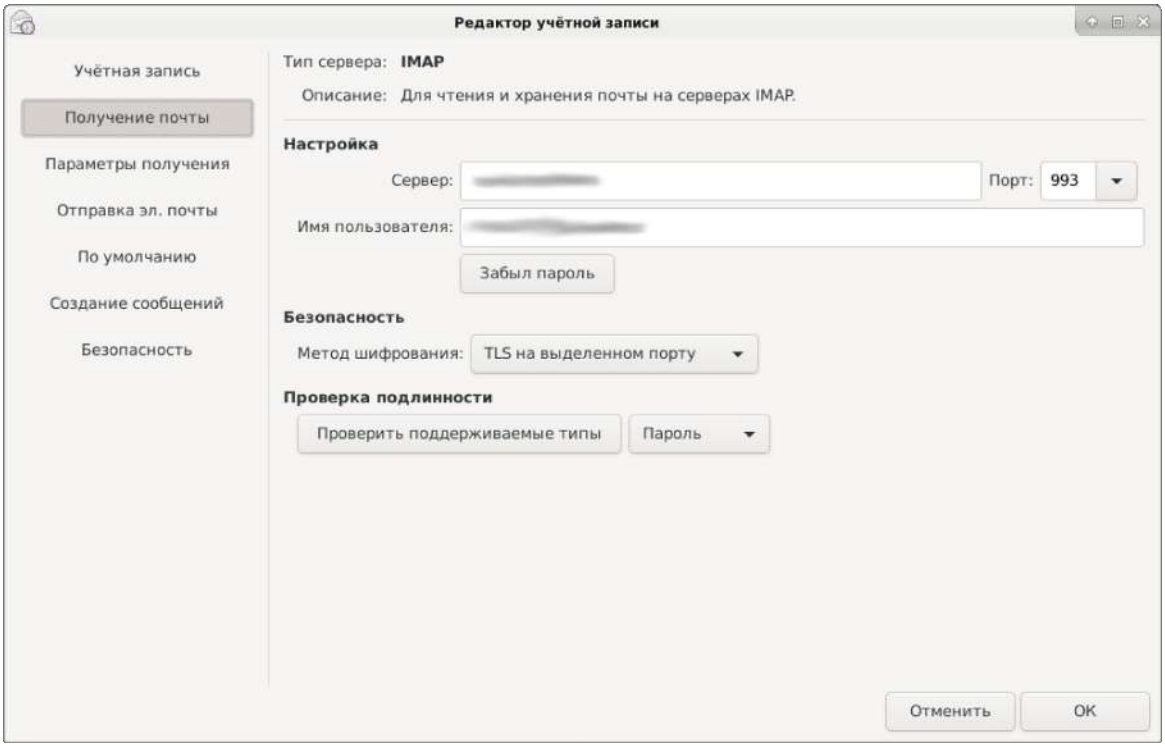
Во вкладке «Отправка эл. почты» проверьте графу «Метод шифрования», желательно, чтобы стояло «TLS на выделенном порту». Если столкнетесь с проблемой при отправке писем, возможно, поможет смена порта на 587. Производите эту смену только в том случае, если письма не отправляются и при этом разрешите этот порт в файерволе. Также под «Проверка подлинности» в графе «Тип» желательно нажать кнопку «Проверить поддерживаемые типы». Рядом отобразиться, какие типы проверки поддерживает сервер, не поддерживаемые будут зачеркнуты. Выставьте один из поддерживаемых, иначе не получится отправлять письма. Большинство почт поддерживает только «Регистрация» и «PLAIN». Рекомендую в этом случае ставить «PLAIN», поскольку он, по моим наблюдениям, работает быстрее и стабильнее.



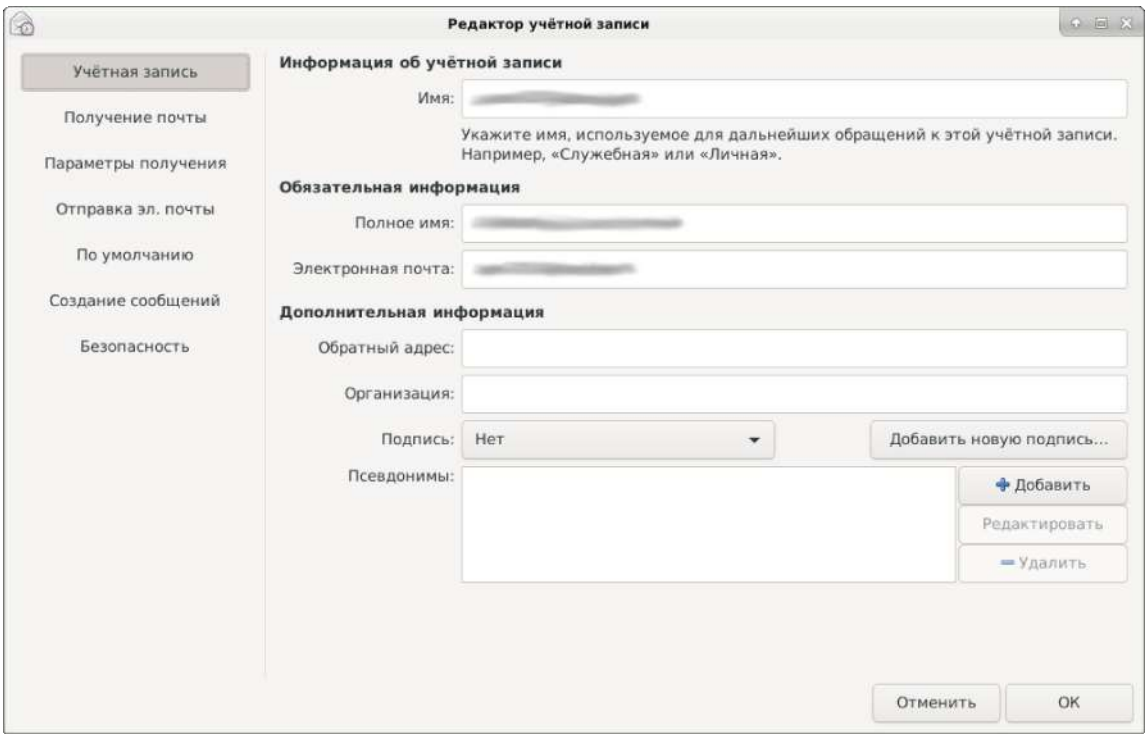
Во вкладке «Параметры получения» рекомендую выставить галочку на «Использовать быструю синхронизацию, если сервер поддерживает такую возможность». Остальные настройки в данной вкладке на ваше усмотрение.



Во вкладке «Получение почты», в графе «Метод шифрования» проверьте, чтобы стояло «TLS на выделенном порту». Также по «Проверка подлинности» можете нажать кнопку «Проверить поддерживаемые типы» и выбрать тот, который поддерживается сервером. Большинство почт поддерживает проверку только с помощью обычного пароля.



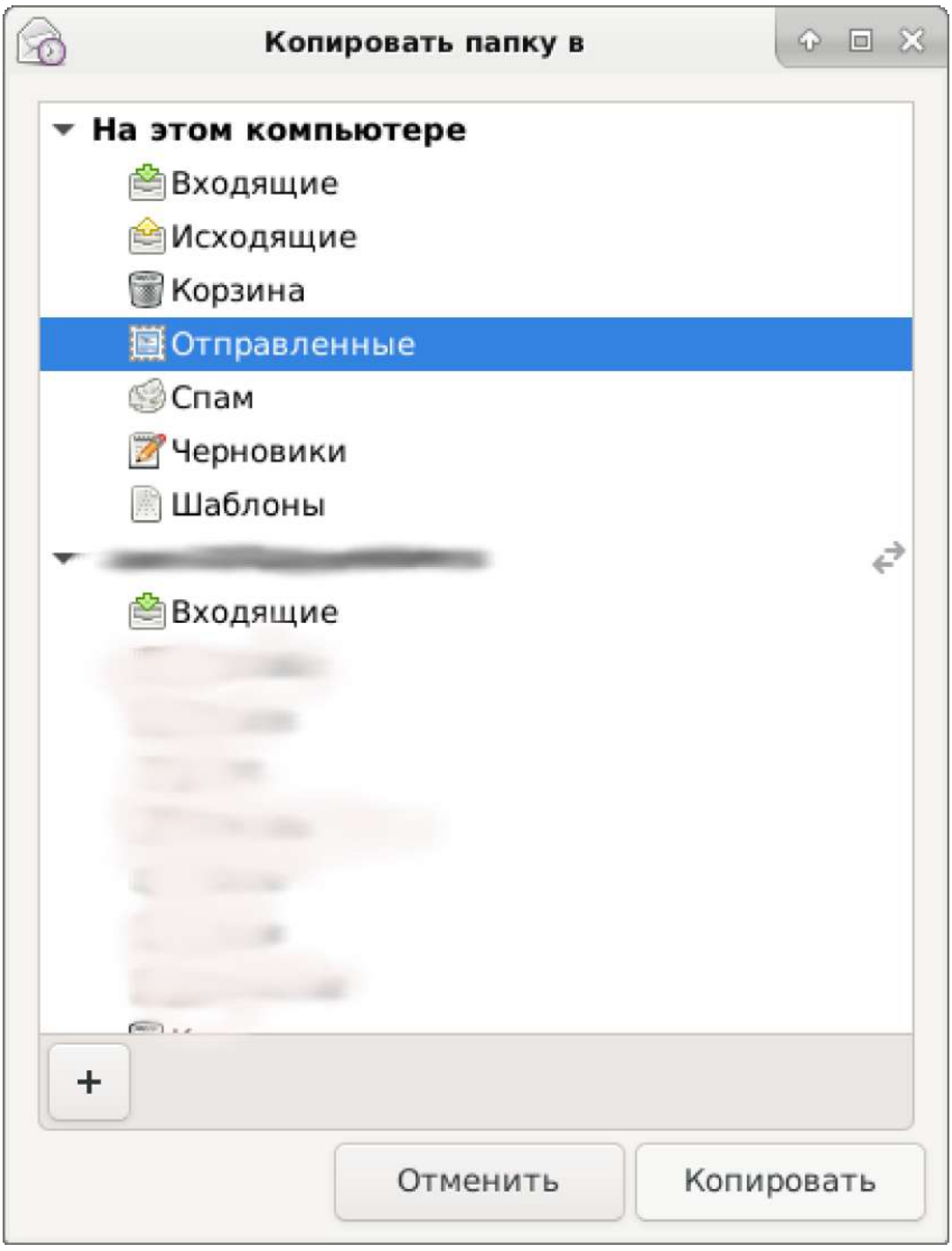
Во вкладке «Учетная запись» указывается ваш адрес электронной почты и то, чем будут подписаны ваши письма. Тут все заполняйте в соответствии со своими нуждами.



После этого нажимаем «Ok».

Теперь в окне параметров Evolution во вкладке «Учетные записи» можете добавить другие почтовые ящики, если они у вас есть. Для этого нажмите кнопку «Добавить» справа сверху и еще раз осуществите все приведенные выше действия. Когда все сделано, нажимаем внизу справа «Закрыть».

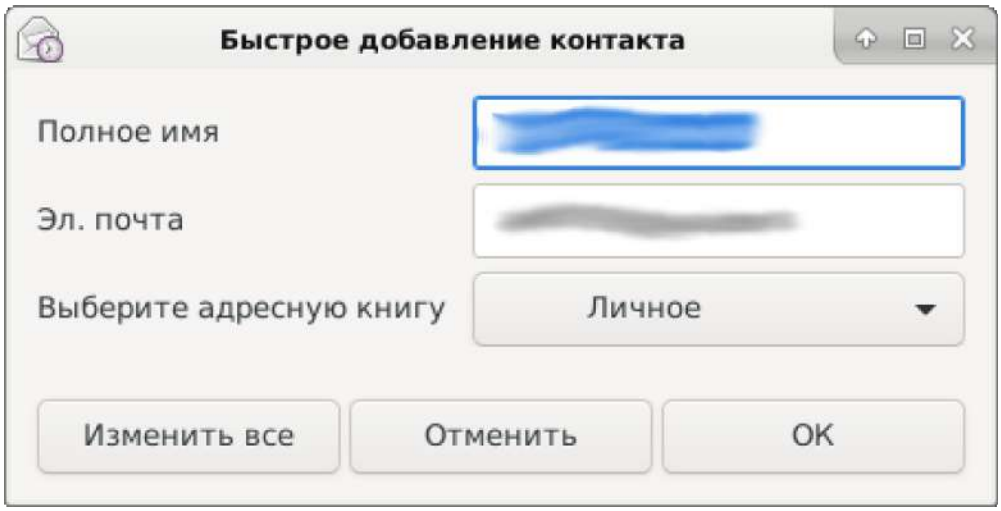
Теперь расскажу, как делать резервные копии писем. Для начала необходимо создать папку, в которую будет сделана копия писем. Для этого в левом поле выделяем «На этом компьютере», нажимаем правой кнопкой мыши и выбираем «Создать папку». В появившемся окне вводим название папки и нажимаем «Ok». Эта папка появится на вашем компьютере в каталоге клиента. Аналогичным образом папки можно создавать внутри папок. Для того, чтобы скопировать целую папку нажмите на нужную в поле слева правой кнопкой мыши и выберите «Копировать папку в». Откроется окно, в котором нужно выделить папку, в которую будут помещены копии, и нажать внизу кнопку «Копировать». Аналогичным образом копируются и отдельные письма. Выделяйте их, нажимайте правой кнопкой мыши, выбирайте «Копировать папку в», в открывшемся окне выделяйте нужную папку и нажимайте «Копировать».



Начнется процесс копирования. После того, как копии будут сохранены, нажимайте слева наверху кнопку «Файл» и выбирайте «Сделать резервную копию данных». В выскочившем окне набирайте название файла или оставляйте предложенное, и нажимайте «Сохранить». Появится окно, сообщающее, что для копирования программу нужно закрыть, а также предлагающую перезапустить ее после окончания процесса копирования. Нажимаем «Закрыть и сделать резервную копию Evolution». После того, как

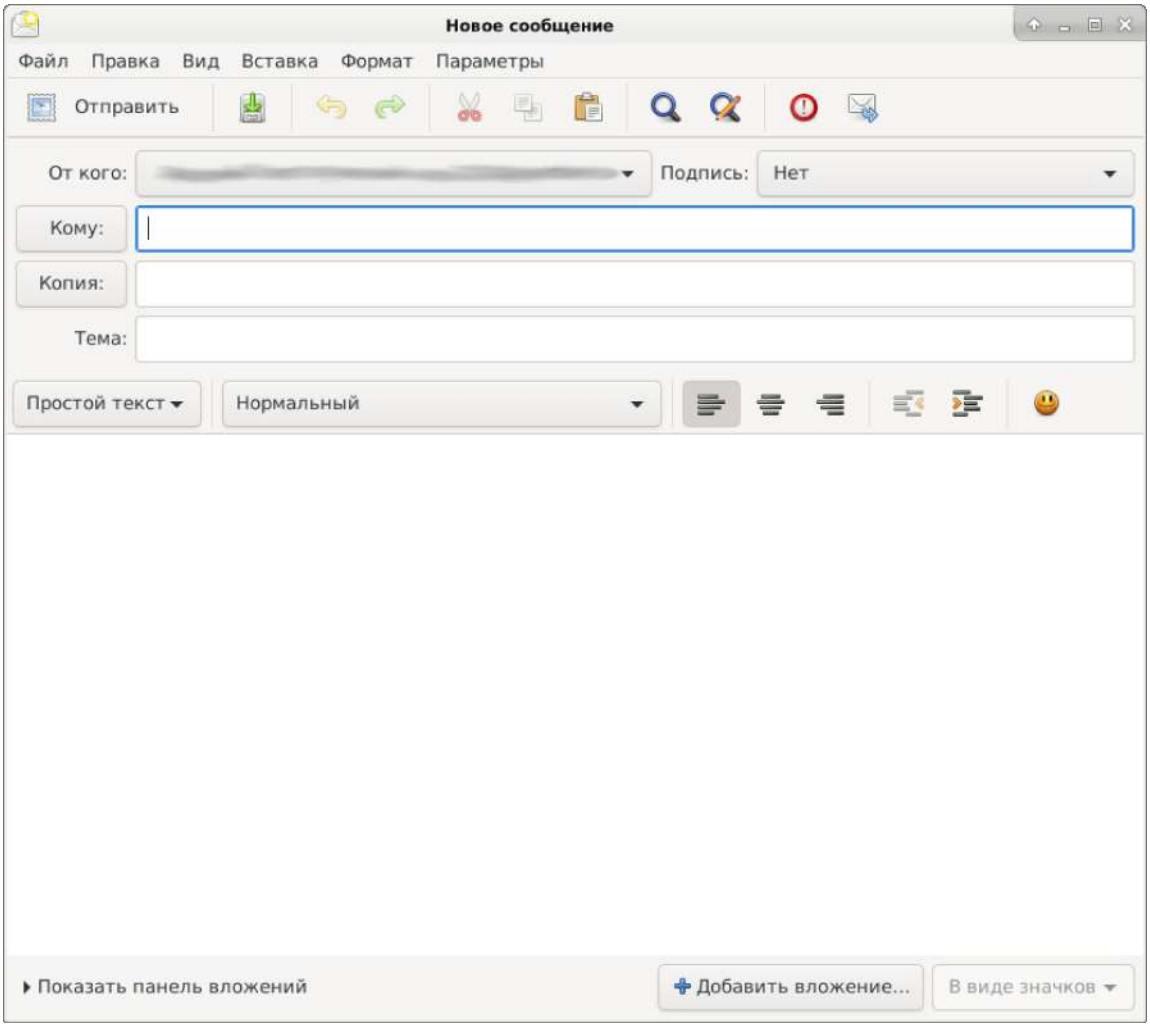
резервная копия будет создана, можете скопировать эти файлы на флешку и они будут сохранены.

Касательно составления адресной книги, в Evolution нет функции импорта контактов с сервера, поэтому список адресов придется формировать вручную. Это возможно делать, как непосредственным забиванием в контакты, для чего слева внизу нужно нажать «Контакты», после чего откроется меню адресной книги. Или можно добавлять их из писем. Для этого откройте письмо, щелкните правой кнопкой мыши по нужному контакту, выскочит окно с именем, адресом и предлагаемой адресной книгой (тут выбирайте нужную, их может быть несколько), и нажмите «Ok».



Подобным образом добавьте все необходимые контакты.

Чтобы создать письмо, щелкните слева сверху «Создать». В появившемся окне, в графе «От кого» выберите тот профиль электронной почты, с которого хотите отправить письмо, также можете выставить подпись. В графе «Кому» наберите имя или адрес того, кому письмо предназначено. При наборе программа сама будет предлагать варианты из адресной книги (если вы эту функцию не отключили в настройках). Можно добавить несколько. В графе «Копия», если нужно, наберите тех, кому будет переслана копия. Заполните, если нужно, графу «Тема» и само поле письма. Если щелкните на кнопку слева «Простой текст», то можете вместо него выбрать «HTML», что откроет больше возможностей для форматирования письма. Если нужно прикрепить файлы, кнопка «Добавить вложение» внизу справа. Когда письмо будет готово, нажмите слева вверху «Отправить». Если пока не хотите отправлять, рядом кнопка «Сохранить».



Вот в общем-то и все, что я хотел рассказать об этом клиенте.

Хочется сказать о клиенте Claws Mail.[1] Он является форком Sylpheed, легковесный, с достаточным количеством функций. У меня с ним подружиться не получилось, но если вам по каким-то причинам не понравится Sylpheed, но при этом вы захотите пользоваться именно легковесным клиентом, можете попробовать Claws Mail.

Ну и также, думаю, стоит сказать о клиенте под названием Mailpile,[2] поскольку его иногда упоминают, когда речь идет о безопасной электронной почте. По заявлениям разработчиков, клиент был сделан специально с упором на безопасность, в него хорошо интегрировано шифрование писем. Однако я его не рекомендую. Во-первых, в репозиториях Devuan его нет, и вам придется лезть на сайт, скачивать его и заморачиваться с установкой из отдельного пакета. Процесс установки затруднен. Во-вторых, он имеет только веб-интерфейс и разворачивается в браузере, что на мой взгляд, не самое удачное

решение. В-третьих, у него не только нет своего программного интерфейса, у него еще и нет простой системы запуска с иконками в Меню. Чтобы его запустить, нужно открыть терминал, набрать в нем «mailpile», и только тогда он откроется. Конечно, существуют способы создать значок для запуска, однако, это также весьма затруднительно.

Конечно, существуют и другие клиенты электронной почты, но эти наиболее распространенные и удобные.

26 Программы для VoIP

Кому-то в связи с его деятельностью может потребоваться использовать IP-телефонию. VoIP, это технология совершения звонков через Интернет.[3] В зависимости от конкретного клиента, функционал может позволять обмен сообщениями, голосовую и видеосвязь.

Если вы пользуйтесь каким-либо сервисом SIP-телефонии, вам необходимо подобрать приличный свободный клиент.[4] К сожалению, не каждый сервис VoIP может работать с такими программами. Многие сервисы позволяют пользоваться ими только через свои несвободные клиенты. От услуг таких поставщиков следует отказаться.

Наиболее предпочтительным вариантом является клиент Linphone.[5] Он крайне функциональный и удобный. В качестве не столь функциональной альтернативы можно порекомендовать клиент Twinkle.[6] Позволяет обмениваться сообщениями и осуществлять голосовые звонки. Оба клиента присутствуют в репозиториях Devuan. Их можно установить оттуда и пользоваться.

27 Сервис MEGA

Для многих может быть важным удаленное хранение файлов. И для всех являются необходимыми стабильные и безопасные инструменты общения, которые можно предлагать для использования даже тем знакомым и близким, кому сложно даются в освоении компьютерные технологии. Существует сервис, который способен предоставить, как надежное удаленное хранилище, так и стабильные, при этом безопасные, инструменты для общения. Он называется MEGA.[7]

Инструменты данного сервиса являются почти свободным ПО. К сожалению, налагаются определенные ограничения на коммерческое

распространение копий исходного кода. Однако сам исходный код открыт.[8] И учитывая, что это единственный сервис с такими возможностями, я могу рекомендовать его.

Вся передаваемая информация в MEGA шифруется непосредственно на устройстве пользователя. Это касается, как помещаемых в хранилище файлов, так и переписки, звонков. При работе с сервером через браузер, это осуществляется с помощью скриптов, что открывает дополнительные уязвимости. Чтобы избежать рисков, связанных с ними, у MEGA есть расширение для браузера, которое реализует функционал собственными механизмами. К сожалению, на момент написания пособия расширение для Firefox перестало поддерживаться, поэтому рекомендовать к использованию нечего.

Объем хранилища для бесплатного аккаунта составляет 20 Гб. За плату его можно значительно расширить. Максимальный объем составляет 16 Тб. Такого объема не предоставляет более никто. Даже популярные удаленные хранилища, от Google и Apple способны предоставить максимум 5 Тб.[9] Для платных аккаунтов также существуют дополнительные функции, например, возможность дополнительно зашифровывать помещаемые в хранилище файлы с помощью паролей.

В отношении общения MEGA позволяет обмениваться сообщениями, файлами, осуществлять голосовую и видеосвязь, вести аудио и видеоконференции. Стабильность связи крайне высокая, чем к сожалению, не могут похвастаться многие свободные средства связи. Именно поэтому я рекомендую данный инструмент в качестве основной рекомендации для широкого круга пользователей. Он способен заменить такие популярные мессенджеры как WhatsApp, Viber и прочее барахло.

Необходимо отметить, что MEGA привязывается к электронной почте, но по сегодняшним временам это не особо критично, поскольку даже ширпотребные почты сейчас массово уходят от идентификации пользователей по номерам телефонов. Конечно, это все равно несколько снижает приватность, почему я и помещаю инструкцию по работе с инструментами MEGA в раздел о публичной Интернет-активности. Но для общения с близкими, с теми с кем ваша связь и так известна, данный инструмент подходит идеально. Защищенность связи, за счет сквозного шифрования, все равно весьма высокая.

Идем на сайт MEGA и нажимаем вверху справа кнопку «Зарегистрироваться». Здесь необходимо указать имя, адрес электронной почты и пароль, для чего, конечно же, нужно создать соответствующую запись в менеджере паролей. Также необходимо проставить галочки на пунктах внизу. После нажатия на кнопку «Регистрация», на указанную почту придет письмо со ссылкой, по которой нужно будет пройти для подтверждения. После этого аккаунт будет создан.

В аккаунте идем в настройки и настраиваем свою учетную запись.

28 Удаленное хранение файлов в MEGA

Чтобы перейти в удаленное хранилище, в своем аккаунте нажимаем на значок папки слева сверху. Для создания папки, нажимаем на кнопку «Новая папка» вверху справа.

В появившимся поле вводим название папки и нажимаем «Создать». Папка будет создана.

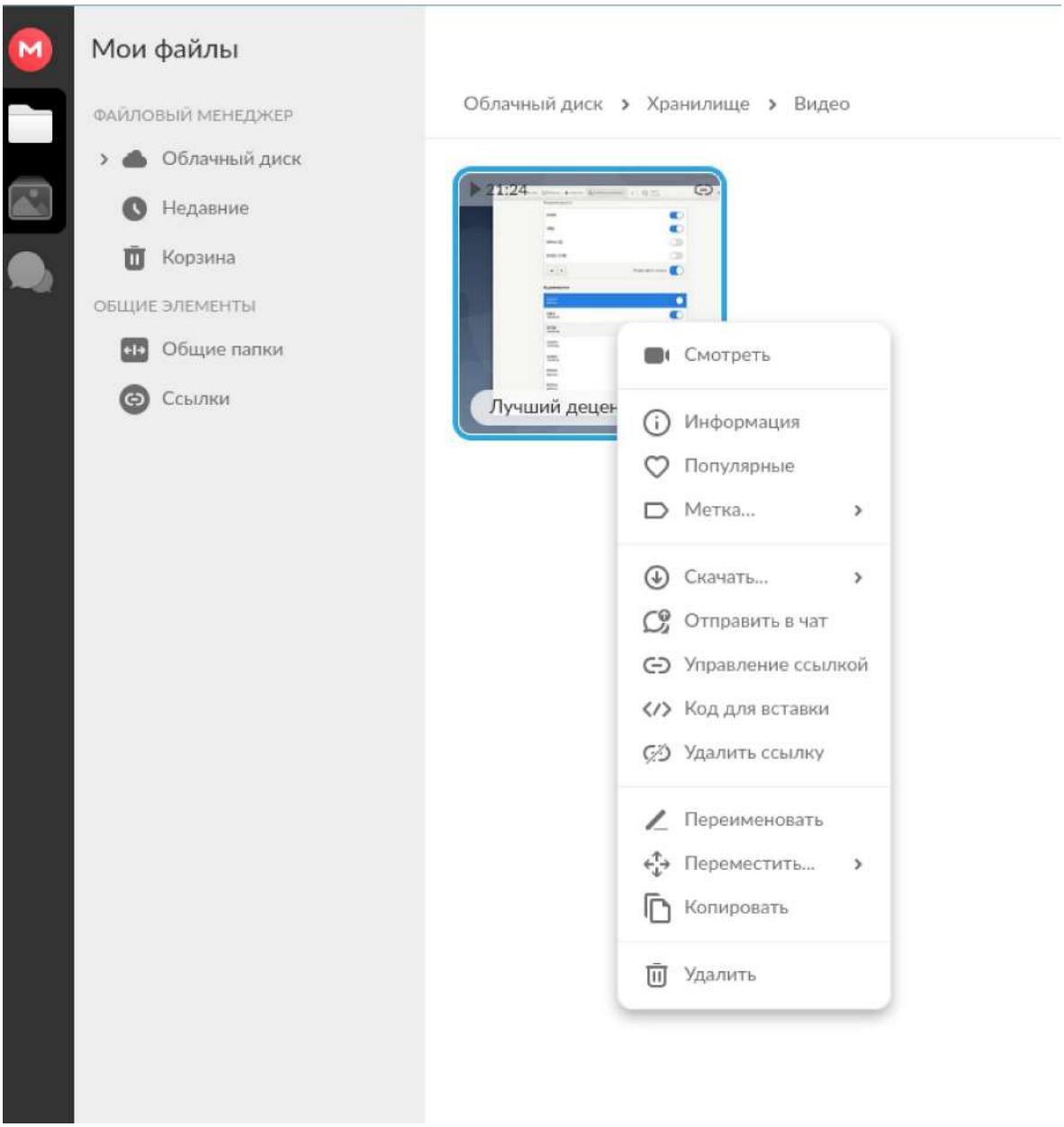
Чтобы поместить в хранилище целую папку, нажимаем «Загрузить» вверху справа и выбираем «Загрузить папку».

В открывшемся окне выбираем ту папку, которую хотим отправить в хранилище, и нажимаем «Открыть». Папка будет загружена.

Чтобы поместить в хранилище файл, также нажимаем «Загрузить» и выбираем «Загрузить файл».

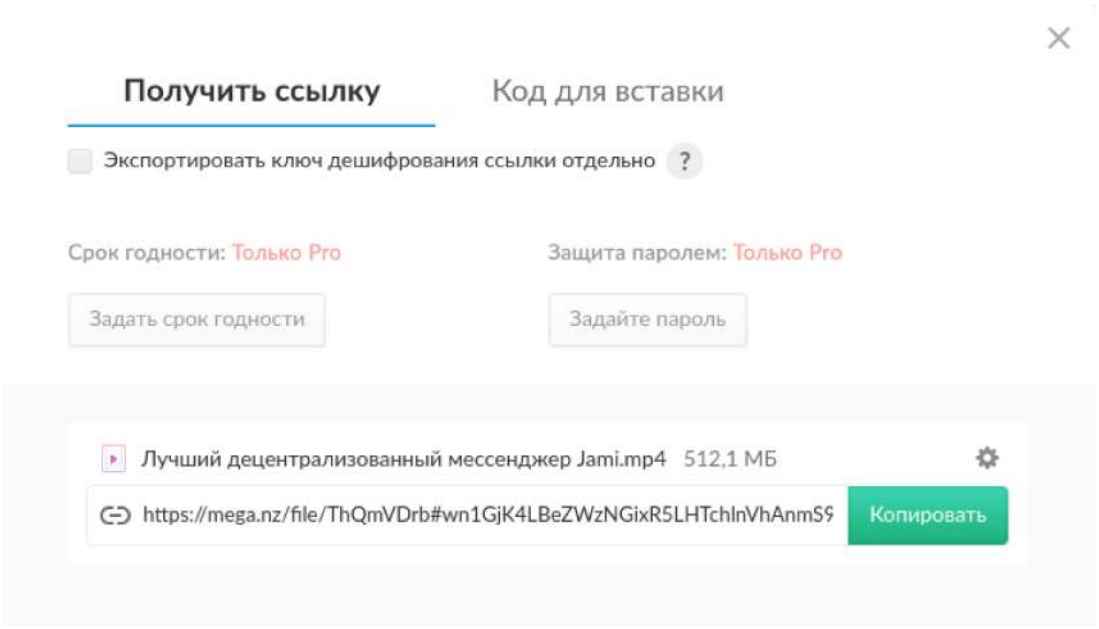
В появившемся окне выбираем нужный файл и нажимаем «Открыть». Файл будет загружен.

Если нажать на папку или файл правой кнопкой мыши, то можно выбрать пункт «Создать ссылку» или если вы прежде уже создавали ссылку на данную папку или файл, то «Управление ссылкой».

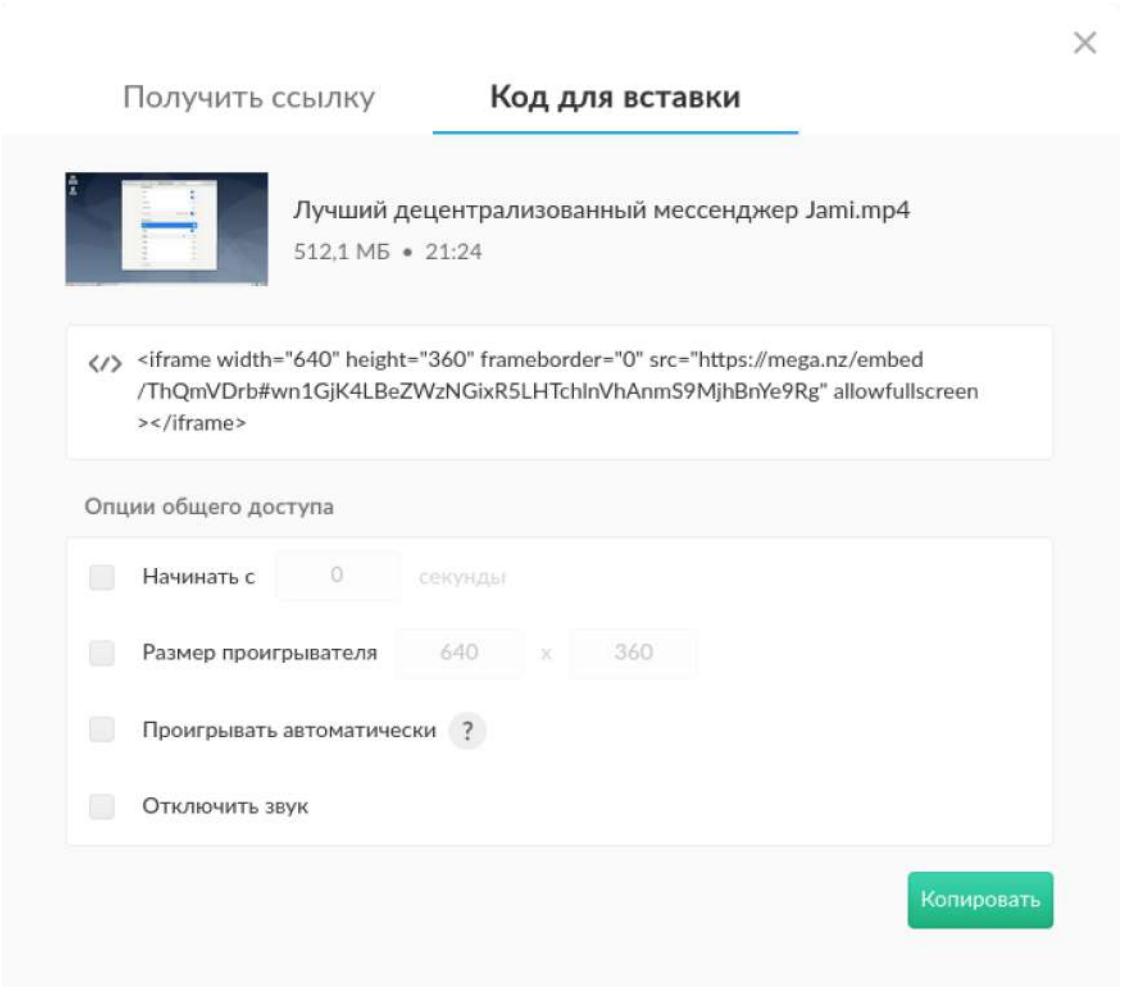


В открывшемся окне внизу показана ссылка, которую можно передать тем, с кем вы хотите поделиться папкой или файлом. Вверху есть возможность активировать разделение непосредственной ссылки и ключа шифрования «Экспортировать ключ дешифрования ссылки отдельно». По-умолчанию ключ шифрования интегрирован непосредственно в ссылку, но если вы хотите отдельно передавать ссылку и ключ, то можете их разделить. Для платных аккаунтов также существует возможность дополнительно защитить папку или

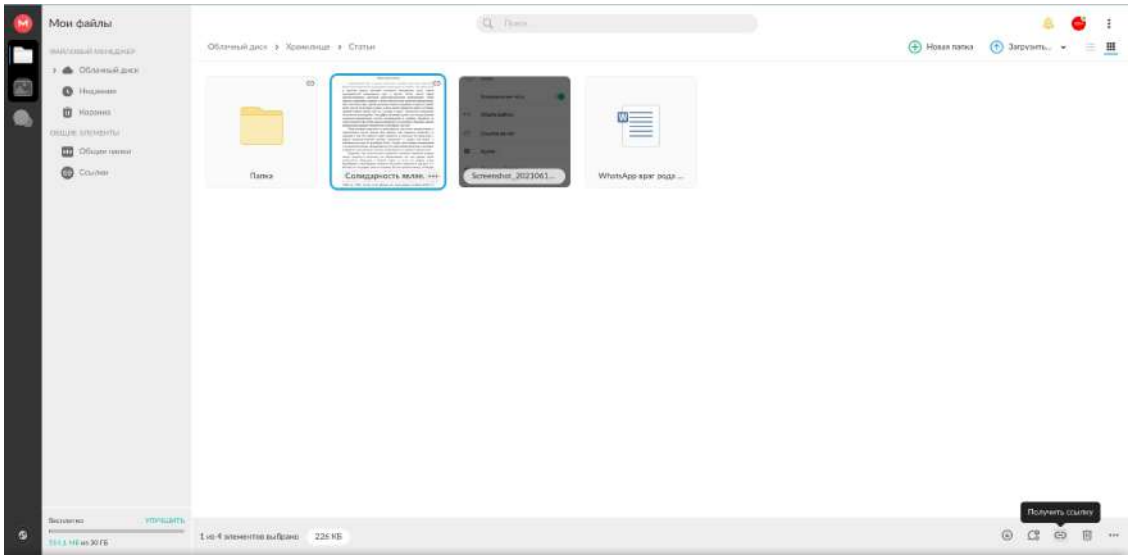
файл с помощью пароля, а также задать время действия ссылки, по истечении которого, она действовать перестанет.



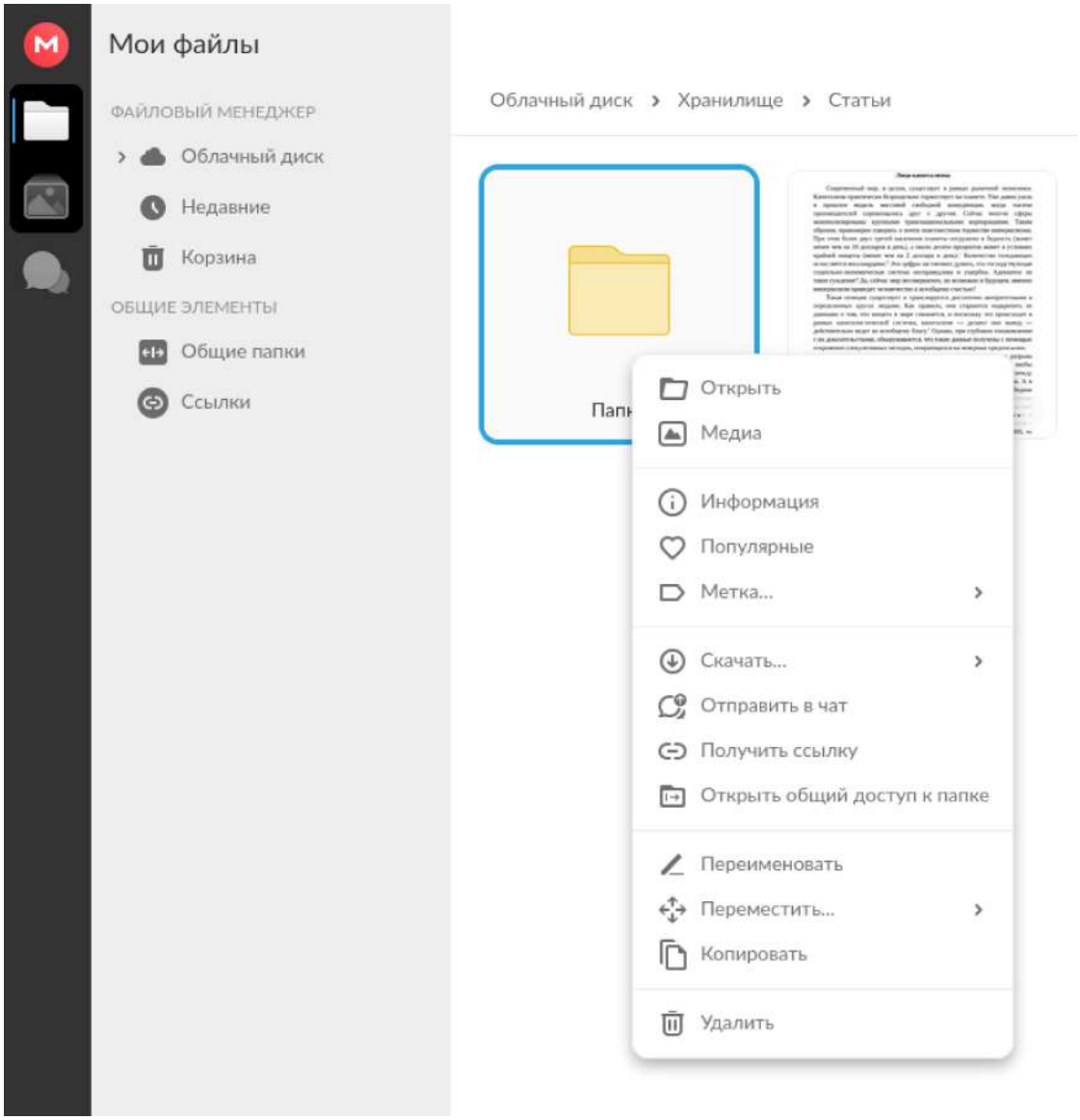
Если файлом является видео, то также будет присутствовать функция «Код для вставки». Это создание тайм-кодов, с помощью которых вы сможете создавать ссылки на конкретные моменты видео.



Также для получения ссылки можно просто выделить папку или файл щелчком мыши и нажать на значок цепочки внизу справа.



Если нажать правой кнопкой мыши сугубо по папке, то в открывшемся поле также будет пункт «Открыть общий доступ к папке». Если его активировать, то тогда те, кому вы передадите ссылку на эту папку, смогут не только просматривать ее содержимое, но и изменять — добавлять либо удалять файлы.



Если кто-то вам прислал ссылку на файл в MEGA, то пройдя по ней вы попадете на страницу файла. Многие форматы текста, изображений, аудио и видео MEGA позволяет просматривать непосредственно в сервисе. Также вы можете легко скачать файл, нажав кнопку «Скачать».

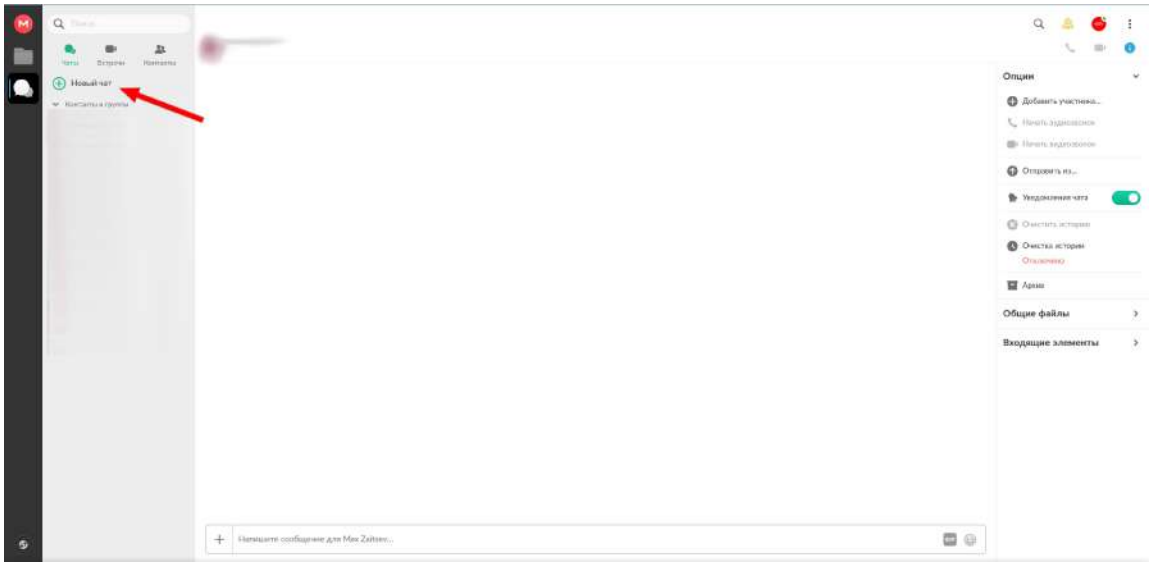
Чтобы скачать файл, будучи в папке, нажмите на него правой кнопкой мыши, нажмите «Скачать» и затем выберите «Обычная загрузка» или «Скачать в ZIP», чтобы скачать файл или папку, запакованные в архив. Также кнопка скачивания присутствует в окне просмотра вверху справа.

Кроме всего этого, при входе в удаленное хранилище по значку слева, под ним появляется значок галереи, пройдя в которую можно легко просматривать медиафайлы.

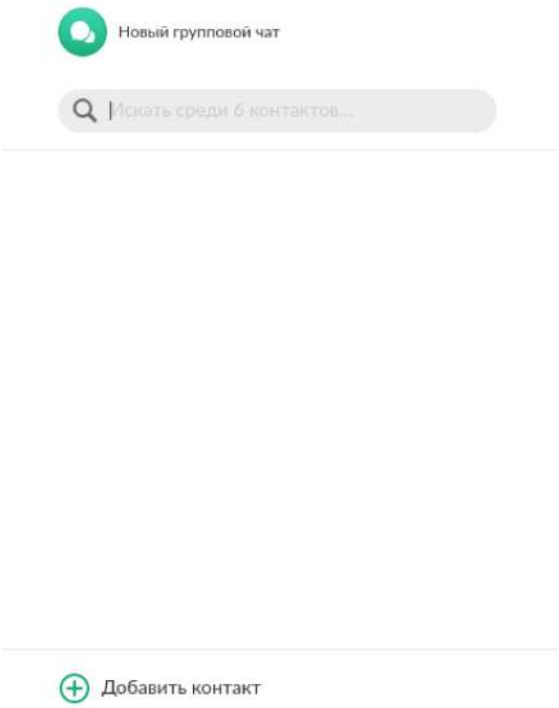
Таковы наиболее важные функции удаленного хранилища.

29 Общение с помощью MEGA

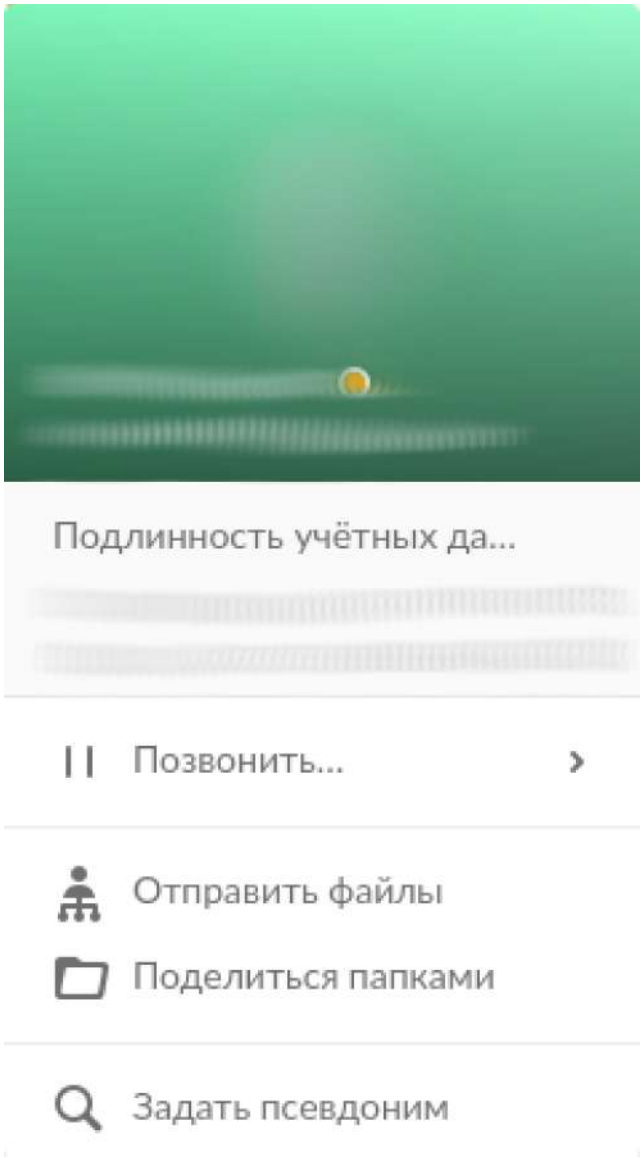
Для того, чтобы открыть инструменты общения, в своем аккаунте нажимаем на значок слева под значками папки и галереи. Для того, чтобы добавить собеседника нажимаем на зеленый значок с плюсом и надписью «Новый чат» слева вверху.



Затем внизу нажмите «Добавить контакт».

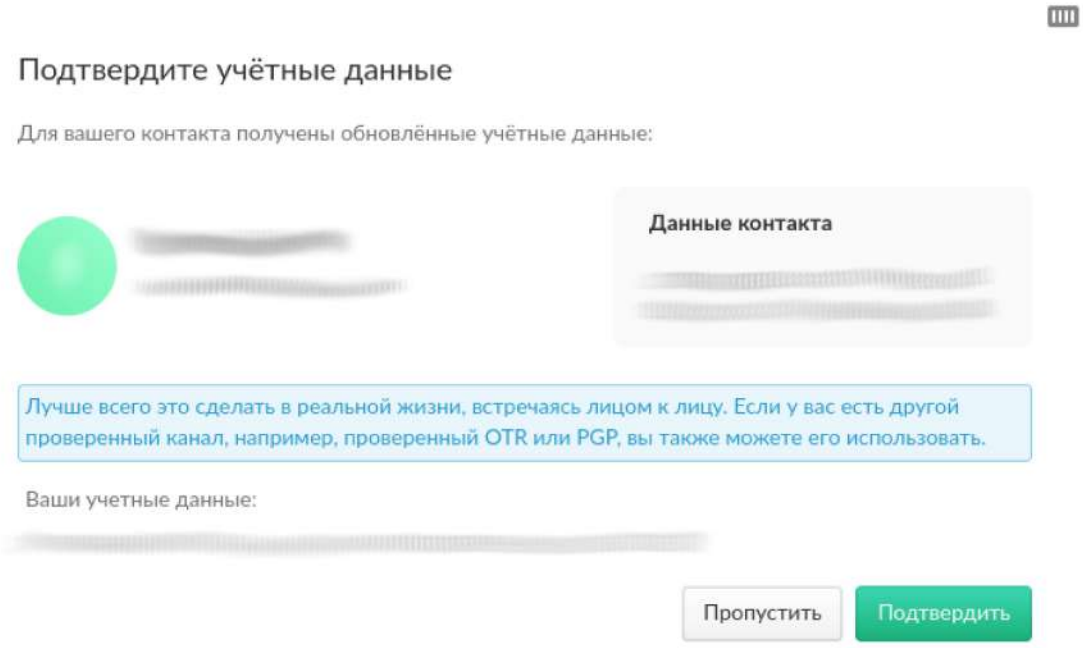


Необходимо ввести адрес электронной почты, который используется собеседником в качестве идентификатора MEGA. После добавления существует возможность подтвердить собеседника. Если нажать на имя контакта, то в открывшемся поле будет информация о нем, в том числе набор символов, являющийся ключом подтверждения.



Если нажать на него, то выскочит поле, где будут также отображены данные контакта вместе с ключом подтверждения, а внизу будут отображен ваш ключ. Если встретится с собеседником и сравнить этот ключ с тем, который видит он в информации о вас, то можно удостовериться, что при формировании контакта, связь установилась именно с вами, а не с кем-то, кто пытался выдать себя за вас. Точно также и вы можете сравнить ключ вашего

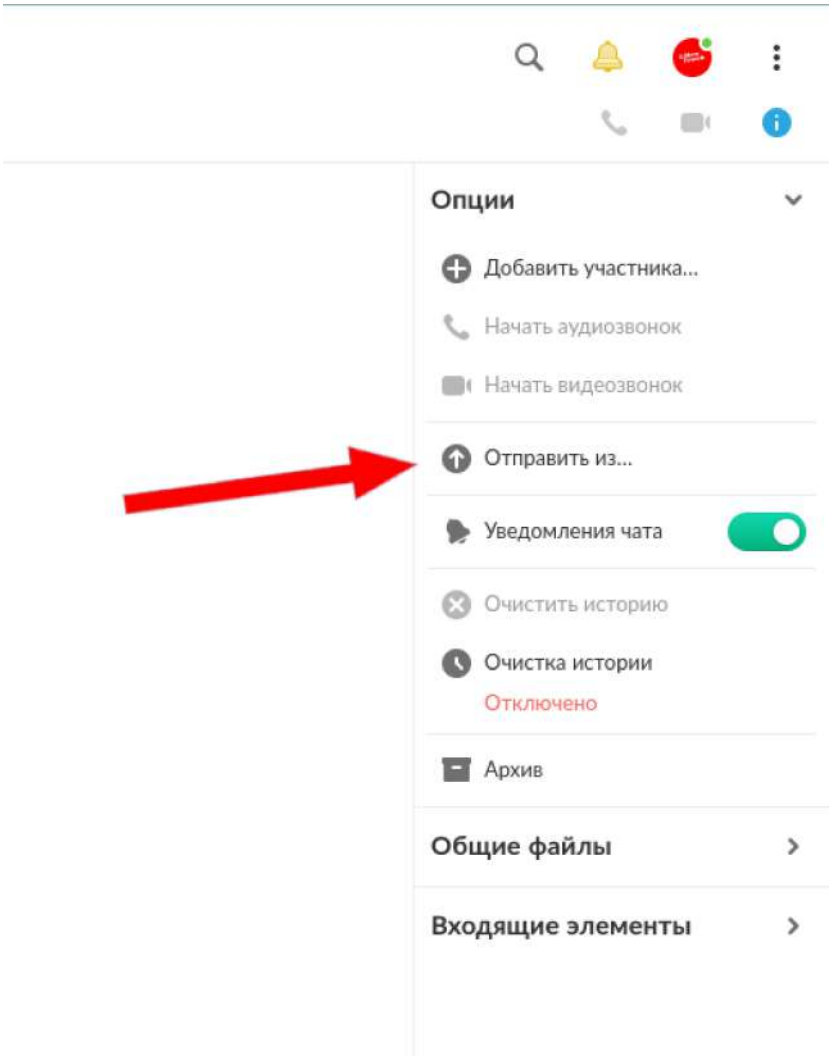
собеседника, отображаемый у него и у вас. Если они совпадают, нажимайте на кнопку «Подтвердить». Контакт будет отмечен, как подтвержденный.



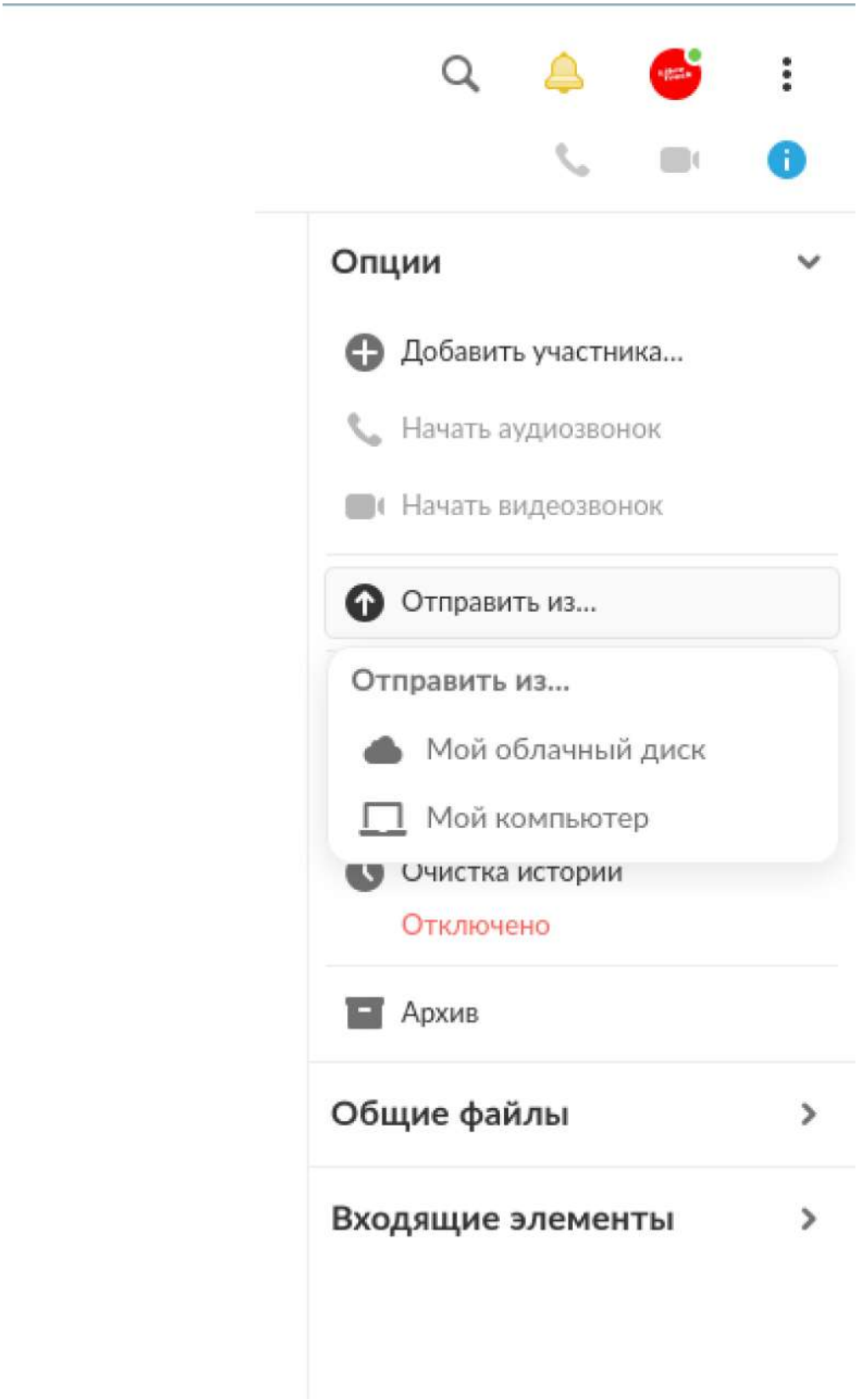
Чтобы начать диалог, нажимаем в поле слева на тот контакт, с которым хотите общаться.

Чтобы отправить сообщение, наберите его в поле внизу и нажмите на значок самолетика справа от него.

Чтобы отправить файл в поле справа выберите пункт «Отправить из».

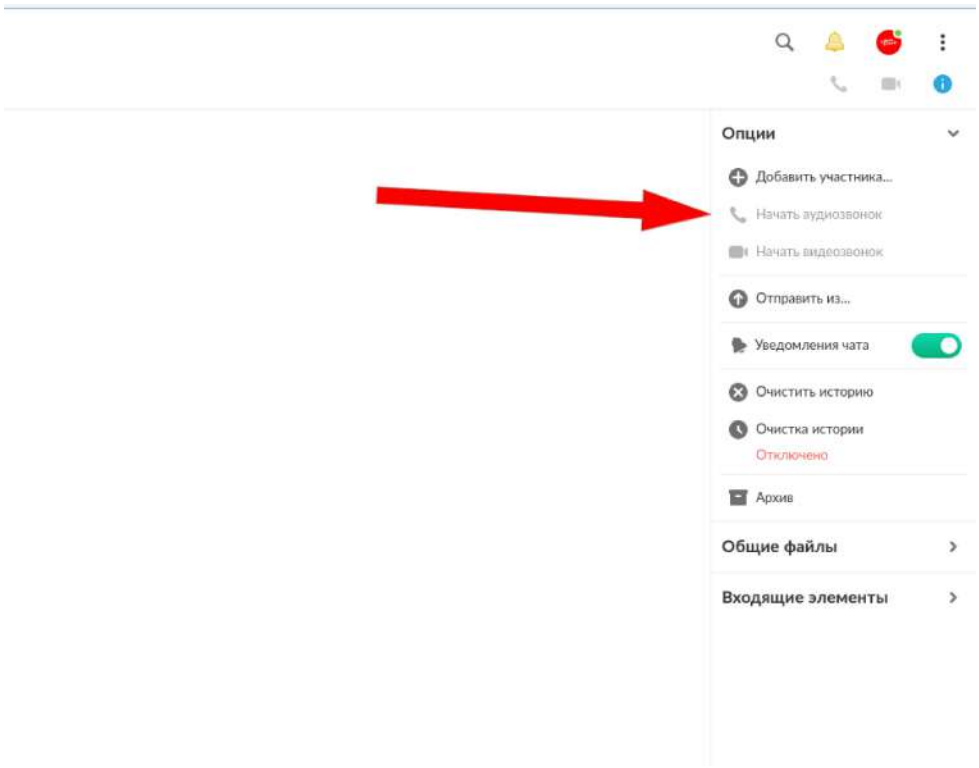


Выберите источник файла — облачный диск или компьютер. Затем в открывшемся окне выберите нужный файл и нажмите «Отправить».

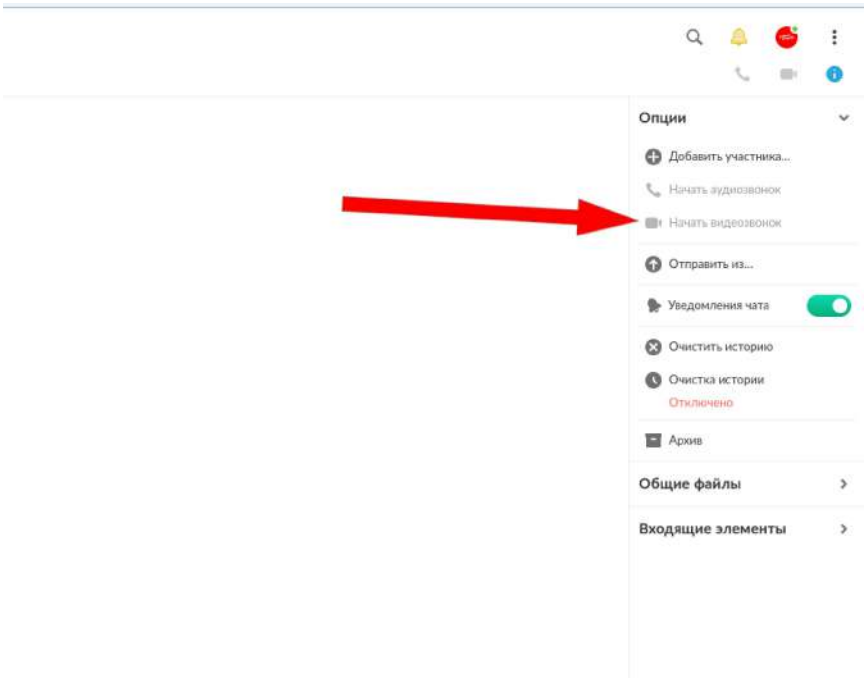


Работа с файлами в чате, такая же как с теми, что лежать в хранилище. Для скачивания нажмите правой кнопкой мыши по файлу и затем «Скачать файл».

Чтобы совершить голосовой звонок, нажмите в поле справа «Начать аудиозвонок» или вверху справа значок трубки.

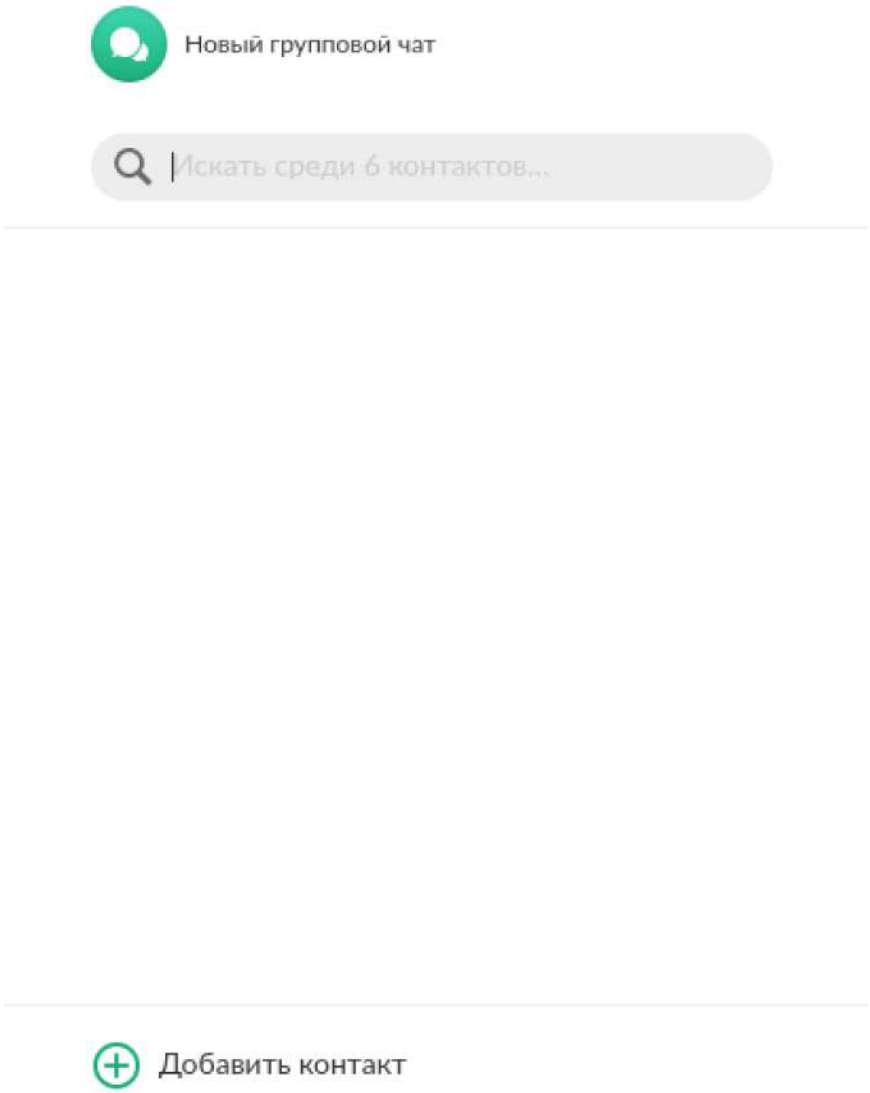


Чтобы совершить видеозвонок, нажмите в поле справа «Начать видеозвонок» или вверху справа значок камеры.

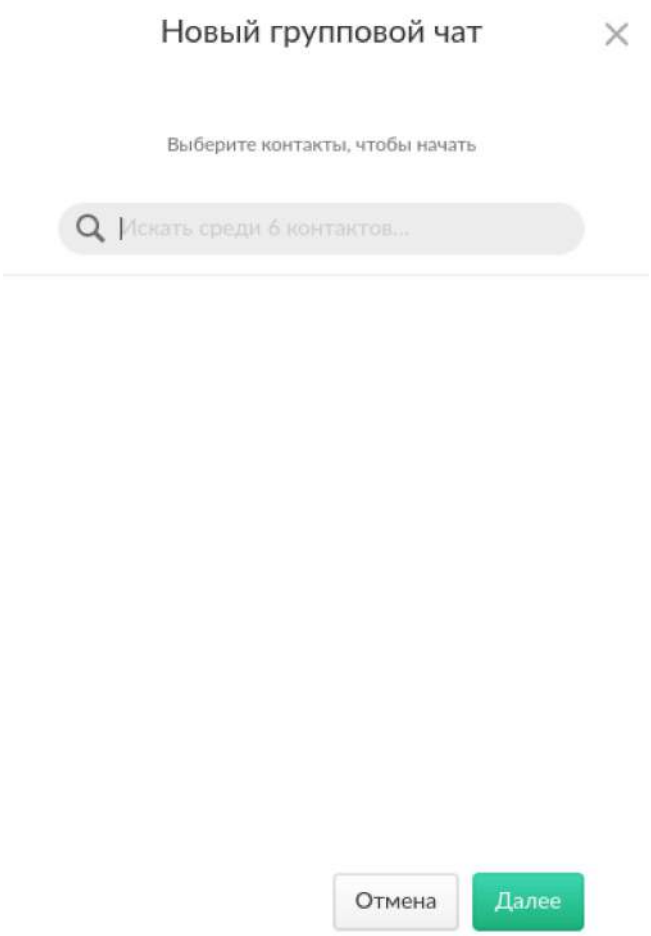


На этом с основными функциями связи с отдельными собеседниками закончили.

В MEGA также есть возможность организовывать групповые чаты и вести аудио и видеоконференции. Чтобы создать группу, нажимаем на зеленый значок с плюсом вверху справа и надписью «Новый чат» и выбираем «Новый групповой чат».

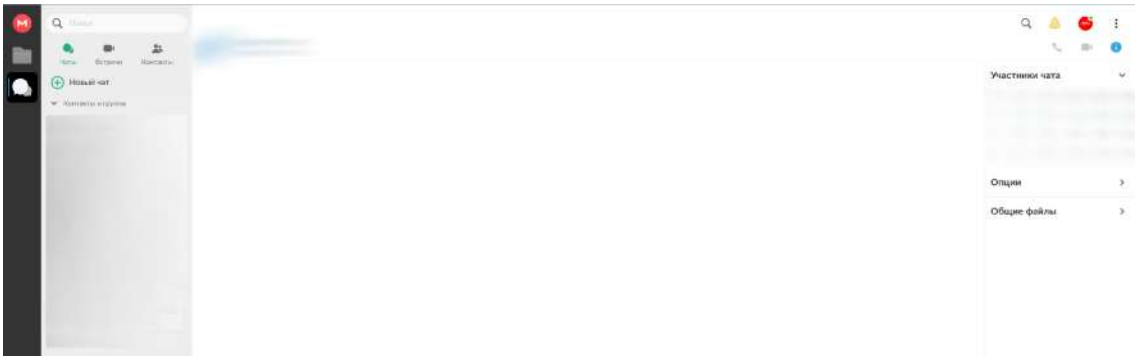


Необходимо указать собеседников, которых вы хотите включить в нее, после чего нужно нажать кнопку «Далее».



После этого необходимо ввести название группы и нажать кнопку «Создать».

Группа появится в общем списке собеседников слева. Чтобы начать общение в группе, нужно нажать на нее. Отправка сообщений и файлов осуществляется здесь также как и при общении с отдельными собеседниками. Для запуска конференции, нажмите на значок трубки вверху справа. Для запуска видеоконференции, нажмите на значок камеры там же.

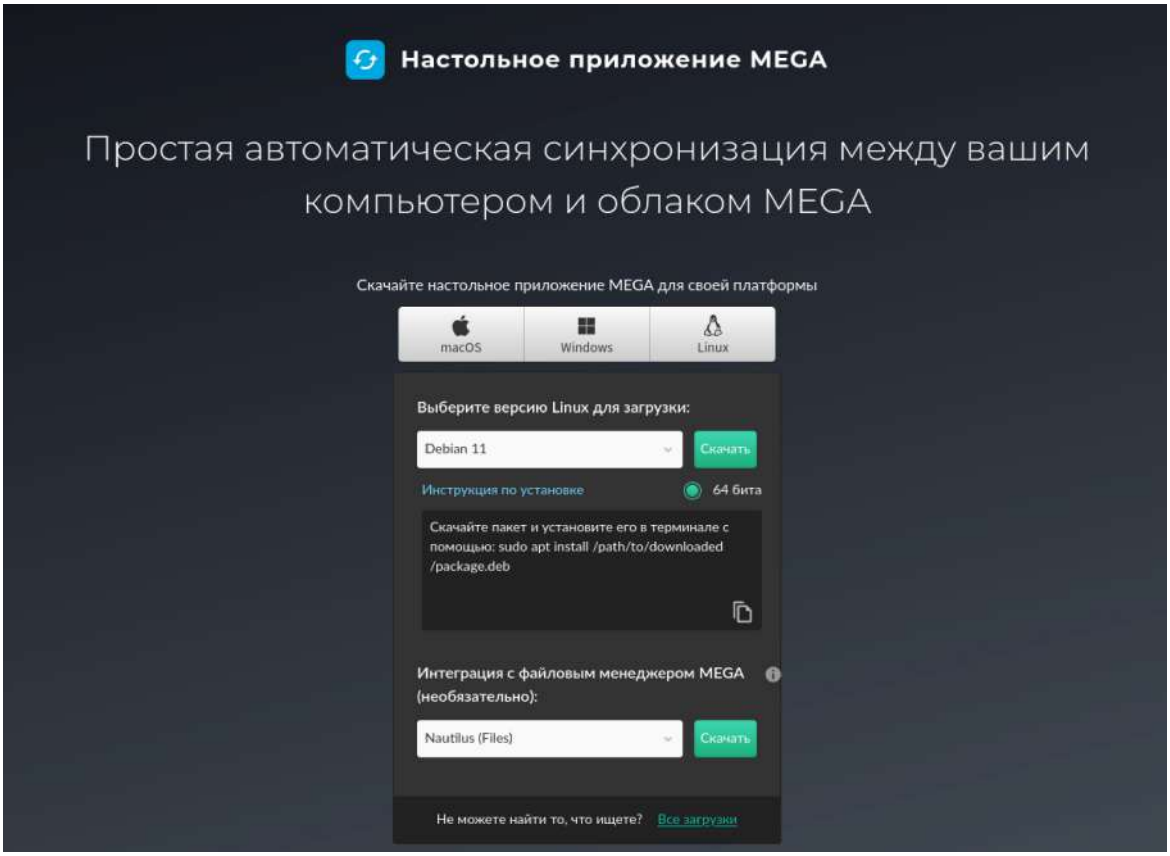


Это все основные функции общения через данный сервис.

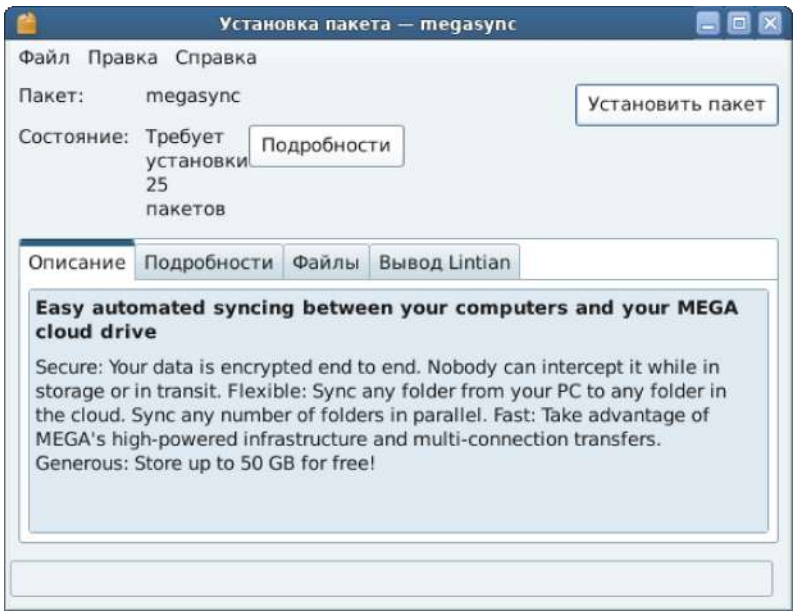
30 Программа синхронизации MEGA

У MEGA есть также программа синхронизации данных между вашим устройством и удаленным хранилищем. С помощью нее возможно загружать и выгружать файлы из хранилища, манипулируя ими в папках на вашем компьютере, синхронизируемых с папками хранилища. Есть также возможность без такой синхронизации загружать файлы на сервер и скачивать их.

Чтобы установить данную программу, идем в раздел «Платформы» и выбираем «Настольное приложение MEGA». На открывшейся странице указываем тип операционной системы «Linux» и выбираем версию дистрибутива Debian 11. После чего нажимаем «Скачать».

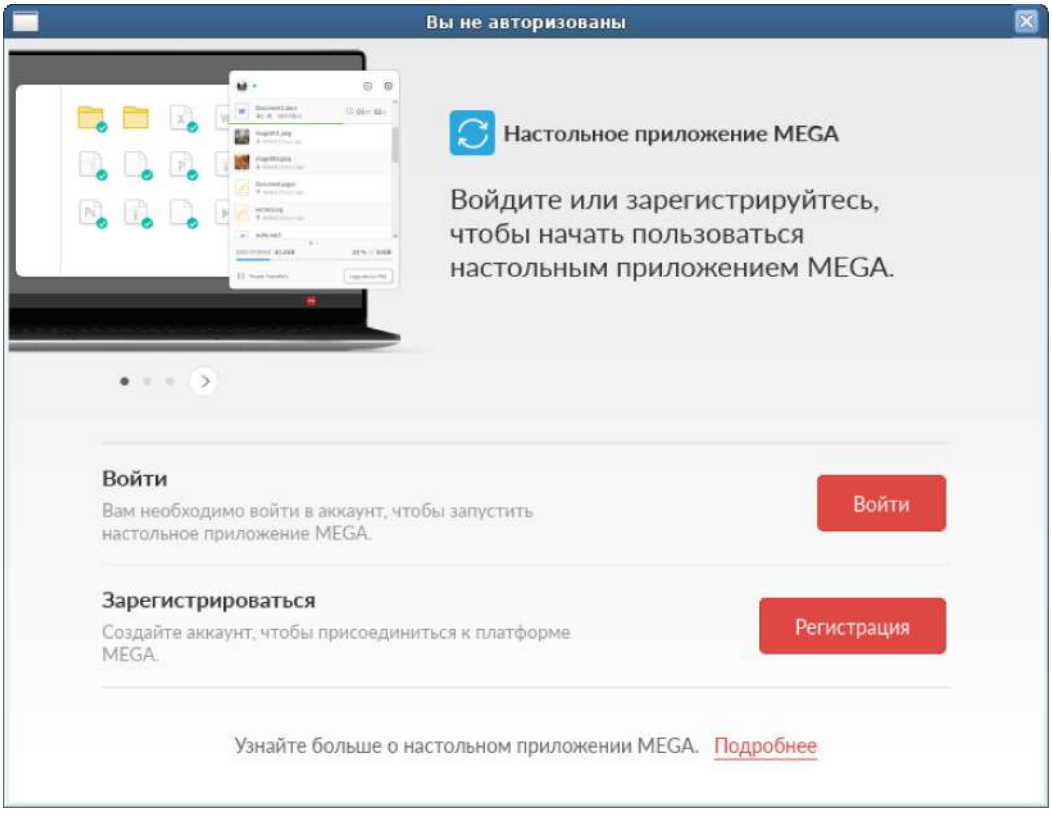


После скачивания идем в Меню, категория «Система» и выбираем GDebi. В окне программы нажимаем «Файл» вверху слева, затем «Открыть», в открывшемся окне выбираем скачанный файл и нажимаем «Открыть». После того, как закончится проверка зависимостей, нажимаем на кнопку «Установить пакет» справа.

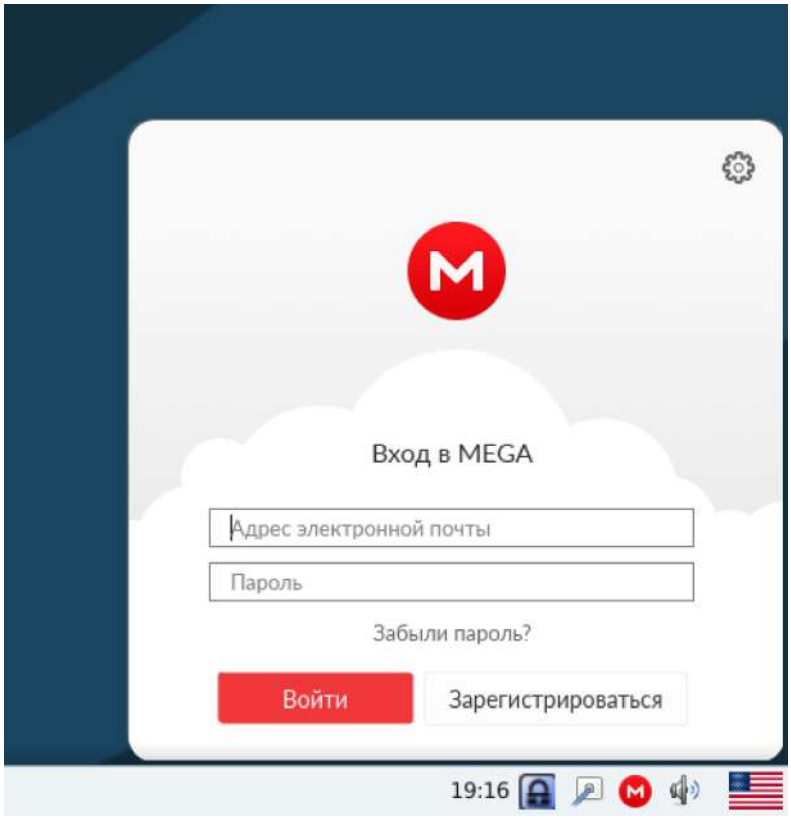


После окончания установки окно можно закрыть.

Чтобы запустить программу, идем в Меню, категория «Интернет» и выбираем MEGA. Откроется окно, где будет предложено войти или зарегистрироваться. Поскольку у нас уже есть аккаунт, нажимаем «Войти».



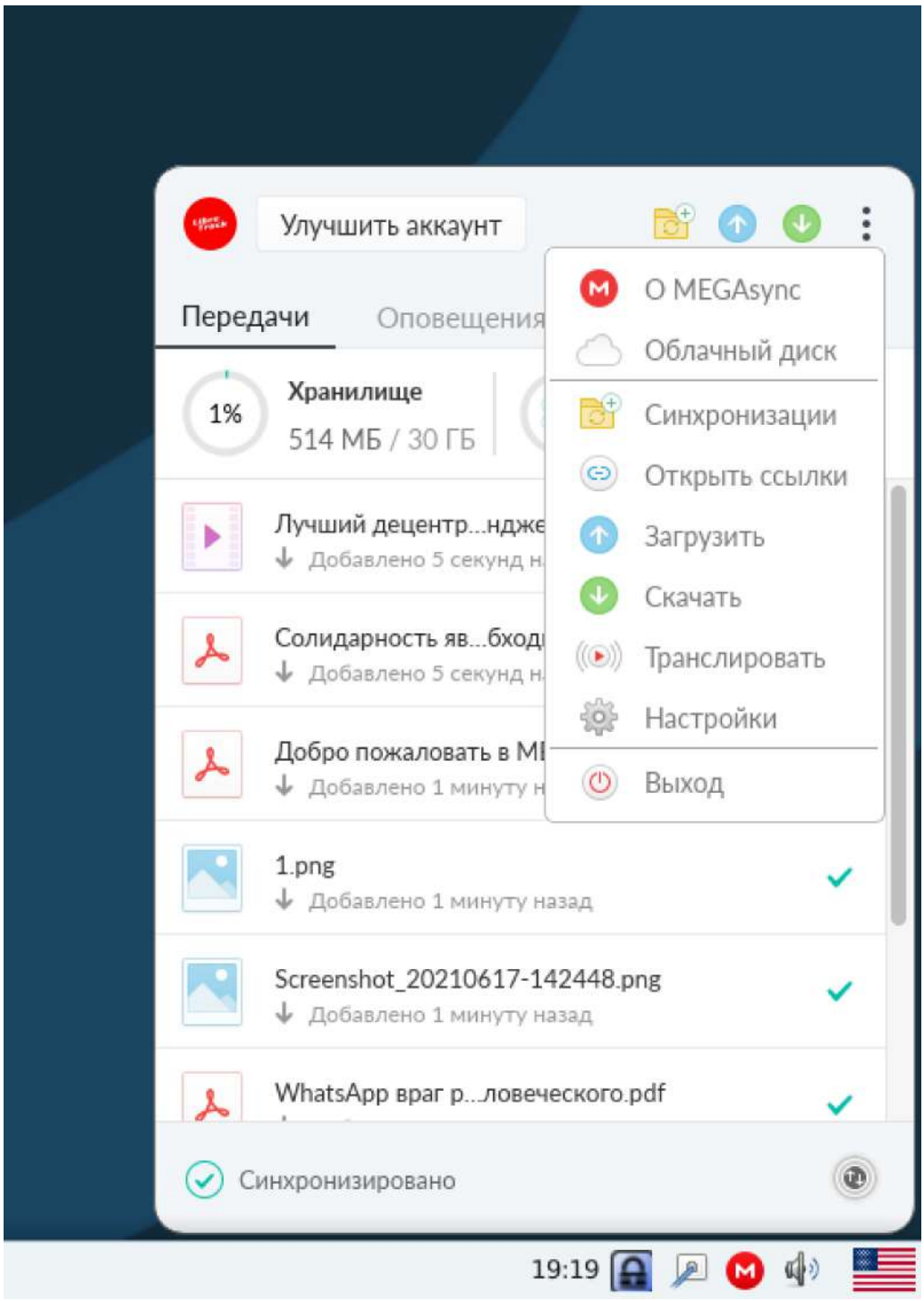
Появится значок программы на нижней панели справа с открывшемся окном авторизации. Вводим данные и нажимаем «Войти».



После авторизации в открывшемся окне можем выбрать либо полную синхронизацию, либо выборачную. В случае полной синхронизации в вашей системе в пользовательском каталоге буде создана папка MEGA, в которой будут присутствовать все папки и файлы, которые лежат у вас в удаленном хранилище. Имейте ввиду, что большое количество информации требует большого дискового пространства. Если у вас объем информации измеряется гигабайтами, то виртуальный диск все это не вместит. При выборочной синхронизации потребуется самостоятельно создать и назначить папки для синхронизации. Этот процесс может запутать. Выбирайте то, что вам больше подходит. Вы всегда можете отключить синхронизацию в программе.

При нажатии на значок программы на нижней панели справа, выскакивает окно, где показаны загруженные файлы.

При нажатии на три точки вверху справа открывается меню, где можно выбрать «Настройки».



В открывшемся окне во вкладке «Синхронизация» можно отключить синхронизацию папок.

Чтобы добавить новую синхронизацию нажмите на значок папки с плюсом и назначьте соответствующие папки.

Чтобы загрузить файл в хранилище, нажмите на синий значок стрелки вверх. В открывшемся окне выберите файлы, которые хотите поместить в

хранилище и нажмите «Открыть». В новом окне выберите папку, в которую хотите поместить файлы и нажмите «Загрузить». Начнется процесс загрузки.

После того, как файлы будут помещены на сервер, если навести курсор мыши на них в поле программы, то справа появится значок, нажав на который можно одним нажатием скопировать ссылку на добавленный файл.

Чтобы скачать файл из своего хранилища, нажмите на зеленый значок со стрелкой вниз. В открывшемся окне выберите нужные файлы и нажмите «Скачать».

На этом с основным функционалом данной программы закончено.

31 Перенос файлов между системами

Необходимо осветить вопрос перемещения файлов между гостевыми и основной системами. Ведь может возникнуть необходимость перенести файл из основной в гостевую, например, чтобы переслать его по почте. Или наоборот, скачанный из Интернета в гостевой системе файл перенести в основную.

Существуют разные методы взаимодействия между системами. Один из них, это общий буфер обмена. Он реализуется достаточно легко, однако совершенно неприемлем с точки зрения безопасности. Существуют различные пути получения доступа к буферу в случае взлома или заражения системы вирусом. Таким образом, общий буфер обмена становится дыркой между системами, сводящей на нет все преимущества использования виртуалок.

Еще одним вариантом является двухуровневый буфер обмена. В этом случае, у каждой системы буфер обмена остается изолированным. При этом он связан с общим буфером, который находится как бы вне систем. Таким образом, использовать стандартные уязвимости, связанные с буфером обмена, для проникновения из виртуалки в основную операционную систему уже не получится. Такой вариант реализован в системе Qubes, о которой я еще скажу в дальнейшем. Он гораздо более надежный. Однако, во-первых, я не представляю как его реализовать на пользовательском уровне. Во-вторых, все равно остается эдакая щель между системами, через которую теоретически можно проникнуть из виртуальной машины в основную систему.

Куда более безопасным вариантом представляется перенос файлов с помощью флешек. Поскольку флешка подключается только непосредственно в момент, когда необходимо перенести на нее или с нее копию, постоянной дыры между системами нет.

Для того, чтобы подключить флешку к виртуальной машине, необходимо вставить ее в порт USB, затем в окне виртуалки нажать «Виртуальная машина» вверху и выбрать «Перенаправление USB». В открывшемся окне со списком подключенных устройств, среди которых могут быть клавиатура (keyboard) и мышь (mouse), необходимо указать флешку. После этого она появится в виртуальной машине. Отсоединяется она также как и в основной системе, нажатием на значок извлечения рядом с ее названием в файловом менеджере. Таким образом, подключив флешку к виртуалке, можно скопировать на нее файлы, отключить ее, а затем присоединить к основной системе и перенести файлы в нее. И наоборот, подсоединив к компьютеру флешку, перенести в основной операционной системе на нее файлы, затем подсоединить ее к виртуальной машине и скопировать файлы в нее.

Однако, этот вариант также нельзя считать абсолютно безопасным, поскольку существуют уязвимости, связанные с USB.[10] Эти уязвимости связаны, главным образом, с вирусами. Если в ходе Интернет-серфинга система оказалась заражена, при подключении флешки к ней, вирус может проникнуть на нее. И когда, затем накопитель будет подключен к основной системе, вирус может перенестись в нее. Конечно, системы GNU/Linux имеют крайне высокую устойчивость к вирусам, однако существует зараза, которая способна поражать и их. Такие вирусы большая редкость, но все же они есть.[11] Конечно, в борьбе с ними возможно использовать свободные антивирусы, которые также существуют.[12] Однако, необходимо помнить, что далеко не каждый вирус может быть выявлен такими инструментами. Кроме того, бывают случаи, что они определяют как вирусы программы, которые ими не являются. Поэтому полагаться лишь на них не стоит.

От тех вирусов, что сливают информацию, спасает отсутствие постоянного подключения к Интернету, которое мы и обеспечиваем в основной операционной системе. Еще одной мерой защиты является отключение автозапуска, поскольку большинство вирусов активизируются именно эксплуатируя этот инструмент. Для отключения необходимо в файловом менеджере нажать «Правка» вверху и выбрать «Параметры». Далее во вкладке «Носители» снять галочку с «Просматривать носители при вставке». Также поставить галочку на «Никогда не спрашивать и не запускать программы при вставке носителей». Или в графе «Программы» указать «Ничего не делать» или «Спрашивать, что делать». Последнее позволит вам определить наличие вируса,

если выскочит сообщение с вопросом о запуске программы при подключении носителя, если вы сами на него никаких исполняемых файлов не помещали. Эти меры позволят предотвратить последствия от многих вирусов.

Правда после ручного запуска, когда вы откройте флешку в файловом менеджере, чтобы перенести файлы, вредоносный код также может начать исполнятся. Для предотвращения негативных последствий этого можно запускать файловый менеджер в песочнице, т.е. среде, изолированной от основной системной среды. Для этого можно использовать программу Firejail с графическим инструментом Firetools, которые есть в репозиториях Trisquel. С помощью него можно запускать в песочнице различные программы, в том числе и файловый менеджер, в котором необходимо открыть флешку.[13] После этого, файлы можно переносить, а вредоносный код при этом будет выполнятся в среде, из которой он не доберется до системных и пользовательских файлов. Конечно, если переносимые вами файлы заражены, то это уже другой случай. Но тут можно только порекомендовать ничего не скачивать с сомнительных ресурсов. А если скачать все же необходимо, то не переносить это в основную систему.

Таким образом, использование флешки для переноса файлов между системами, при условии отключения автозапуска, можно считать безопасным.

32 Рекомендации по обновлению основной и гостевых ОС

На этом настройка виртуальной машины для публичной Интернет-активности завершена. Осталось перезагрузить, на всякий случай, и почистить ее с помощью Bleachbit. После этого, сделать снапшот (снимок системы), и после каждой Интернет-прогулки откатывать состояние виртуалки к этому снапшоту. Предыдущие снапшоты можно удалить, чтобы не занимать место. Я рекомендую где-то раз в месяц производить обновление гостевой операционной системы. После этого обновления производить перезагрузку, затем обновлять расширения в браузере, для чего в Firefox в меню нужно нажать «Дополнения» и в правом верхнем углу нажать на стрелку, после чего выбрать «Проверить наличие обновлений». Когда обновления будут произведены, рекомендую сменить шум графического отпечатка, для чего нужно нажать значок расширения Canvas Defender Fingerprinting и сгенерировать новый шум. Затем, после закрытия браузера, произвести чистку и сделать новый снапшот, и в дальнейшем уже к нему откатывать виртуалку после Интернет-прогулок. Во

время всех этих процедур лучше не лазить ни по каким сайтам, чтобы ничего лишнего не залетело в систему и не сохранилось в ней при создании снапшота. Общая схема регулярного обновления выглядит так, после того, как все виртуалки обновлены выше описанным образом, делается снимок состояния основной операционной системы с помощью TimeShift, затем производится обновление основной операционной системы (предварительный снимок является страховкой от потери установленных обновлений в виртуалках, в случае некорректного обновления основной операционной системы), далее следует перезагрузка, за ней обновление расширений в браузере основной ОС, потом делается ее чистка и снимок. Таким образом, ваша основная операционная система и виртуальные машины будут всегда поддерживаться в актуальном состоянии.

33 Обновление Devuan до новой версии

Также как и у Trisquel, существует способ обновить Devuan до более новой версии, когда та выпускается. Также как и в случае Trisquel успешная работа системы после такого обновления не гарантируется. Тем не менее, методику я покажу.

В первую очередь необходимо полностью обновить и почистить Devuan. Затем после перезагрузки, нужно пройти в репозитории через Synaptic и заменить название нынешней версии дистрибутива на название новой. После чего произвести обновление системы, так же как производится обычное.

По ее окончанию нужно будет перезагрузить компьютер и можно начинать работать в новой версии системы.

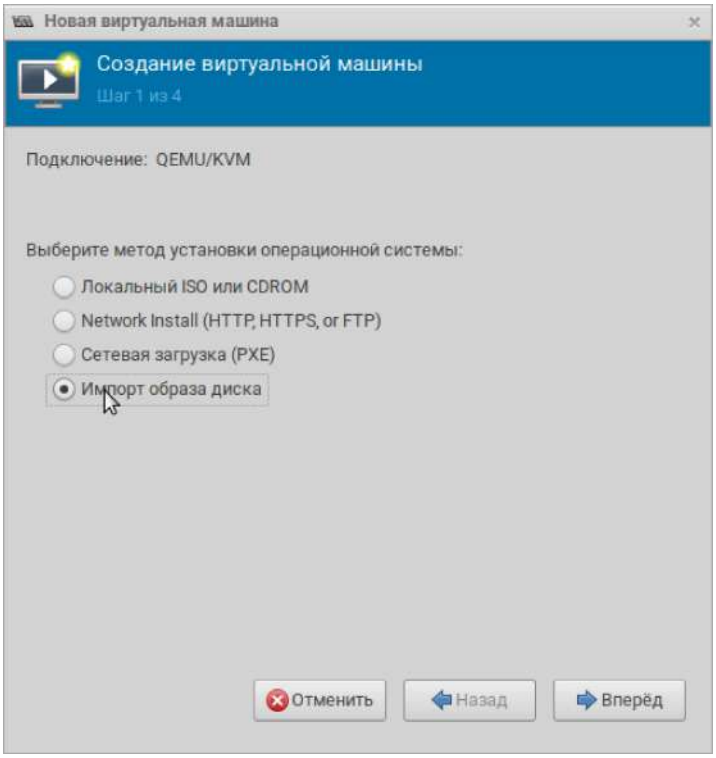
34 Копирование виртуальных машин

Иногда возникает необходимость перенести уже созданную виртуальную машину в другую операционную систему. Сделать это не очень сложно. Прежде чем приступать к копированию, я рекомендую обновить и почистить гостевую систему. После чего, крайне важно, удалить все снапшоты. Для копирования виртуалки достаточно скопировать виртуальный жесткий диск. Образ этого диска содержит, в том числе, все снимки системы. И если его перенести в новую операционку, то при создании новых снопшотов и откате к ним, система будет возвращена в состояние в котором она была скопирована, а не к состоянию, зафиксированному в новых снимках системы.

После удаления всех снапшотов, открываем терминал, переходим в учетную запись суперпользователя и открываем файловый менеджер, набрав в терминале caja. Затем идем в корневой каталог, потом в папку var, затем lib, потом libvirt, далее images и здесь находим по названию виртуальный диск нужной системы. После чего просто копируем его на какой-нибудь носитель, с помощью которого он будет перенесен в другую операционную систему.

В системе, в которой предполагается развернуть скопированную виртуалку, виртуальный диск нужно поместить в папку по тому же пути, по которому он находился в системе из которой он скопирован. Все это также делается с правами суперпользователя.

После этого открываем Менеджер виртуальных машин и нажимаем «Создать». В открывшемся окне выбираем «Импорт образа диска».



Нажимаем «Вперед». Далее нажимаем кнопку «Обзор» и в открывшемся окне выбираем скопированный виртуальный диск. Указываем в качестве операционной системы ту, которую указывали при создании диска, которая в наибольшей мере соответствует гостевой операционной системе. Затем проходим остальные этапы создания виртуалки, также как и при создании новой машины.

После того, как машина будет запущена, это будет та самая виртуалка, которая была в системе, из которой была взята. На этом копирование закончено.

5 Шлюз для туннелирования трафика

35 Средства анонимизации трафика

Как уже было сказано, для обеспечения полноценной приватности в Интернете, необходимо использовать туннелирование. Напоминаю, что туннелирование позволяет нам скрывать от различных шпионов то, к каким Интернет-ресурсам мы обращаемся, а также скрывать от этих ресурсов свои атрибуты, такие как ip-адрес, чтобы они не могли установить кто мы. Осуществляется это за счет пропускания запросов от нас до ресурса через промежуточные узлы.

Существуют разные технологии, обеспечивающие это самое туннелирование. Самый старый и простой тип, это прокси-сервер. На самом деле прокси называется любой промежуточный сервер. То есть, когда мы будем говорить о других технологиях, мы по сути, по-прежнему будем говорить о прокси, в роли которых выступают сервера, реализующие какие-то другие технологии. Так что же имеется ввиду, когда говорится просто о прокси? Имеются ввиду такие промежуточные сервера, которые не реализуют никакие другие технологии. То есть те, которые не являются ни VPN-сервером, ни SSH-сервером, ни узлом сети Tor, ни чем бы то ни было еще кроме узла, через который производятся запросы с других устройств (обо всех упомянутых технологиях мы поговорим дальше). Иногда отмечается, что отличие прокси от других технологий, это отсутствие шифрования по пути от нашего устройства до сервера. На самом деле, это не совсем так. Видов прокси довольно много, и действительно, некоторые из них не шифруют трафик, например http-прокси. Но есть и те, которые этот трафик шифруют, например https-прокси.[14]

Такими простыми прокси мы пользоваться не будем. Если говорить о тех типах прокси, которые не шифруют трафик, то тут причину и пояснять не нужно. Что касается тех, которые шифруют, то по сегодняшним временам эта технология все же не очень надежна. Кроме того, прокси, к которым можно было бы получить доступ бесплатно, во всяком случае надежных, я не встречал.

Еще одна технология, позволяющая реализовать туннелирование, это VPN — виртуальная частная сеть.[15] Это внутренняя приватная сеть, формируемая VPN-сервером. Компьютеры, находящиеся в этой сети, выходят в Интернет через этот сервер. По сути, VPN-сервер выступает как прокси. Трафик в такой сети всегда шифруется. Подключаться к этой сети компьютеры могут как по локальной, так и по глобальной сети. Как было сказано, трафик в такой сети всегда шифруется, а значит, когда вы обращайтесь к какому-то ресурсу через VPN-сервер ваше соединение до этого сервера всегда защищено. Соответственно, если подключайтесь через Интернет, ни провайдер, ни другие следящие системы не смогут прочитать содержимое вашего трафика. Возвращаясь к вопросу о том, чем отличается прокси от других технологий, способных выполнять схожие задачи, следует заметить, что в Интернете можно встретить такое заявление, что VPN и прокси, это одно и тоже, только VPN шифрует трафик, а прокси нет.[1] Это не верно. Как уже было сказано, прокси точно также может шифровать трафик. Разница в том, что прокси никакой внутренней сети не формирует, а является просто перевалочным пунктом. Когда же VPN используется в качестве перевалочного пункта, она выступает в роли прокси, хотя суть технологии совсем в другом — в создании приватной сети.

Существует огромное количество коммерческих предложений подключения к VPN именно с целью анонимизации трафика. Компании, предоставляющие такие услуги, как правило клянутся, что не собирают о вас никаких данных, а если и собирают то не используют их в коммерческих целях и не сдают властям даже по запросам. В абсолютном большинстве случаев, это ложь. Ведь во многих случаях для подключения к такому серверу пользователю необходимо идентифицировать себя, прямо, указывая свои личные данные при заключении договора на оказание услуг, или косвенно, указывая при регистрации свой телефон или почту. Кроме того, палево присутствует и при оплате, так как счета, обычно привязаны к личным данным. Да и сам факт того, что эти сервисы платные уже может создать проблему для многих. Свидетельства того, как VPN-провайдеры шпионят за своими пользователями также имеются.[2]

Существуют, конечно, порядочные VPN-серверы, радеющие за свободное общество, не требующие идентификации от своих пользователей. В основном это некоммерческие проекты, живущие на пожертвования и гранты. К сожалению, стабильных таких проектов крайне мало.

Однако существуют и непродолжительные проекты подобного рода, организуемые различными компаниями, институтами и энтузиастами по всему миру. Несмотря на то, что найти среди них стабильный долгоживущий VPN крайне трудно, они достойны внимания и нам пригодятся.

Еще одна технология туннелирования, это SSH.[3] Данный протокол используется для удаленного подключения к компьютеру. В этом случае, компьютер, к которому подключаются, называется сервером, а тот, который подключается, клиентом. Технология SSH специально создана для обеспечения защищенного соединения между устройствами. Вся передаваемая информация шифруется. То есть, если с помощью SSH подключиться к удаленному компьютеру и уже с него осуществлять выход в сеть, те кто следит за вашим соединением будут видеть шифрованный трафик, идущий на какой-то узел, но не будут видеть ресурс, на который вы идете за этим узлом. В свою очередь, ресурс, к которому вы обращайтесь, будет видеть ip и другие атрибуты SSH-сервера, через который вы на него выходите, и ваши идентификаторы останутся ему не видны. То есть, SSH-сервер выступает в роли прокси.

Туннелирование с помощью SSH не менее надежно чем с помощью VPN. Однако данной технологией мы пользоваться не будем, поскольку мне не известно публично доступных SSH-серверов.

Итак, прокси-сервера ненадежны и труднодоступны. VPN надежны и их можно найти в открытом доступе, хотя такие сервера, как правило, нестабильны. SSH надежны, но труднодоступны. Из всех этих технологий, как видно, обратить особое внимание стоит только на VPN.

Однако, VPN все же нельзя использовать в качестве основного инструмента для анонимизации трафика. Дело в том, что при использовании одиночного VPN, хоть те, кто шпионит за вашим соединением и не будут видеть, куда вы гуляйте в Интернете, а Интернет-ресурсы не увидят кто их посещает, сам сервер видит и вас и то, куда вы направляйте запросы. Большинство VPN-сервисов хранят логи, в которых записываются сведения о работе сервера, в том числе, кто, когда и куда ходил через этот сервер. Если поставщик VPN сам является мошенником (такое теоретически может быть), использование его сервера создаст опасность для ваших данных. Также он может быть просто недобросовестным, и сотрудничать с теми, кто к нему обратиться за данными пользователей. Он может стать жертвой шантажа или подкупа. В конце концов, сам сервер может быть взломан и скомпрометирован

злоумышленниками.

Для предотвращения деанонимизации в подобных ситуациях, в принципе, можно использовать два VPN. Кстати, в сети существуют предложения подключения по технологии DobleVPN, то есть перенаправления вашего трафика последовательно через два VPN-сервера. Смысла в этом нет, поскольку, если оба сервера принадлежат одному и тому же поставщику, в выше обозначенных ситуациях, вас это не спасет. Кроме того, при такой организации, трафик сохраняет однослойное шифрование. То есть данные шифруются до первого VPN-сервера, на нем расшифровываются, зашифровываются повторно по пути до второго сервера, и уже после него идут на запрашиваемый ресурс. [4] Очевидно, что надежнее было бы, если бы шифрование было многослойным. То есть внутри шифрованного запроса к первому серверу, уже был бы зашит шифрованный запрос ко второму серверу. Таким образом, на уровне вашего соединения имелось бы два слоя шифрования. То есть, каскад из двух VPN был бы организован по, так называемой, технологии ParallelVPN.[5] И здесь опять же важно, чтобы сервера принадлежали разным поставщикам. В этом случае, первый VPN-сервер будет видеть вас, но дальше он будет видеть, что запрос идет на еще какой-то сервер, но не увидит ресурс, к которому вы обращайтесь за ним. Второй, в свою очередь, будет видеть ресурсы, на которые идут запросы, но кто их посещает останется ему неизвестным, потому, что он будет видеть, что они идут с какого-то сервера.

Однако, при использовании подобной схемы всплывает другая проблема. Как я сказал, VPN-сервера, не требующие регистрации, как правило нестабильны, и вы замучайтесь регулярно искать новые сервера, для последовательного соединения, и для каждого переписывать правила в файерволе, поскольку важно, чтобы при обрыве одного из серверов, трафик не пошел напрямую, и не спалил вас перед другим сервером, или не спалил ресурсы, которые вы посещайте перед тем сервером, коему видны непосредственно вы. Да, при таком подключении, важно настроить файервол на обрыв всего Интернет-соединения, при потере связи с одним из VPN-серверов. И, как я сказал, при каждом обрыве такого соединения, вам придется проверять, какой именно сервер отвалился, первый или второй, перенастраивать файервол, для поиска нового сервера, искать его, затем снова перенастраивать межсетевой экран. Ни о какой даже просто приемлемой в отношении комфорта работе, говорить не приходится. Значит необходимо обратить пристальное внимание на

другие средства анонимизации. И такие средства есть.

Существует инструмент, позволяющий перенаправлять трафик сразу через несколько узлов, обеспечивающий многослойное шифрование, при этом являющийся свободным ПО. Именно такой инструмент нам и нужен. Он называется Tor.

36 Луковая маршрутизация

Tor, это технология луковой маршрутизации. Трафик с компьютера шифруется последовательно тремя ключами и перенаправляется через цепочку из трех прокси-серверов, на каждом сервере, происходит расшифровка одного слоя шифрования, этот слой как бы снимается, словно у лука, почему технология и называется луковой маршрутизацией. Сеть из таких узлов Tor распределена по всему миру и насчитывает по меньшей мере тысячи. Чтобы подключиться к этой сети, достаточно установить и настроить специальное ПО, которое является свободным.[6]

На самом деле, цепочка узлов может составлять больше трех, или наоборот меньше, но для этого необходимо провести дополнительные настройки подключения, к тому же цепочка из трех серверов наиболее оптимальная.

К сожалению, вокруг технологии Tor сложилось много мифов. Далее я их разберу, а заодно поближе познакомлю вас с этой технологией.

37 Разоблачение мифов о Tor

Проект Tor, возник из разработок, проводимых Военно-морской исследовательской лабораторией США. В дальнейшем его рассекретили, и исходные коды были опубликованы под свободной лицензией.[7] Так и возник этот инструмент сетевой анонимности. И поскольку у истоков проекта стояли военные разработки, многие посчитали, что он был специально пущен в массы, как дополнительное средство контроля. Что якобы его государственные и военные структуры США используют для слежки за теми, кто им пользуется. Масла в огонь подливает и тот факт, что внушительную долю финансирования проекта Tor, осуществляет как раз Министерство обороны и Государственный департамент США.[8] Что ж, давайте разберемся, насколько обоснованы эти подозрения.

То, что этот инструмент изначально разрабатывался для военных целей, никак не говорит о том, что сейчас это проект слежки. Множество разработок,

которые когда-то проводились в военной сфере в дальнейшем стали вполне мирными и вошли в обиход простых граждан. Считать, что Tor является средством американских спецслужб нет никаких оснований. По такой логике сам Интернет необходимо считать средством, существующим для одной лишь слежки и контроля, ведь изначально он разрабатывался для военных целей. Кроме того, как было сказано, Tor является свободным программным обеспечением,[9] и любой может проверить его действительный функционал.

Конечно, невозможно проверить что творится на отдельных серверах, распределенных по миру, но так как сервер поднять может любой, нельзя их считать поголовно скомпрометированными. Многие узлы (иначе называемые нодами) поднимаются различными организациями (в том числе правозащитными), институтами и энтузиастами по всему миру. Некоторые, возможно, и впрямь принадлежат спецслужбам. Но вероятность нарваться на все такие ноды в цепочке исчезающе мала. Поскольку шифрование происходит на вашем компьютере, вашей копией ПО, которую вы всегда можете проверить (к слову, если вы скачивайте ее из официальных репозиториев такой системы как Devuan, можно быть вполне уверенным, что с ней все в порядке), невозможно «раскрутить» всю цепочку, скомпрометировав только один узел. В случае компрометации входного узла, ему не будет известно не только к каким ресурсам вы обращайтесь, но даже через какой узел Tor, вы это делайте, поскольку он видит только вас и промежуточный узел. Если будет скомпрометирован промежуточный узел, ему не будут известны ни ваши идентификаторы, вроде ip, ни то, к каким ресурсам вы обращайтесь, поскольку он видит только входной и выходной узлы. Если же будет скомпрометирован выходной узел, ему будут оставаться неизвестными не только ваши идентификаторы, но и то, через какой узел вы входите в Tor. Правда, ему будут видны ресурсы, к которым вы направляйте запросы, и если эти ресурсы работают не по шифрованному протоколу, выходной узел может увидеть передаваемые данные. С этим связан еще один миф, что выходной узел знает о вас все. Это не так. Вас он не видит, и не знает, кто обращается к конкретным ресурсам. Но если вдруг вы по не шифрованному каналу передадите какие-то личные данные, вы можете быть деанонимизированы.[10] Как избежать подобного будет сказано в дальнейшем. Ну а вероятность того, что вы нарветесь на два и тем более все три узла, скомпрометированные одними и теми же злоумышленниками, как уже было сказано, исчезающе мала. Кроме того, у

самого Tor, есть средства защиты от этого.[11]

Финансирование же проекта Tor государственные органы США осуществляют, поскольку могут использовать свободную анонимную сеть для своих целей. Например исследовательских задач, а также для коммуникации. Поскольку Tor может пользоваться кто угодно, сотрудник спецслужб, осуществляя связь через него, может раствориться в море пользователей и сохранить конспирацию.

Также существует миф, что Tor ненадежен в отношении безопасности, и его пользователей легко деанонимизировать. Действительно, деанонимизация становится возможной, если пользователи не применяют виртуализацию, при этом используя java-скрипты, WebRTC, Flash, Java. Также, осуществляя в одной среде как публичную, так и приватную активность, не очищают cookie-файлы, кеш и т.д.[12] В общем, зачастую причиной деанона становится простая безграмотность пользователей. Tor не волшебная панацея, он обеспечит вам защиту только в совокупности с другими средствами, такими как виртуализация, с разделением среды, подключаемой к Интернету и той, в которой осуществляется активность (об этом будет сказано в дальнейшем). Конечно существуют сложные и затратные схемы по деанонимизации пользователей непосредственно в сети Tor. Например, метод глобального пассивного наблюдения. Для его осуществления необходимо создание огромного количества узлов, которые будут собирать и систематизировать данные о проходящем трафике. Это позволит выявить корреляции, что может способствовать установлению реальных данных подключения пользователя и деанонимизировать его. Точность метода зависит от количества следящих узлов.[13] Однако, во-первых, этот метод требует больших ресурсов и потенциально доступен только очень серьезным структурам. Во-вторых, держать крупную сеть следящих нод продолжительное время, для обеспечения постоянной слежки, даже для таких структур может оказаться неподъемной задачей. В-третьих, существуют инструменты позволяющие если не полностью предотвратить эту угрозу, то как минимум, серьезно затруднить ее осуществление.[14] Также существуют тайминг-атаки.[1] Этими атаками часто пугают при разговоре о надежности Tor, однако, мне не известно реальных случаев их применения. Они хорошо работают в теории и в лабораторных условиях, но случаев успешного деанона в реальной среде с помощью них, я не нашел. В любом случае, даже у очень серьезных структур не хватит средств,

раскручивать подобными методами хоть сколько-нибудь широкий круг пользователей, что уж говорить о простых взломщиках.[2]

Еще один миф заключается в том, что подключаясь к сети Tor, ваше устройство якобы само становится нодой, через него начинает проходить трафик других пользователей, и если кто-то через вас что-то взломает или осуществит другое незаконное действие, проблемы могут быть у вас. Это не так. Подключаясь к сети Tor, вы не становитесь автоматически его узлом. Вы просто пользователь. Для того, чтобы ваше устройство стало ретранслятором, его необходимо целенаправленно настроить, и если вы этого специально делать не будите, в ретрансляции ваше устройство и не будет участвовать. Кроме того, как уже было сказано, через узлы Tor трафик передается в зашифрованном виде, поэтому, даже если вы настроите свое устройство в качестве ретранслятора, проходящий через него трафик будет зашифрован, и невозможно будет определить, какие данные через вас передаются. Исключением являются только выходные ноды, на которых происходит окончательная расшифровка трафика. И действительно были случаи, когда владельцев выходных нод задерживали по подозрениям в незаконных действиях.[3] Для промежуточных нод таких случаев не известно. А настройка выходной ноды, еще более сложна и нетривиальна, так что если вы ее специально настраивать не будите, боятся вам нечего.

Ну и пожалуй наиболее популярный миф, что у сети Tor низкая скорость. Сама по себе технология Tor не имеет ограничения по скорости, но вы можете нарваться на одну или несколько нод в цепочке, имеющих низкую пропускную способность. В этом случае, скорость действительно будет небольшой. Также важно понимать, что быстро и медленно, понятия относительные. Если вы живете в продвинутом городе и привыкли к скоростям в 100, 150 и более Мбит/с, то скорость, которую может выдать сеть Tor, несопоставима с этим. Лично я обозначил для себя величину скорости, ниже которой уровень комфорта работы становится неприемлемым и ориентируюсь на нее. Это

величина 4 Мбит/с. Это та скорость, при которой возможно спокойно, без тормозов смотреть в Интернете видео в HD качестве. Какие же скорости способен выдать Tor? На сегодняшний день уверенно можно говорить о 5–10 Мбит/с. Подчеркиваю, эта та скорость, о которой можно говорить уверенно. Ниже 5 Мбит/с я давно не видел. Очень часто можно увидеть 15 Мбит/с. И все чаще я начинаю наблюдать около 20 Мбит/с. Ну а рекорд, который лично я наблюдал, был около 25 Мбит/с. Таких скоростей хватает, чтобы смотреть видео в хорошем качестве, параллельно что-то скачивать и еще серфить, открывая новые страницы.

Я разобрал все известные мне мифы о Tor. Конечно, как уже было сказано, Tor не панацея, и для достижения действительно высокого уровня безопасности необходима грамотная организация подключения к Сети. Это касается, как подключения в целом, так и доступа непосредственно к Tor.

38 Предотвращение детектирования подключения к Tor

Основной минус Tor, это палево факта его использования, поскольку ip-адреса его узлов находятся в публичном доступе. За счет этого он уязвим к способам блокирования. В некоторых странах осуществляется блокировка доступа к сети Tor. В других, отдельные провайдеры могут осуществлять такую блокировку. Но даже без подобной цензуры, плохо уже само по себе то, что те, кто шпионит за вашим соединением, видят факт использования этой сети. Это может вызвать необоснованные подозрения, поскольку к сожалению, усилиями безответственных и безграмотных журналистов и блогеров, в общественном сознании укоренилось представление о том, что данной сетью пользуются сплошь криминальные элементы. Конечно, это совершенно не так. Данной сетью пользуются те, кому на себя не наплевать, а уголовников там не больше чем в поверхностном Интернете. Тем не менее, лучше предпринять меры по сокрытию факта использования Tor.

Существуют разные методы избежания палева. Например, можно выход в сеть Tor осуществлять через VPN-сервер. Это, в принципе, очень хороший метод. Он повышает нашу анонимность, вводя дополнительный узел, добавляет еще один слой шифрования, скрывает наш ip-адрес от входного узла сети Tor, что тоже может сыграть на руку, если узел окажется скомпрометирован. Но у такого метода есть проблема. VPN, используемый для таких целей, должен быть очень стабильным и быстрым, иначе вы замучайтесь перенастраивать файервол

и подключение, каждый раз, когда он отваливается. А такие сервера, как я уже неоднократно говорил, в большом дефиците.

Существуют средства сокрытия, разработанные самим проектом Tor. Во-первых, это Tor-мосты.[4] Это такие узлы Tor, адреса которых специально не публикуются. Использование их по сегодняшним временам не очень надежно, поскольку у многих провайдеров стоят DPI — системы глубокой инспекции пакетов, позволяющие выявлять тип трафика. Поясню что это значит.

Когда вы смотрите в Интернете, например, какой-то текст по не шифрованному соединению, ваш провайдер видит во-первых, что это именно текст, а не видео или картинка, а также содержание этого текста. Когда вы смотрите текст по шифрованному соединению, если у вашего провайдера нет DPI, он не видит не только содержание текста, но и то, что вы смотрите именно текст, а не видео или что-то еще. Если же вы смотрите текст по шифрованному соединению, а у провайдера есть DPI, он по-прежнему не видит содержание текста, но сможет распознать, что это именно текст, а не что-то другое.

Для противодействия таким системам, проект Tor разработал технологии обфускации, позволяющие скрыть тип трафика. Существуют разные реализации этой самой обфускации.[5] Наиболее распространенной является технология, при которой трафик мимикрирует под какой-то другой тип, например, под VoIP.[6] В большинстве случаев этой технологии хватает для предотвращения палева. Однако, в таких странах, как Китай, внедрены настолько продвинутые DPI, что способны выявлять определенные типы пакетов даже при использовании такой технологии. В этом случае может спасти другой тип обфускации, при котором трафик перенаправляется в сеть Tor через узлы какого-то крупного Интернет-ресурса, такого как Azure.[7] Также существует технология snowflake, при использовании которой трафик перенаправляется по протоколу WebRTC через узел, не задействованный как обычная нода Tor, что делает его для следящих систем не отличимым от обычной связи между компьютерами.[8] Для большинства случаев достаточно обычной мимикрии трафика. Именно ей мы и будем пользоваться, входя в сеть Tor через ноды, использующие технологию obfs4 (до сих пор есть узлы, применяющие технологию obfs3, но они менее надежны). При этом мы будем использовать незасвеченные в широком доступе obfs4-мосты, что позволяет сделать их даже более надежными, чем использующие другие технологии сокрытия факта использования Tor. Также есть и другие типы обфускации, но они мало

распространены, и о них я рассказывать не буду.

Распознавать Tor могут не только те, кто следит за вашим соединением, но и ресурсы, на которые вы ходите через эту сеть. Иногда такие ресурсы блокируют доступ к себе из сети Tor. Чтобы избежать блокировки, использование Tor нужно скрывать и от них. Сделать это можно, используя VPN. Здесь уже нет никаких трудностей. Если VPN отвалится, можно просто подобрать новый, не нужно перенастраивать файервол, поскольку нет необходимости настраивать его на предотвращение утечек трафика в обход VPN, ведь даже если он упадет, Tor по-прежнему будет скрывать вас от многочисленных Интернет-шпионов, ваша анонимность не пострадает.

Использование VPN в дополнение к Tor дает нам и другие преимущества. Как уже говорилось, в разъяснении другого случая, VPN повышает нашу анонимность, становясь дополнительным перевалочным узлом, добавляет еще один слой шифрования, который к тому же защищает нас от возможного снифинга (то есть прослушивания) на выходной ноде Tor. Правда, здесь уже сам VPN может прослушивать наш трафик и палить то, какие ресурсы мы посещаем, но поскольку нас от него скрывает Tor, опасности в этом нет.

Также сам по себе Tor не способен защитить вас от деанонимизации при использовании таких технологий, как например java-скрипты, а также в случае взлома вашей системы. Это не минус самого Tor, но необходимо предпринимать дополнительные меры, чтобы защититься от этого вектора угроз.

Для этого необходимо организовать подключение так, чтобы сама система не знала, какой у нее ip-адрес и другие реальные идентификаторы.

39 Разделение среды подключения к Сети и Интернет-активности

Наиболее надежной схемой является такая, при которой виртуальная машина, которая подключается к Интернету и перенаправляет весь трафик через сеть Tor, не используется непосредственно для Интернет-активности. Для нее используется отдельная виртуалка, подключаемая к первой по виртуальной локальной сети. Таким образом, эта виртуалка не знает ни реальный ip-адрес, ни MAC-адрес, поскольку не связана непосредственно с сетевым адаптером, а использует только виртуально эмулированный. Соответственно, даже если при Интернет-серфинге в ней будет выполнен вредоносный java-скрипт, выуживающий данные об Интернет-соединении, он получит только локальный ip, который является стандартным, и по которому невозможно провести

никакую идентификацию, и MAC-адрес виртуального адаптера, также никак не связанный с реальным. Если в браузере будет включен WebRTC, утечки ip также не произойдет по той же причине, система его просто не знает. Если залетит вирус, сканирующий данные системы, слитая им информация никак не поспособствует идентификации пользователя. И даже если операционка будет взломана, и злоумышленнику даже удастся скомпрометировать учетную запись суперпользователя, выудить реальные идентификаторы и провести деанон не получится. Злоумышленнику останется пробиваться из рабочей станции (так называется виртуалка, из которой осуществляется Интернет-активность) в шлюз (так называется виртуалка, подключаемая к Интернету и производящая туннелирование трафика), что требует дополнительных затрат сил и времени. Ни один мелкий взломщик этим заниматься не будет. На такое могут пойти только специалисты «компетентных органов» и лишь в том случае, если вы им ну очень нужны. Сложно представить, кем вы должны быть, чтобы вас разрабатывали подобными методами.

Подводя итог, подобная организация доступа к Интернету превосходно защищает от простых взломщиков и общих инструментов слежки. Преодолеть ее способна лишь точечная разработка очень могущественных структур, но даже им это будет очень не просто. Простому домашнему пользователю, таким образом, бояться совершенно нечего.

Разумеется, даже все эти меры будут бесполезны, если пользователь сам себя раскроет, к примеру, войдя в свой аккаунт, который он завел неанонимно на каком-либо ресурсе. Или отправив какую-то информацию, которая может помочь его идентифицировать, например, использовав псевдоним, содержащий информацию о нем, или обсуждая свою жизнь, упоминая увлечения, род занятий и т.д. Подобные замечания могут казаться самоочевидными, но к сожалению, неискушенные пользователи порой этого не осознают.[9]

Прежде чем переходить непосредственно к настройке шлюза, стоит сказать пару слов об операционных системах, специально заточенных на безопасность и анонимность.

40 Сомнительные инструменты безопасности

В первую очередь стоит рассмотреть системы, которые анонимизируют весь Интернет-трафик и основное отличие которых, в том, что они не оставляют следов на компьютере. Самой известной из них является Tails.[1] Как уже было

сказано, основное их отличие, это отсутствие следов их использования на компьютере. То есть, это live-системы, которые загружаются в оперативную память (с флешки или диска) и работают только в ней, а по завершении, память очищается. Соответственно, все настройки, какие были сделаны во время сеанса, также слетают. Для простого пользователя это не удобно и не нужно. Это первая причина, по которой эти системы я не могу рекомендовать.

Еще одна причина, самая главная, это наличие в этих системах несвободных компонентов. Tails, например, использует обычное ядро Linux с блобами.[2]

Ну и наконец отсутствие в них, как раз того самого разделения между средой с Интернет-подключением и средой, в которой осуществляется Интернет-активность. То есть, при активации java-скриптов, при попадании вируса и при взломе этих систем, есть риск быть деанонимизированным.

Следующая популярная система, это Whonix.[3] Она как раз реализовывает разделение функций подключения и активности по виртуальным машинам. Поскольку операционки шлюза и рабочей станции Whonix основаны на Debian, в них изначально отсутствуют несвободные компоненты. Однако, в отличие от Debian, в них по-умолчанию включены разделы репозиториев с несвободным ПО. Впрочем, их можно легко отключить, поэтому это не является большой проблемой.

Однако сами образы виртуалок распространяются главным образом с ориентиром на инструмент виртуализации VirtualBox, о проблемах которого уже было сказано. Образы для Qemu/KVM также существуют, но распространяются они в таком виде, что их установка очень сложна.

Кроме того, все мои попытки подключить шлюз Whonix непосредственно к Интернету не увенчались успехом, ему требуется раздача с хоста через NAT. То есть для использования этих инструментов, к сети нужно подключить основную операционную систему, а это уже риск. Ввиду всего этого, рекомендовать Whonix я также не могу.

Еще одна система, о которой необходимо сказать, это Qubes.[4] Это полноценная операционная система, целиком построенная на инструментах виртуализации. В ней реализуется принцип разделения задач по виртуалкам. В нее же интегрированы инструменты Whonix, при этом основная операционная система отделена от Интернета, он подключен к отдельной виртуалке и раздается с нее.

Основная причина, по которой ее не приходится рекомендовать, это все также наличие несвободных компонентов.

Кроме того, реализация данной системы лично мне кажется не очень удобной для простого пользователя, который только перешел на GNU/Linux. Каждая программа из разных виртуалок открывается в отдельных окнах, и несмотря на цветовую индикацию, это может кого-то запутать. Безусловно, тут речь о моих личных субъективных предпочтениях, и этот аргумент достаточно спорный. Но объективным остается факт наличия несвободных компонентов, что не может считаться приемлемым.

Напоследок хочется упомянуть о системе Subgraph.[5] Данная система также реализует пропускание всего трафика через Tor. Кроме того, в ней каждая программа открывается в отдельной песочнице, изолированной среде. Ее я также не могу рекомендовать.

Во-первых, это опять же наличие несвободных компонентов.

Во-вторых, использование песочниц все же менее надежно чем виртуализация.

В-третьих, ввиду отсутствия виртуализации, нет и разделения среды по подключению и активности.

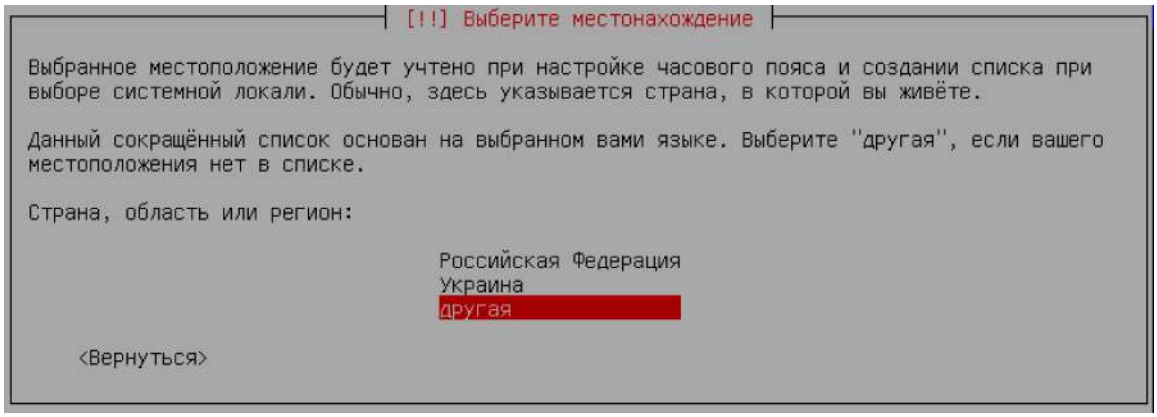
Я рассмотрел самые популярные на сегодняшний день операционные системы, реализующие определенные принципы безопасности и анонимности. Если появляются другие, то они как правило, следуют каким-либо из этих же принципов. При этом проблемы у них, скорее всего, аналогичны.

41 Установка шлюза

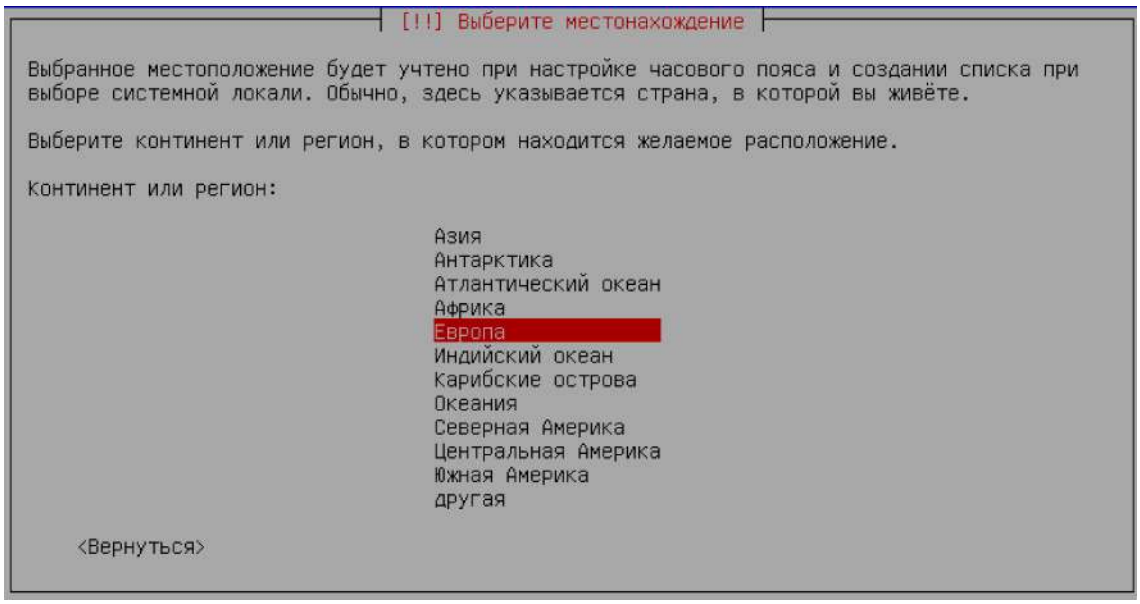
Открываем Менеджер виртуальных машин и нажимаем кнопку «Создать виртуальную машину» вверху слева. Процесс создания виртуальной машины для шлюза аналогичен созданию виртуалки для публичной Интернет-активности, только оперативной памяти достаточно 1 Гб, от процессора лучше выделить 2 ядра, а объем виртуального диска можно задать 10 Гб, этого достаточно.

Когда виртуалка запустится и появятся надписи в ее окне, разверните его под размер ВМ, а затем, также как и при настройке предыдущей виртуалки, выберите графическую установку. При выборе языка также укажите русский. Дальше в процессе установки начинаются отличия.

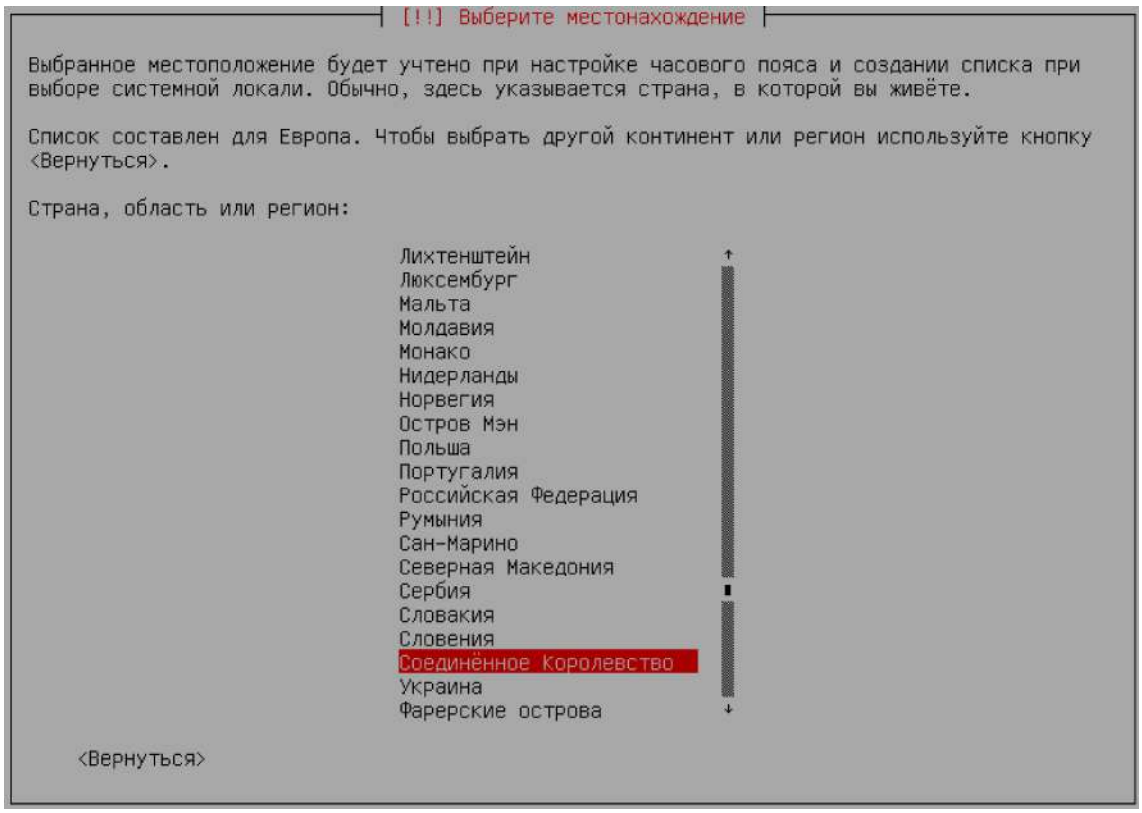
Поскольку мы собираемся настраивать анонимизацию через эту виртуалку, лучше не указывать в ней реального местоположения, а задать то, которое соответствует нулевому часовому поясу. Обычно в качестве локации в таких случаях указывается Лондон. Выбираем «другая».



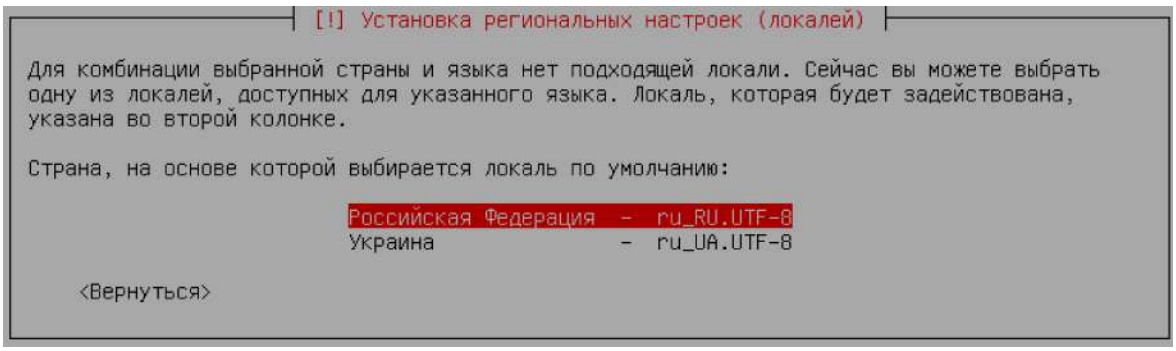
Затем выбираем «Европа».



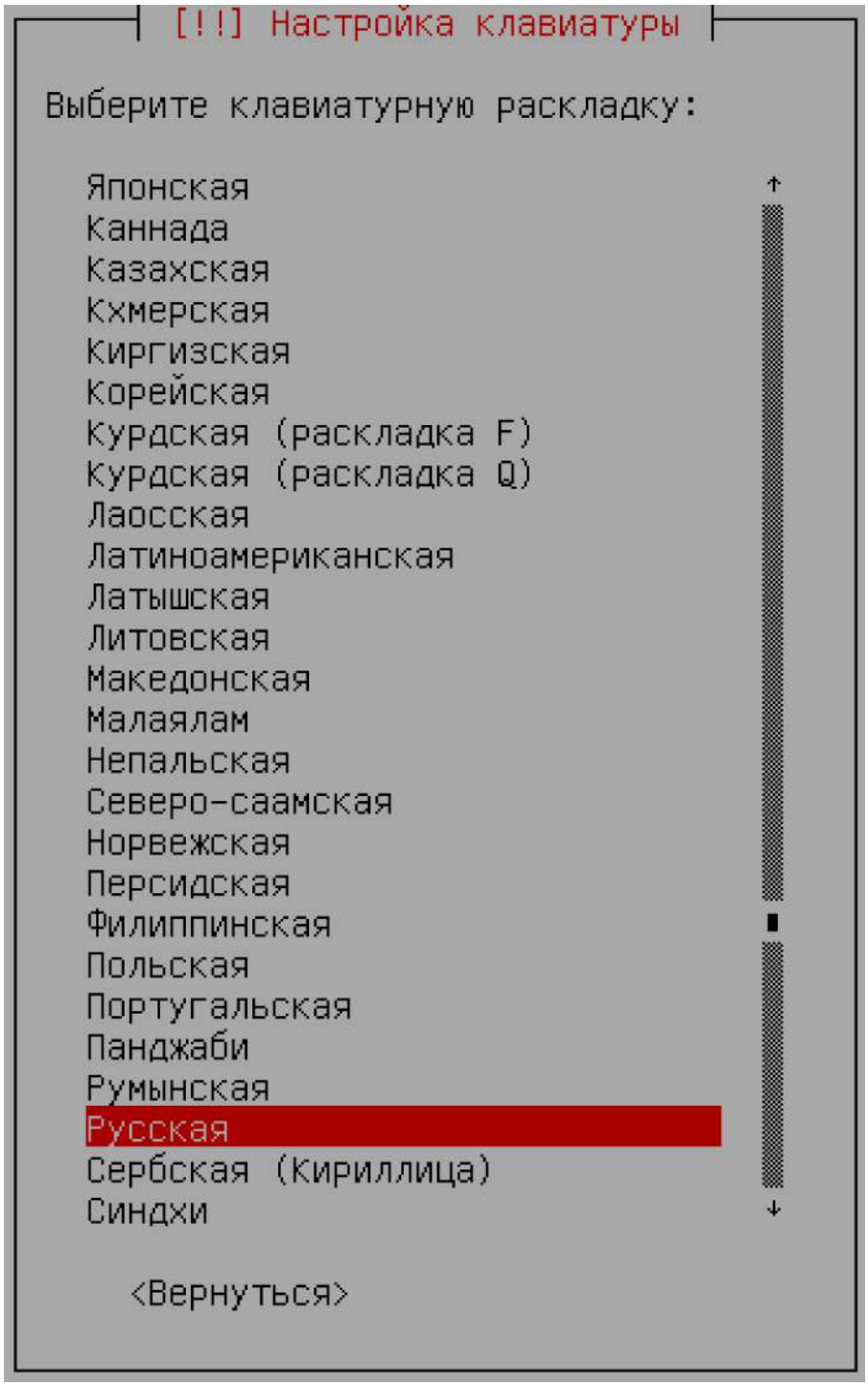
Затем «Соединенное Королевство».



Затем «Российская Федерация», чтобы иметь возможность использовать русскую раскладку клавиатуры.

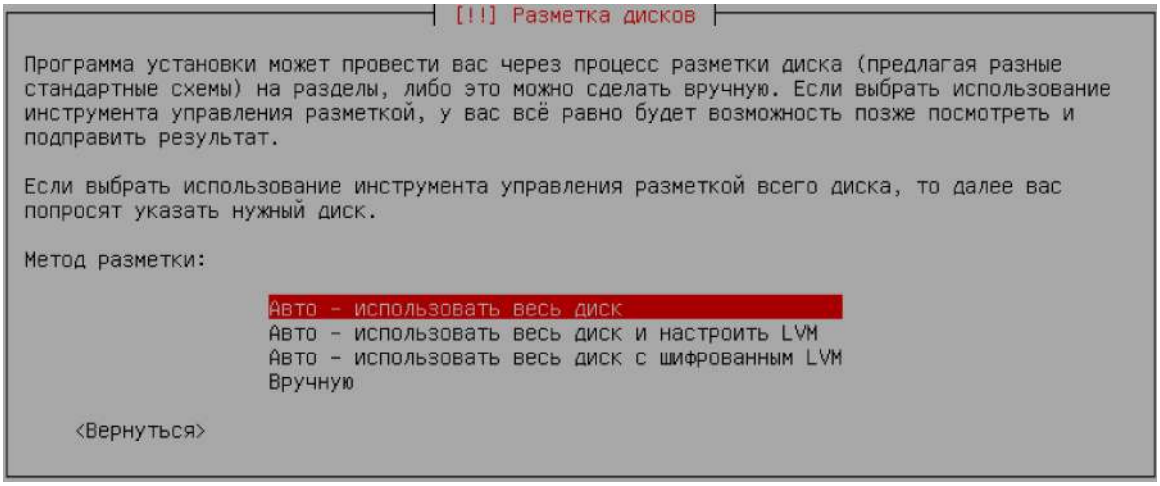


Теперь «Русская».



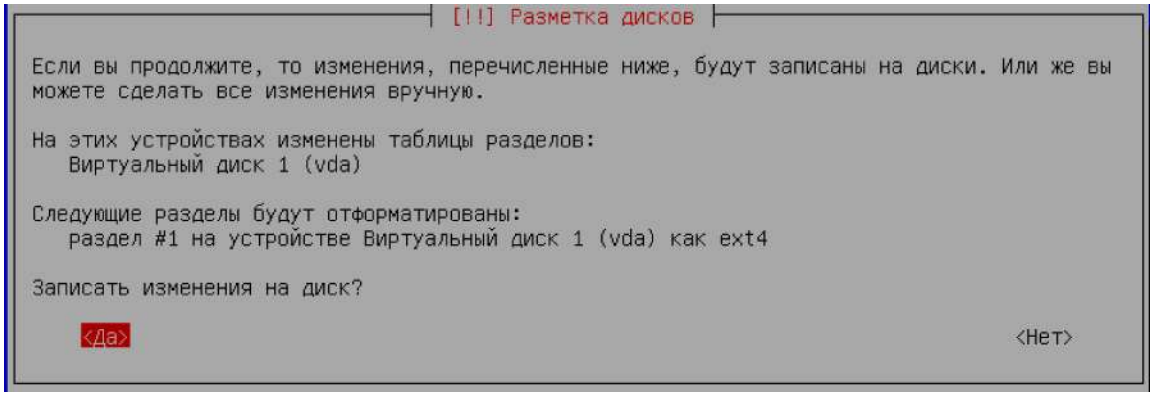
Далее все аналогично виртуалке для публичной активности.

Имя компьютера придумываем отличное от тех, что уже использовали. При разметке дисков можно не настраивать все вручную, а выбрать «Авто — использовать весь диск», поскольку данной виртуалке выделяется небольшое количество оперативной памяти и, соответственно, целесообразно позволить задать файл подкачки.



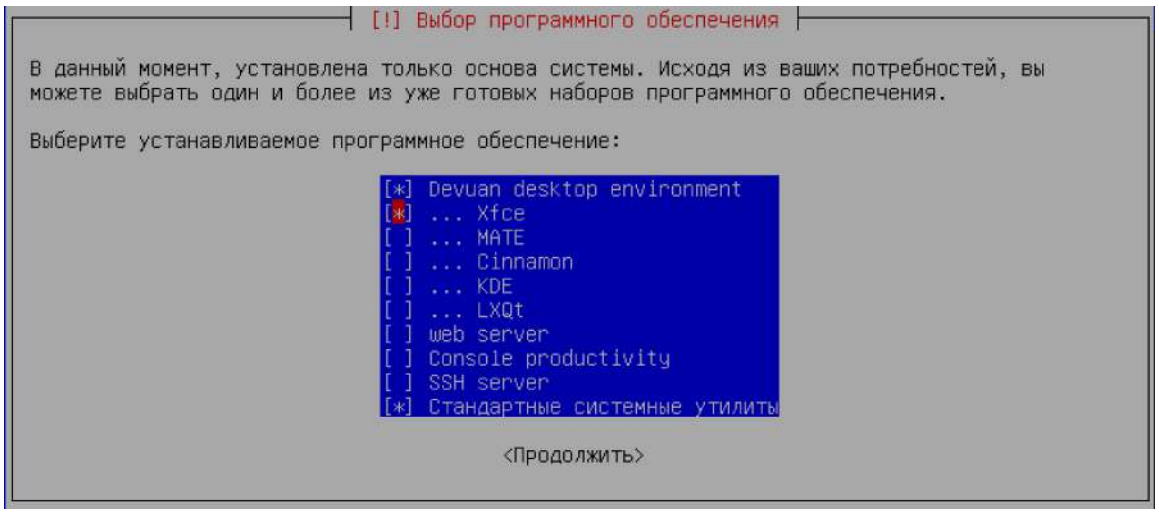
Последующие три окна смело нажимаем «Enter».

При вопросе «Записать изменения на диск», выбираем «Да».



Далее все аналогично уже знакомой настройке виртуалки.

При выборе программного обеспечения, в качестве графического окружения рекомендую выбрать XFCE, поскольку она наиболее легковесная из представленных.



Далее до конца установки все аналогично уже знакомой методике.

После перезагрузки шлюз необходимо настроить.

42 Настройка шлюза

Настройка внешнего вида и автоматического входа в систему производится по уже знакомой методике.

После этого идем в Меню, категория «Параметры» и выбираем «Менеджер пакетов Synaptic». Настраиваем репозитории и производим обновление системы по также уже знакомой методике.

Перезагружаем виртуалку, снова идем в Synaptic, удаляем telnet и устанавливаем нужные программы — Bleachbit, GDebi, gnome-system-monitor, gnome-system-tools, firefox-esr-l10n-ru, libreoffice-l10n-ru, ecj. Еще очень важным является пакет dnsmasq. Также понадобится пакет network-manager-openvpn-gnome, для подключения к VPN. Для чего это нам нужно, я объясню чуть позже. Также, конечно, устанавливаем сам tor и пакет для настройки обфускации obfs4proxy.

Также я рекомендую подключить репозитории Whonix, поскольку в них содержатся некоторые полезные программные решения. Для этого открываем терминал, набираем su, затем вводим пароль, затем набираем sudo bash, после этого переходим в каталог репозиториев с помощью следующей команды

```
cd /etc/apt/sources.list.d
```

Затем вводим команду добавления ключей подписи

```
wget https://www.whonix.org/derivative.asc
```

После этого копируем ключи в каталог с ними

```
cp /etc/apt/sources.list.d/derivative.asc /usr/share/keyrings/derivative.asc
```

Затем добавляем сами репозитории следующей командой

```
echo "deb [signed-by=/usr/share/keyrings/derivative.asc] https://deb.whonix.org bullseye main" | tee /etc/apt/sources.list.d/derivative.list
```

Далее в Synaptic обновляем список пакетов, а затем ищем пакет anon-apps-config. Данный пакет производит настройки, позволяющие повысить уровень безопасности. Во-первых, он выставляет часовой пояс UTC, отключает использование серверов NTP и DNS, предустановленных в системе, что особенно критично в системах с systemd (напоминаю, что Devuan к ним не относится), предотвращает создание соединений Tor через Tor (что будет особенно критично в рабочих станциях), а также вносит некоторые другие настройки безопасности.[6] В общем, пакет крайне полезный, и я настоятельно рекомендую установить его. Также можете попробовать установить пакет sdwdate, который позволяет проводить синхронизацию часов через Tor.[7] К сожалению, у меня он отказался работать корректно — синхронизация не происходила. Я предполагаю, что возможно, его работа завязана на компоненте systemd, который присутствует в Whonix, как системе, основанной на классическом Debian. В шлюзах Debian, к слову, он работал нормально. Возможно, у меня причина была в чем-то другом, и вы можете попробовать установить его. После этого установка ПО закончена.

Затем настраиваем браузер Firefox. Настройка аналогична той, что мы уже производили, правда теперь, поскольку мы практически не будем пользоваться этим браузером, в него нет необходимости устанавливать расширения. Достаточно во вкладке «Privasy & Security» вместо «Standard» («Стандартная») установить «Strict» («Строгая»). Это заблокирует всю рекламу, трекеры, отпечатки и прочий функционал, который может быть использован для слежки и компрометации системы.

Что касается шифрования DNS-запросов, то здесь я их не рекомендую настраивать. Хотя для шлюза это большой роли не играет, поскольку мы не будем использовать здешний браузер для постоянного Интернет-серфинга, но в

дальнейшем, этот момент крайне важный, Tor не стоит интегрировать на постоянной основе с отдельными шифрующими DNS-серверами. Tor пропускает DNS-запросы также через цепочку узлов, анонимизируя их. При этом он автоматически выбирает DNS-сервер из огромного числа оных. Большинство из них, к сожалению, работают без шифрования. При настройке же определенного DNS-сервера, поддерживающего шифрование, с одной стороны, запросы передаются безопасно. С другой, данные обо всех посещаемых вами ресурсах оказываются у одного такого сервера. И соответственно, он может собирать на вас обширную статистику, что было бы невозможно, если бы он был лишь одним из множества используемых вами серверов. Конечно, вы можете настроить подключение к нескольким серверам. Однако обеспечить такое же их количество, с каким по-умолчанию работает Tor, и тем более проконтролировать попеременное их использование не удастся. Таким образом, настраивая подключение к подобным серверам, вы серьезно снизите рандомность ваших подключений, что негативно скажется на обезличивание трафика. В отдельных случаях, когда у вас есть действительно серьезные причины опасаться подмены DNS-запросов, можно использовать кратковременное подключение к серверам, использующем шифрование. И это необходимо делать не в шлюзе, а в виртуалкеиз-под которой вы осуществляете Интернет-активность. Но на постоянной основе этого лучше избегать.[8]

Также в конфигурационном файле браузера, помимо уже известных настроек необходимо изменить еще несколько параметров.

media.peerconnection.enable, отвечающий за активацию технологии WebRTC, которая может сливать наш реальный ip-адрес. Поскольку мы не устанавливали расширения, препятствующие такому сливу, необходимо отключить ее. К тому же, такое отключение само по себе надежнее.

dom.enable_perfomance, эта функция отправки сайтам сведений о времени загрузки Интернет-страниц. С помощью нее возможно определить факт использования технологий туннелирования. Для предотвращения этого, отключаем ее.

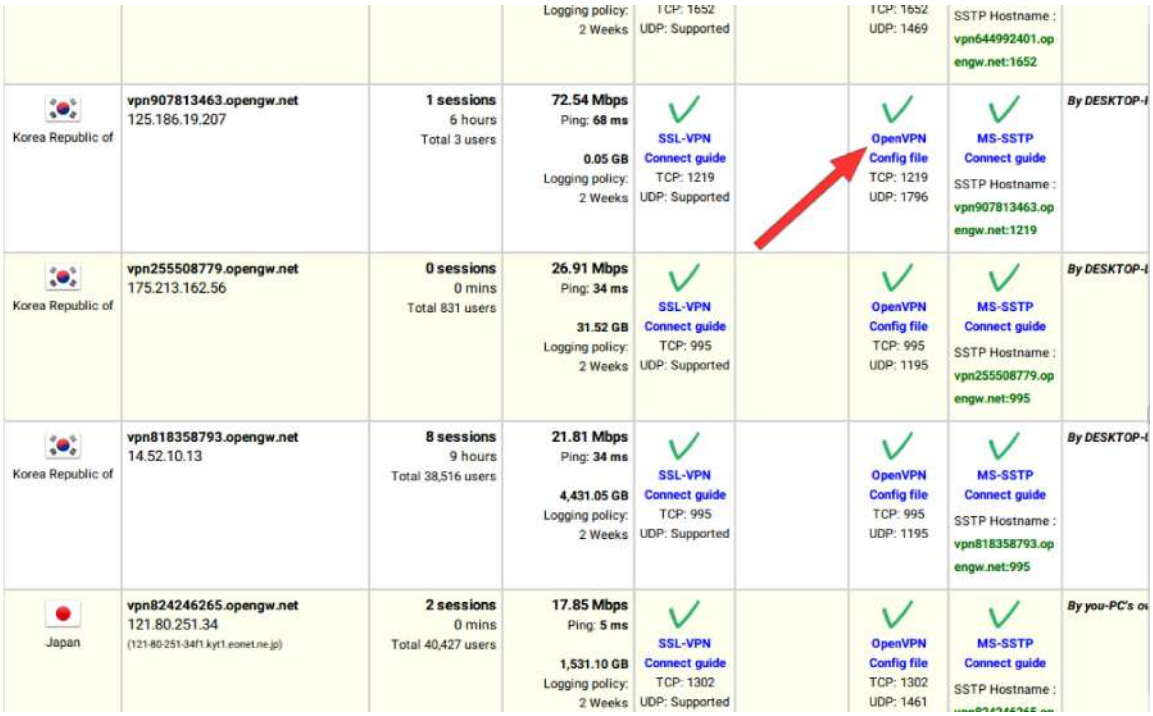
geo.enable, функция отправки сайтам сведений о местоположении. По-умолчанию, она обычно запрашивает у пользователя разрешения на предоставление геоданных, если сайт их спрашивает. Однако, надежнее будет вовсе отключить ее.

browser.send_pings, функция пинга. Позволяет сайтам отслеживать действия пользователя.

dom.netinfo.enable, функция отправки сайтам данных о параметрах подключения к сети.

layout.css.visited_links_enable, функция, позволяющая видеть изменение ссылок. Это может позволить сайтам выяснить, какие ресурсы посещал пользователь. Также с помощью java-скриптов теоретически возможно эксплуатировать данную функцию, чтобы попытаться идентифицировать пользователя по отпечаткам.

Перезагружаем браузер. Теперь необходимо скачать конфигурации obfs-мостов. При этом крайне желательно, чтобы провайдер этого не увидел. Именно для этого мы и устанавливали пакет OpenVPN, чтобы подключиться к VPN и через него скачать данные мостов. Однако прежде необходимо скачать конфигурации VPN-серверов. Переходим на сайт, где они выложены в свободный доступ.[9] Этот сервис организован одним японским институтом, здесь выкладывают конфигурационные файлы своих VPN-серверов различные энтузиасты и исследователи. При выборе сервера желательно только избегать той страны в которой вы находитесь, стран СНГ, Китая и США. В седьмом столбце слева выбираем OpenVPN.



Открывается страница со ссылками на конфигурационные файлы. Нажимаем на любую из нижних двух.

Файл скачивается. Желательно повторить процедуру сразу для нескольких серверов, поскольку, во-первых, некоторые из них могут не работать, во-вторых, нам, возможно, придется менять сервера, при скачивании конфигураций разных obfs-мостов.

После скачивания конфигурационных файлов OpenVPN, закрываем браузер, нажимаем правой кнопкой мыши на значок подключения к сети справа на нижней панели и выбираем «Изменить соединения». В открывшемся окне нажимаем значок плюс (+) внизу слева, в выскочившем окошке нажимаем на «Ethernet», и в открывшемся списке выбираем «Импортировать сохраненную конфигурацию VPN», после чего нажимаем «Создать». В появившемся окне идем в папку «Загрузки», выделяем там один из скачанных конфигурационных файлов OpenVPN и нажимаем «Открыть» внизу справа. В появившемся окне идем во вкладку «Параметры IPv4», вверху в графе «Метод» выбираем «Автоматический (DHCP, только адрес)». Теперь нам нужно указать вручную адрес DNS-сервера. Я говорил, что DNS хранит данные о том, какому адресу

какое имя сайта (или точнее домена) соответствует. Стандартно используется DNS-сервер провайдера Интернета, соответственно, для предотвращения деанона необходимо использовать другой DNS. Провайдеры VPN, которые мы собираемся использовать, предотвращают этот вектор угроз и проводят DNS-запросы через сторонние сервера. Одними из этих серверов выступают их собственные. Другими, DNS от Google. Как и все инструменты Google, их DNS собирают сведения пользователей. Ввиду этого, лучше предотвратить их использование и указать однозначно DNS самого VPN-провайдера. Общий адрес DNS у VPN с данного сервиса 10.211.254.254. Вбиваем его в поле «Серверы DNS». Затем во вкладке «Параметры IPv6» в графе «Метод» выбираем «Игнорировать». Поясню этот момент.

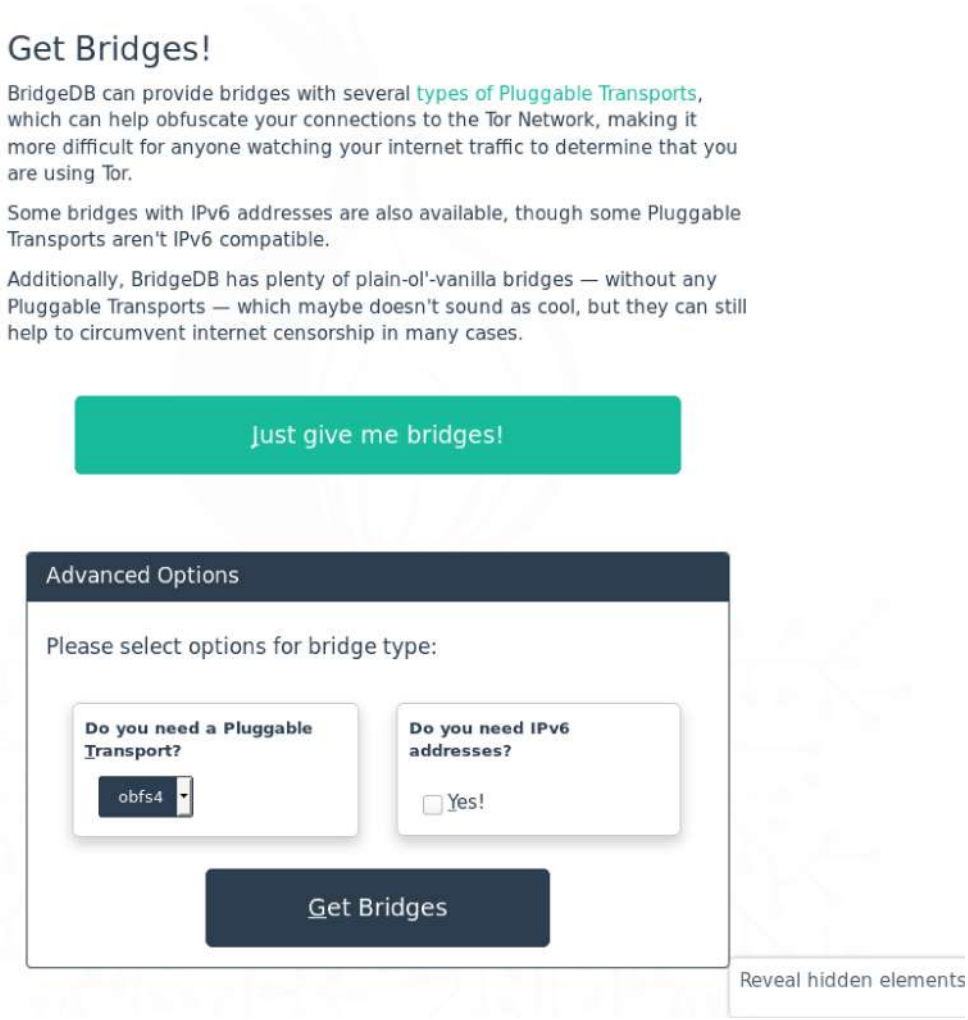
Протокол IPv4 способен предоставить ограниченное число ip-адресов.[10] Со времени возникновения этого протокола, человечество уже успело использовать их все, в результате чего его потребовалось перевести на режим сменяемости у отдельных устройств.[11] То есть, при каждом новом подключении к Интернету одного и того же устройства, провайдер выдает ему новый ip-адрес, из тех, что в данный момент не используются. Выражение «Динамический ip-адрес» описывает как раз эту практику. «Статический ip-адрес», описывает практику, когда ip у одного и того же устройства неизменный при каждом подключении. Для обычных Интернет-пользователей такая услуга по сегодняшним временам недоступна. Динамические ip, являются по сути временным решением до полноценного перехода Интернета на протокол IPv6, который способен предоставить непомерно большое количество адресов (соотношение количества ip протокола IPv4 к IPv6, сопоставимо как соотношение размера яблока и Земли).[12] Данный протокол предоставляет уникальный адрес каждому Интернет-подключению. Соответственно, с ним пользователя проще идентифицировать, чем с IPv4, в случае которого только провайдер Интернета может знать какой конкретно пользователь в какое время под каким адресом выходил. Для сторонних наблюдателей доступен лишь диапазон ip-адресов, по которому возможно лишь установить приблизительный круг пользователей, которые потенциально могли быть за определенным ip-адресом (в случае, если у этих наблюдателей есть обширное досье на каждого). Таким наблюдателем может быть, например Google, чьи следящие жучки заткнуты в тучу сайтов Интернета, они же навязывают пользователям свои приложения в Android, свои DNS и многое другое, позволяющее им собирать

это самое досье. IPv6 будучи потенциально более легким вектором деанона, также может стать каналом слива реального ip при использование туннелирования. Соответственно, при анонимизации трафика, связь по данному протоколу целесообразно отключать.

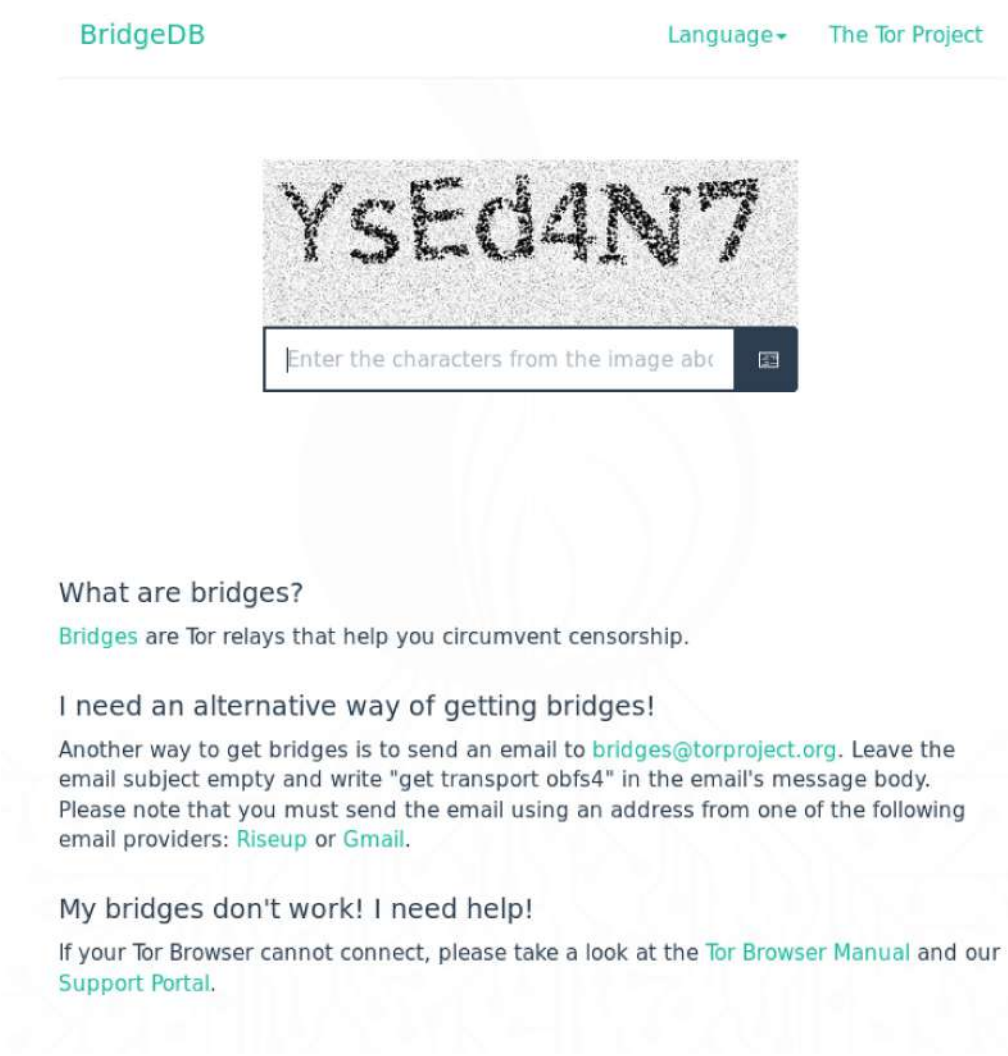
После проведения всех вышеописанных процедур, нажимаем «Сохранить» внизу справа. Проделываем все тоже самое для всех скачанных файлов OpenVPN. Также рекомендую пройти в настройки самого Интернет-подключения, для этого выделяем щелчком мыши все в том же окошке строку с подключением и затем нажимаем кнопку со значком колеса внизу слева. В открывшемся окне идем во вкладку «Параметры IPv6» и ставим также «Игнорировать». Нажимаем «Сохранить».

Закрываем окно, снова нажимаем на значок Интернета на нижней панели правой кнопкой мыши и выбираем «Соединения VPN». Нажимаем левой кнопкой мыши на любой VPN из списка. Ждем пока соединение установится, о чем выскочит соответствующее уведомление в правом верхнем углу экрана. Если соединение не устанавливается больше десяти секунд, то снимаем его и пробуем другое.

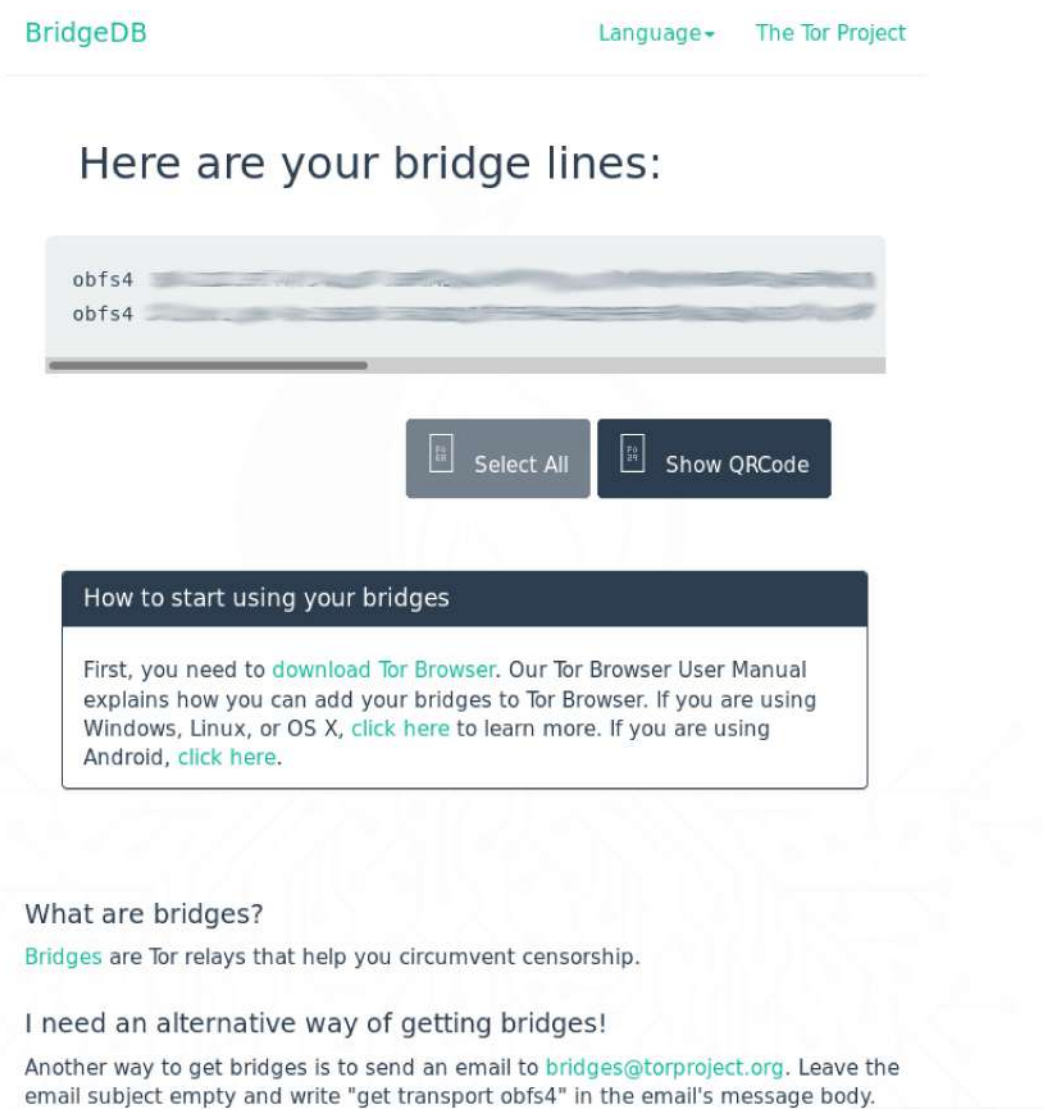
После того, как соединение с VPN установлено, снова открываем браузер. Идем на сайт с мостами Tor.[13] Выбираем obfs4 и нажимаем «Get Bridges».



На открывшейся странице вводим капчу и нажимаем «Enter».



Появятся две или три строки с конфигурациями obfs4-мостов.



Их необходимо скопировать в отдельный файл. Выделяем и копируем их в буфер обмена (если вдруг не знаете как, нажмите правой кнопкой мыши по выделенному и выбирайте «Копировать») после чего идем в Меню, категория «Стандартные» и выбираем Mousepad. В открывшейся файл вставляем данные конфигурации (если вдруг не знаете как, нажмите правой кнопкой мыши на пустом поле файла и выберите «Вставить») и сохраняем, но не закрываем файл. Для сохранения нажимаем слева вверху «Файл» и выбираем «Сохранить», в появившемся окне выбираем какую-нибудь папку, задаем любое имя файлу и нажимаем «Сохранить» внизу справа.

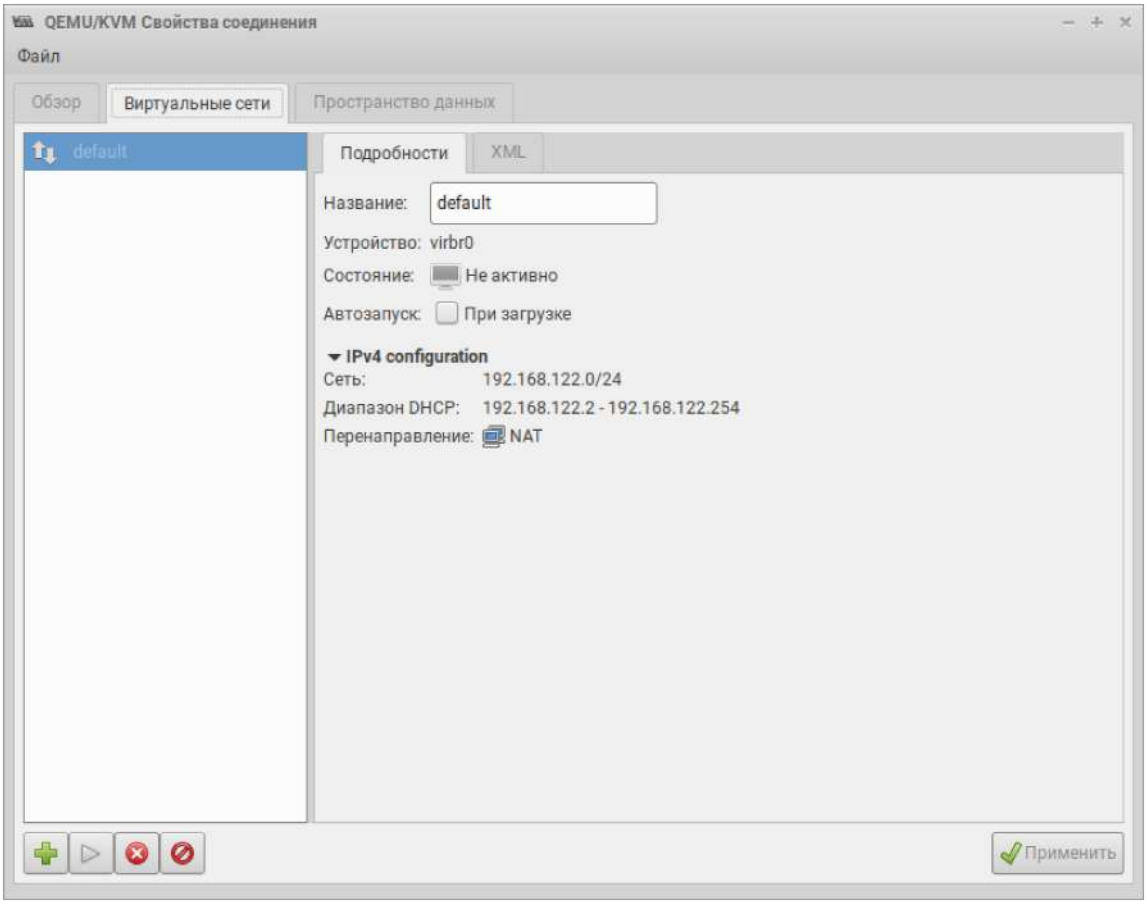
Теперь нужно вернуться на страницу назад в браузере и повторить процедуру получения мостов. Если выданные мосты окажутся теми же самыми, то необходимо сменить VPN-сервер и снова пройти процедуру получения. Я рекомендую сохранить сразу несколько десятков, чтобы обеспечить сменяемость и страховку, на случай, если какие-нибудь перестанут работать.

В качестве альтернативы этим VPN, например, если возникнут проблемы с доступом к ним, можно использовать Web-прокси.[14] Сами по себе они не очень надежны, но в некоторых случаях могут пригодиться. Подключение к ним не нужно настраивать в системе, достаточно перейти на сайт и указать адрес нужного ресурса в строке посередине. После этого вы перейдете на указанный вами сайт. При этом в адресной строке будет отображаться адрес прокси, а не того ресурса, на который вы прошли. Если из предлагаемых прокси-серверов ни один не будет корректно работать, то можно поискать иные через поисковик. Также можно воспользоваться расширениями с VPN для браузера. Они также не могут считаться надежными, но для единичных использований подойдут. Их можно найти на странице с расширениями Mozilla, по соответствующему запросу. Также желательно, чтобы они были свободными.

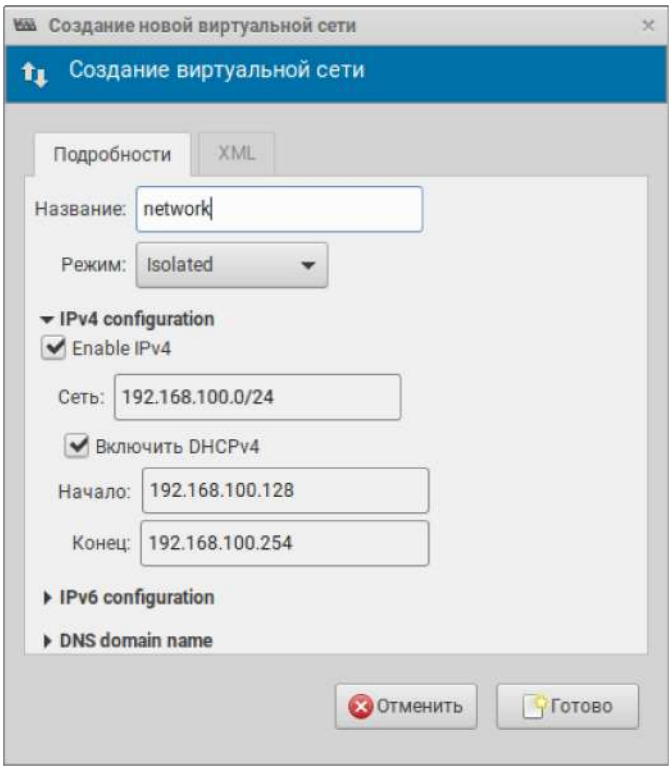
После того, как конфигурации мостов получены, сохраняем и закрываем файл с ними. Закрываем браузер и выключаем виртуалку. Не перезагружаемся, а именно выключаем.

На этом этапе можете сделать снапшот, на случай, если дальше что-то не получится, чтобы можно было вернуться и попробовать снова.

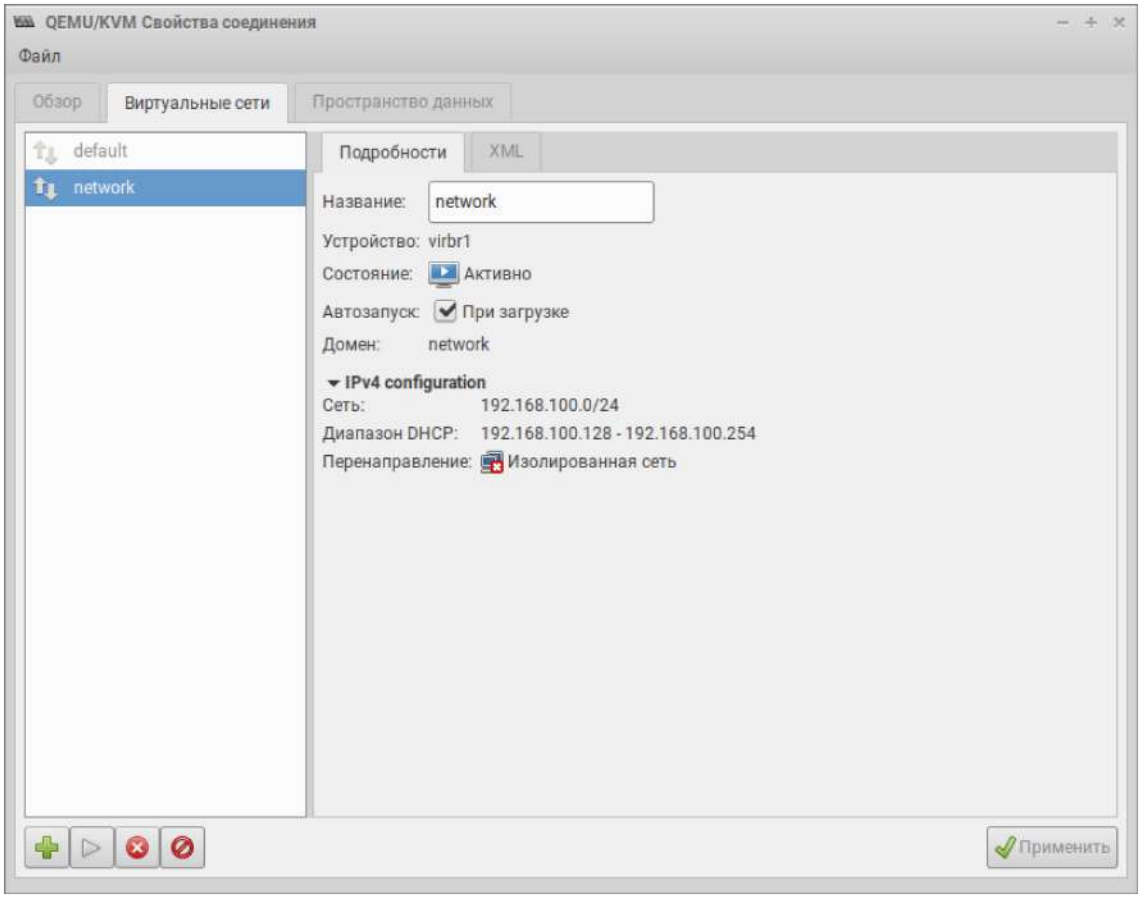
Сейчас нужно создать виртуальную локальную сеть, через которую к шлюзу будут подключаться другие виртуалки для анонимного выхода в Интернет. В основном окне Менеджера виртуальных машин нажимаем на вкладку «Правка» и выбираем «Свойства подключения». Идем в «Виртуальные сети» и нажимаем зеленый значок плюс (+) внизу слева.



В появившемся окне набираем название сети. Режим выбираем «Isolated». Также нужно выбрать адресное пространство IPv4. Можно оставить как есть или задать другой частный диапазон. Пространство адресов IPv6 определять не нужно, поэтому не трогаем этот пункт. Нажимаем «Готово» внизу справа.

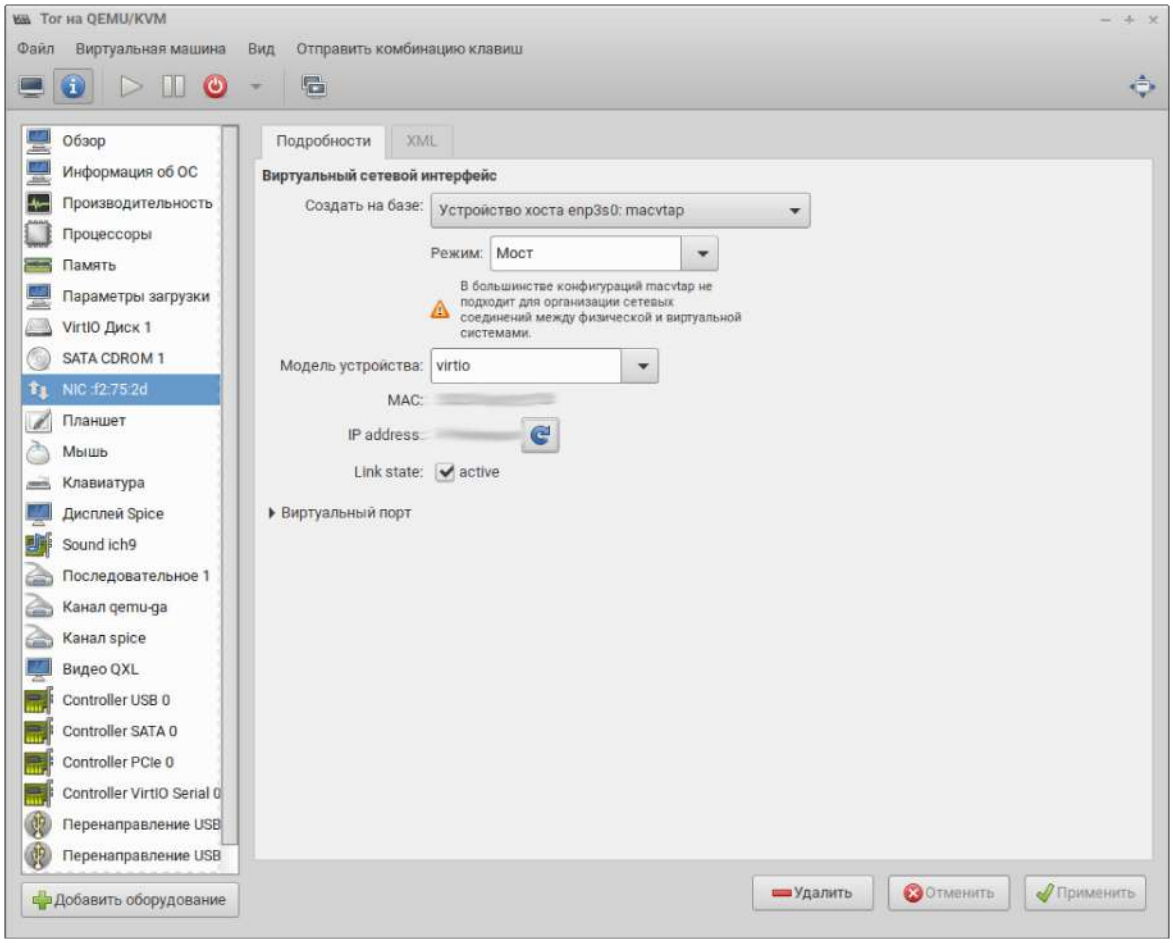


Проверяем, чтобы у новой сети стояла галочка на «Автозапуск».

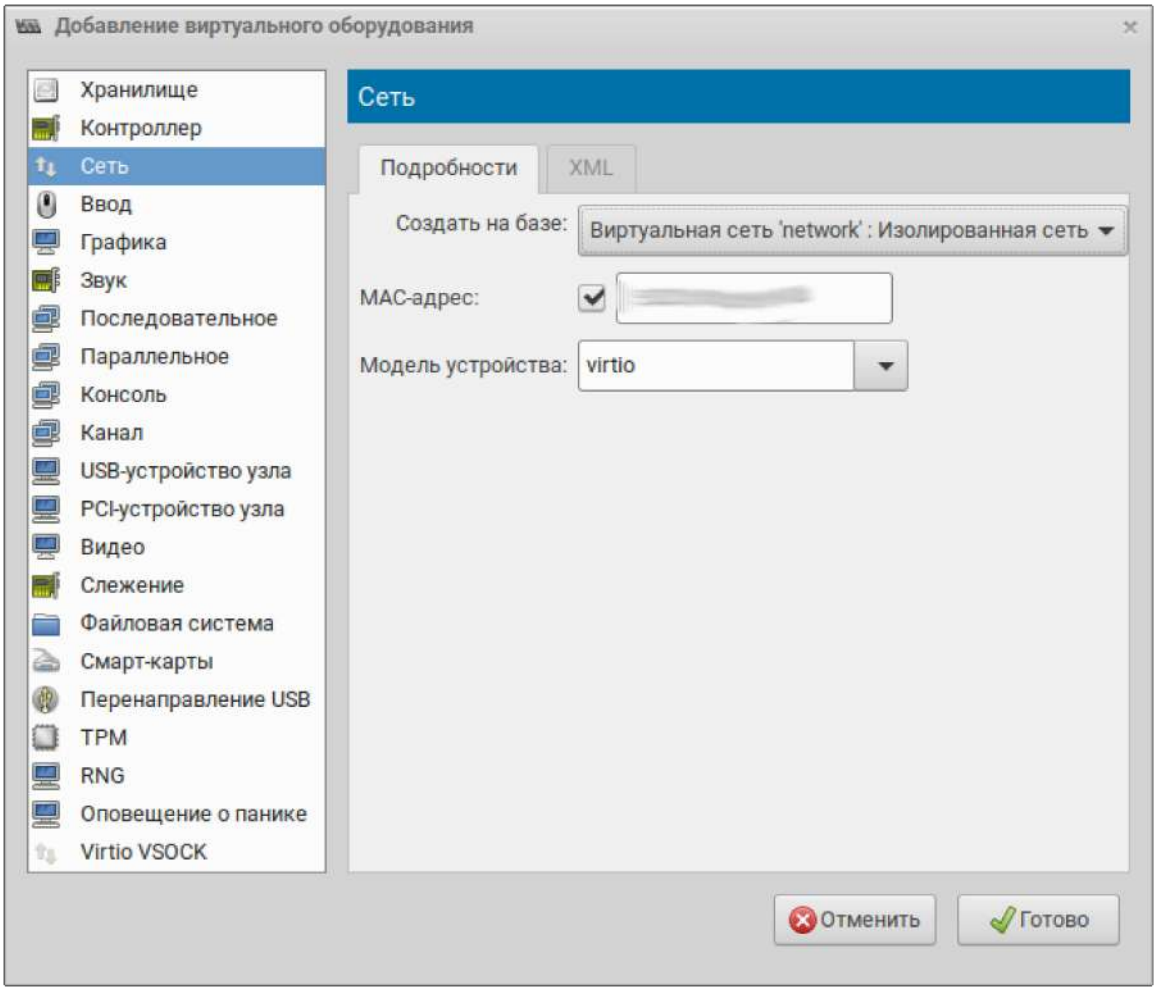


Окно можно закрыть.

Открываем шлюз и нажимаем «Свойства». Затем нажимаем на кнопку с зеленым плюсом «Добавить оборудование» внизу слева.



Выбираем слева «Сеть», в графе «Создать на базе» выбираем «Изолированная сеть». Нажимаем «Готово» внизу справа.



Также, поскольку виртуальные машины берут информацию о времени с хоста, проверьте, чтобы время на компьютере было выставлено правильно. Это важно для работы Tor. Разница в несколько минут может быть не критичной, но лучше, чтобы она была как можно меньше. Синхронизация через Интернет не поможет, поскольку стандартные средства синхронизации используют протокол UDP, по которому не умеет работать Tor. А пакет, о котором я рассказывал выше, как и отмечалось, может не работать в Devuan. Поэтому, лучше просто выставить время вручную на хосте.

Нажимаем в окне виртуалки «Консоль» и запускаем виртуальную машину.

Теперь нажимаем на значок Интернета на панели. После добавления адаптера, появилось новое соединение. Оно не подходит для наших нужд, его необходимо удалить и настроить другое. Выделяем новое соединение и нажимаем на значок минус (–) внизу слева. Затем нажимаем на значок плюс (+) рядом. Нажимаем на «Ethernet» и выбираем «VLAN». Нажимаем «Создать».

В открывшемся окне во вкладке «VLAN» нажимаем на стрелочку в конце поля «Родительский интерфейс» и выбираем сетевой адаптер, подключенный к виртуальной локальной сети. Если не помните какой MAC-адрес принадлежит какому адаптеру, откройте свойства виртуальной машины и посмотрите. После того, как адаптер указан, в поле «Имя интерфейса VLAN» набираем то название, которое давали созданной виртуальной локальной сети. Это важно указать, поскольку без этого, соединение не будет работать. После этого идем во вкладку «Параметры IPv4» и в графе «Метод» выбираем «Вручную». Нажимаем на кнопку «Добавить» справа от пустого поля. В нем появится строка. Нажимаем на ней под надписью «Адрес» и вводим первый ip-адрес из того диапазона, который вы указали при создании виртуальной сети. Такой адрес заканчивается на единицу после последней точки. То есть, если вы выбрали 192.168.100.0/24, то указываем 192.168.100.1. Затем нажимаем на строку под надписью «Маска сети» и указываем эту маску. Можете смело указать 255.255.255.0 или просто 24. Больше ничего указывать здесь не нужно. Идем во вкладку «Параметры IPv6» и в графе «Метод» выбираем «Игнорировать». Нажимаем «Сохранить» внизу справа. Можем также удалить VPN-соединения. Закрываем окно настройки сетевых соединений. Пришло время переходить к настройке Tor.

Открываем терминал и первым делом добавляем себя как пользователя в группу sudo, которая позволяет вам работать с правами суперпользователя (необходимость ввода пароля при этом никуда не девается). Набираем su, затем вводим пароль, затем набираем sudo bash, после этого вбиваем следующую строку

adduser **user** sudo

Жирным шрифтом указано имя пользователя. Вам необходимо указать свое. Нажимаем «Enter». Перезагружаемся и снова открываем терминал. Набираем sudo thunar. Вводим пароль и открывается файловый менеджер с правами суперпользователя. Переходим в корневой каталог, идем в папку etc, затем в папку tor, в ней открываем в редакторе Mousepad файл torrc. Листаем открывшийся файл до конца и в конец вставляем следующие строки[15]

VirtualAddrNetworkIPv4 10.192.0.0/10
AutomapHostsOnResolve 1

TransPort **192.168.1.1**:9040 IsolateClientAddr IsolateClientProtocol IsolateDestAddr IsolateDestPort
TransPort 127.0.0.1:9040 IsolateClientAddr IsolateClientProtocol IsolateDestAddr IsolateDestPort
DNSPort **192.168.1.1**:5353
DNSPort 127.0.0.1:5353

Жирным шрифтом выделен ip-адрес шлюза в виртуальной локальной сети. Вам необходимо изменить его на тот, который задали вы. Если это 192.168.100.1, то вписывайте его. Под эти строки вносим следующие

UseBridges 1
ClientTransportPlugin obfs4 exec /usr/bin/obfs4proxy managed
bridge obfs4 11.111.111.1:1111 4GYF734JORJcert=89r3hgbv9qYGF/ug39H/hx8ew iat-mode=0
bridge obfs4 11.111.111.2:2222 4GYF734JORJcert=89r3hgbv9qYGF/ug39H/hx8ew iat-mode=0
bridge obfs4 11.111.111.3:3333 4GYF734IORJcert=89r3hgbv9qYGF/ug39H/hx8ew iat-mode=0
bridge obfs4 11.111.111.4:4444 4GYF734JORJcert=89r3hgbv9qYGF/ug39H/hx8ew iat-mode=0

Жирным шрифтом выделены конфигурации obfs4-мостов, представленные как пример. Вместо них вносите все мосты, которые скачали вы. Их ключи будут длиннее и ip с портами будут другими. Обратите внимание, что перед каждой строкой с конфигурацией есть слово bridge. Его обязательно проставляем. Под них вписываем еще одну строку

ExcludeExitNodes {ru},{ua},{by},{kz}

Данная настройка исключает при построении цепочки Tor ноды в определенных странах, в качестве выходных. В скобках указываются индексы этих стран. Необходимо прописать индекс той страны, в которой вы находитесь, ru — Россия, ua — Украина и т.д.[16] Если страна вашего пребывания отличается от указанных, вписывайте ее. Иногда рекомендуют ноды страны, в которой находитесь, полностью исключать из построения цепочки, но такую меру можно считать чрезмерной. Кроме того, это может даже негативно сказаться на безопасности, в случае глобального пассивного наблюдения, поскольку будет заметно, что конкретный пользователь никогда не затрагивает определенные ноды при создании цепочки анонимизации. Для дополнительной безопасности можно также указать некоторые страны, в том числе и страну, в которой находитесь, как те, ноды в которых не используются в рамках одной цепочки одновременно, поскольку бывает, что Tor использует два узла в одной и той же стране. А в некоторых случаях даже все узлы могут оказаться в ней.

Чтобы это предотвратить, вписываем следующую строку.

```
NodeFamily {ru},{ua},{by},{kz},{kg},{us},{de}
```

Здесь, опять же, указываете те страны, которые нужно вам. Сохраняем и закрываем файл.

После этого возвращаемся в файловом менеджере в папку etc, находим в ней и открываем файл sysctl.conf. В нем находим строку net.ipv4.ip_forward=1 и расскомментируем ее, сняв значок решетки (#) перед ней. Это позволит включить трансляцию пакетов с других виртуалок через шлюз в Интернет, таким образом эти виртуалки получат доступ к сети. Сохраняем и закрываем файл. Файловый менеджер также можно закрыть.

Включенная трансляция пакетов применится только после перезагрузки, чтобы осуществить ее без перезагрузки, вбиваем в терминале строку

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

И нажимаем «Enter». Далее необходимо предотвратить DNS утечки. Для этого настроим использование локального DNS, задействующего средства Tor. [17] Сначала удалим файл, в который заносятся адреса DNS вашего провайдера, создадим новый и впишем в него локальный адрес, используемый для доступа к DNS сети Tor. Для этого набираем в терминале

```
sudo rm -f /etc/resolv.conf
echo "nameserver 127.0.0.1" | sudo tee /etc/resolv.conf
```

Чтобы NetworkManager не перезаписал содержимое файла, заблокируем его для записи, набрав команду

```
sudo chattr +i /etc/resolv.conf
```

Теперь необходимо узнать uid под которым работает Tor на вашей системе. Для этого используем команду

```
grep tor /etc/passwd
```

Будет выведен ответ примерно такого вида

```
debian-tor:x:111:145::/var/lib/tor:/bin/false
```

Цифры 111 это и есть uid (у вас они, возможно, будут другими). Они нам в дальнейшем понадобятся.

Открываем файловый менеджер, в папке пользователя нажимаем на пустом месте правой кнопкой мыши и выбираем «Пустой файл». В появившемся окне вводим название iptables_setup.sh (в принципе, можно придумать и другое, но обязательно, чтобы в конце стояло .sh). Открываем созданный файл. В данный файл вносятся настройки подключения к Tor и правила файервола, которые будут предотвращать утечку трафика в обход Tor. Эти правила преимущественно взяты с сайта проекта Tor.[18] Также сюда внесены дополнения из замечания одного пользователя, обнаружившего еще один канал утечки информации, способствующей деанону.[1] Также добавлены ограничивающие правила, взятые из настроек системы Whonix, о которой говорилось выше. Они также предотвращают слив информации окольными путями, в частности отключают временные метки TCP.

Итак, ниже представлено содержимое, которое необходимо внести в созданный файл. Жирным шрифтом отмечены параметры, которые вам необходимо заменить на ваши. Рядом с ними курсивом в скобках даны пояснения, на что именно менять. Эти пояснения вносить в файл не нужно. Вот полный скрипт

```
#!/bin/sh
#

### Set variables
# The UID that Tor runs as (varies from system to system)
_tor_uid="111" #As per assumption          (Необходимо указать uid, который мы смотрели)
#_tor_uid=`id -u debian-tor` #Debian/Ubuntu
#_tor_uid=`id -u tor` #ArchLinux/Gentoo

# Tor's TransPort
_trans_port="9040"

# Tor's DNSPort
_dns_port="5353"

# Tor's VirtualAddrNetworkIPv4
```

```
_virt_addr="10.192.0.0/10"

# Your outgoing interface
_out_if="eth0"  (виртуальный адаптер, подключаемый к Интернету)

# Your incoming interface and assigned local IP (Gateway)
_inc_if="eth1" (адаптер, подключаемый к локальной сети)
_inc_ip="192.168.1.1" (ip шлюза в локальной сети, 192.168.100.1 или какой прописывали)

# LAN destinations that shouldn't be routed through Tor
_non_tor="127.0.0.0/8 10.0.0.0/8 172.16.0.0/12 192.168.0.0/16"

### Flush iptables
iptables -F
iptables -t nat -F

### *nat PREROUTING (For middlebox)
iptables -t nat -A PREROUTING -d $_virt_addr -i $_inc_if -p tcp -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -j REDIRECT --to-ports $_trans_port
iptables -t nat -A PREROUTING -i $_inc_if -p udp --dport 53 -j REDIRECT --to-ports $_dns_port

# Allow lan access for hosts in $_non_tor
for _lan in $_non_tor; do
  iptables -t nat -A PREROUTING -i $_inc_if -d $_lan -j RETURN
done

iptables -t nat -A PREROUTING -i $_inc_if -p tcp -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -j REDIRECT --to-ports $_trans_port

### *nat OUTPUT (For local redirection)
# nat .onion addresses
iptables -t nat -A OUTPUT -d $_virt_addr -p tcp -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -j REDIRECT --to-ports $_trans_port

# nat dns requests to Tor
iptables -t nat -A OUTPUT -d 127.0.0.1/32 -p udp -m udp --dport 53 -j REDIRECT --to-ports $_dns_port

# Don't nat the Tor process, the loopback, or the local network
iptables -t nat -A OUTPUT -m owner --uid-owner $_tor_uid -j RETURN

# Allow lan access for hosts in $_non_tor
for _lan in $_non_tor; do
  iptables -t nat -A OUTPUT -d $_lan -j RETURN
done
```

```
# Redirect all other pre-routing and output to Tor's TransPort
iptables -t nat -A OUTPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -j REDIRECT --to-ports $_trans_port

### *filter INPUT
# Allow DNS lookups from connected clients and internet access through tor.
iptables -A INPUT -d $_inc_ip -i $_inc_if -p udp -m udp --dport $_dns_port -j ACCEPT

# Drop everything else
iptables -A INPUT -m conntrack --ctstate INVALID -j DROP
iptables -A INPUT -m state --state INVALID -j DROP
iptables -A INPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG FIN,SYN,RST,ACK -j DROP
iptables -A INPUT -p tcp -m tcp --tcp-flags FIN,SYN FIN,SYN -j DROP
iptables -A INPUT -p tcp -m tcp --tcp-flags SYN,RST SYN,RST -j DROP
iptables -A INPUT -f -j DROP
iptables -A INPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG FIN,SYN,RST,PSH,ACK,URG -j DROP
iptables -A INPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG NONE -j DROP
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p icmp -j DROP
iptables -A INPUT -d $_inc_ip -i $_inc_if -p tcp -m tcp --dport $_trans_port --tcp-flags FIN,SYN,RST,ACK SYN -j ACCEPT
iptables -A INPUT -j DROP

### *filter FORWARD
iptables -A FORWARD -j DROP

### *filter OUTPUT
iptables -A OUTPUT -m conntrack --ctstate INVALID -j DROP
iptables -A OUTPUT -m state --state INVALID -j DROP
iptables -A OUTPUT ! -o lo ! -d 127.0.0.1 ! -s 127.0.0.1 -p tcp -m tcp --tcp-flags ACK,FIN ACK,FIN -j DROP
iptables -A OUTPUT ! -o lo ! -d 127.0.0.1 ! -s 127.0.0.1 -p tcp -m tcp --tcp-flags ACK,RST ACK,RST -j DROP
iptables -A OUTPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG FIN,SYN,RST,ACK -j REJECT --reject-with icmp-admin-prohibited
iptables -A OUTPUT -p tcp -m tcp --tcp-flags FIN,SYN FIN,SYN -j REJECT --reject-with icmp-admin-prohibited
iptables -A OUTPUT -p tcp -m tcp --tcp-flags SYN,RST SYN,RST -j REJECT --reject-with icmp-admin-prohibited
iptables -A OUTPUT -f -j REJECT --reject-with icmp-admin-prohibited
```

```
iptables -A OUTPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG FIN,SYN,RST,PSH,ACK,URG -j REJECT --reject-with icmp-admin-prohibited
iptables -A OUTPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG NONE -j REJECT --reject-with icmp-admin-prohibited
iptables -A OUTPUT -m state --state ESTABLISHED -j ACCEPT

# Allow Tor process output
iptables -A OUTPUT -o $_out_if -m owner --uid-owner $_tor_uid -p tcp -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -m state --state NEW -j ACCEPT

# Allow loopback output
iptables -A OUTPUT -d 127.0.0.1/32 -o lo -j ACCEPT

# Tor transproxy magic
iptables -A OUTPUT -d 127.0.0.1/32 -p tcp -m tcp --dport $_trans_port --tcp-flags FIN,SYN,RST,ACK SYN -j ACCEPT

# Drop everything else
iptables -A OUTPUT -j DROP

### Set default policies to DROP
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT DROP

### Set default policies to DROP for IPv6
ip6tables -P INPUT DROP
ip6tables -P FORWARD DROP
ip6tables -P OUTPUT DROP
```

Названия адаптеров, подключаемого к Интернету и подключаемого к локальной сети, можно посмотреть, нажав правой кнопкой мыши на значок Интернета на нижней панели и выбрав «Сведения о соединении». Соединение VLAN, это локальная сеть, другое, например, Ethernet или Wi-Fi, это Интернет. Название адаптера указано наверху в графе «Интерфейс».

Сохраняем и закрываем файл. Запускаем скрипт следующими командами

```
chmod +x iptables_setup.sh
sudo ./iptables_setup.sh
```

Проверяем работу Tor. Набираем для его запуска следующую команду

```
sudo /etc/init.d/tor restart
```

Открываем браузер, идем в поисковик DuckDuckGo и набираем в строке поиска «my ip». Если результат высвечивается как «Your IP address is unavailable», а в указателе страны указано «All Regions» или какая-то страна, отличная от вашей, значит все в порядке. Закрываем браузер и набираем в терминале

```
sudo /etc/init.d/tor stop
```

Это остановит Tor. Если все настроено как нужно, то без Tor трафик идти не будет. Запускаем браузер и идем на любой сайт. Если страница не грузится или выдается сообщение о проблемах с Интернетом, значит все хорошо. Закрываем браузер. В некоторых случаях эта команда не работает. Если сайты продолжают грузиться, то еще раз проверьте ip. Если он не ваш, то все в порядке.

Теперь необходимо добавить правила файервола в автозагрузку, поскольку по-умолчанию при следующем запуске настройки iptables очистятся, и правила не будут применены. Снова запускаем Tor командой

```
sudo /etc/init.d/tor restart
```

Открываем Менеджер пакетов Synaptic и устанавливаем пакет iptables-persistent. Во время установки, в окошке, где идет шкала загрузки, нажимаем «Подробнее» и в открывшемся поле терминала, при вопросе о сохранении правил, набираем «y», то есть подтверждение, и нажимаем «Enter». Вопрос появится дважды для правил IPv4 и IPv6. Когда установка закончится, закрываем Synaptic и добавляем Tor в автозагрузку, набрав в терминале строку

```
sudo update-rc.d tor enable
```

После этого закрываем терминал, перезагружаемся и снова проверяем работу Tor. После запуска он автоматически запускается (иногда бывает, что нет, обычно это редко, в другой раз при запуске этого не будет) и при запросе в браузере, будет указан неизвестный ip. Также проверяем в выключенном состоянии, т.е. останавливаем Tor указанной выше командой и проверяем, есть

ли доступ к Интернету. Если нет, все хорошо.

Для того, чтобы иметь быстрый доступ к основным командам для работы с Tor, можно создать файл на Рабочем столе или в папке и вписать туда

sudo /etc/init.d/tor restart — *Перезапуск Tor*
sudo /etc/init.d/tor stop — *Остановка Tor*

Если во время работы, начнутся тормоза, то нужно будет просто открыть терминал, дать команду на перезапуск, ввести пароль, и Tor перезапустится.

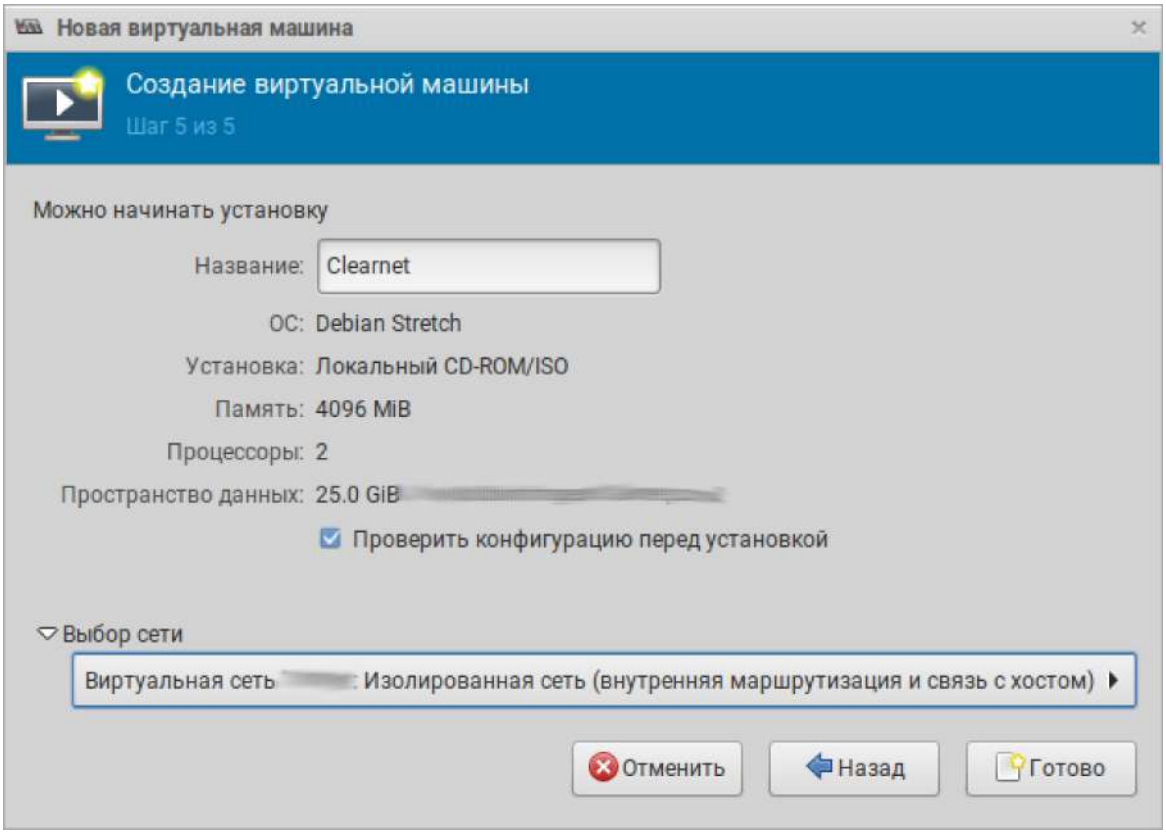
Чистим систему с помощью Bleachbit, выключаем и делаем снапшот.

На этом настройка шлюза закончена. Через него из других виртуалок можно гулять по Интернету и пользоваться различными сервисами не опасаясь слежки, цензуры, саботажа и прочих неприятностей. Правда из других виртуалок пройти на скрытые сервисы Tor (в onion-пространство) не получится. Я так и не разобрался, какие именно настройки нужны для этого. Однако простому пользователю это и не к чему. Доступ же к поверхностному Интернету для него при такой организации всецело безопасен.

6 Виртуальная машина для приватной Интернет-активности

43 Установка рабочей станции

В основном окне Менеджера виртуальных машин нажимаем кнопку «Создать». Процесс создания виртуальной машины для приватной Интернет-активности аналогичен созданию виртуалки для публичной активности вплоть до момента указания сети. Здесь в графе «Выбор сети» необходимо указать «Изолированная сеть».



Нажимаем «Готово». Далее все аналогично установке шлюза, т.е. в качестве страны выбирается «Соединенное королевство», при этом язык можно указать по-прежнему русский (если хорошо владеете английским, то лучше, конечно, использовать его, это еще повысит анонимность). Имя компьютера, как и прежде, задаем уникальное. На этапе разметки дисков аналогия со шлюзом заканчивается и далее все аналогично установке системы для публичной активности. Разметку диска выполняем вручную, без файла подкачки. На этапе «Выбор программного обеспечения», графическую

оболочку также выбираем исходя из рекомендаций для публичной виртуалки.

После установки и загрузки первым делом настраиваем внешний вид, если стандартный вас не устраивает, затем нажимаем правой кнопкой мыши на значок Интернета на панели и выбираем «Изменить соединения». Удаляем появившееся подключение «Ethernet», нажимаем на значок плюс внизу слева и выбираем «VLAN». В появившемся окне во вкладке «VLAN» в графе «Родительский интерфейс» выбираем единственный имеющийся. В графе «Имя интерфейса VLAN» набираем название виртуальной локальной сети. Во вкладке «Параметры IPv4» в графе «Метод» выбираем «Вручную», справа от поля «Адрес» нажимаем на кнопку «Добавить» и в поле под «Адрес» вводим ip нашей виртуалки. Можно не заморачиваясь указать на единицу больше чем адрес шлюза, т.е. если ip шлюза 192.168.100.1, то ip рабочей станции 192.168.100.2. Под «Маска сети» указываем 255.255.255.0 или просто 24. Под «Шлюз» указываем ip-адрес шлюза, если это 192.168.100.1, то его и прописываем. В графе «Серверы DNS» также указываем ip шлюза. Во вкладке «Параметры IPv6» в графе «Метод» выбираем «Игнорировать». Нажимаем «Сохранить» внизу справа.

Закрываем окно настройки сетей. Снова нажимаем на значок Интернета и снимаем галочку с «Управление сетью». После чего ставим обратно. Это перезапустит подключение к сети, и заработает настроенное нами соединение. После этого открываем Synaptic, настраиваем репозитории, обновляем систему, перезагружаемся, снова идем в Synaptic, удаляем telnet, затем устанавливаем необходимые программы — Bleachbit, GDebi, gnome-system-monitor, gnome-system-tools, network-manager-openvpn-gnome, libreoffice-l10n-ru, firefox-esr-l10n-ru, curl, ecj, caja. Также устанавливаем menulibre. Последний пакет позволяет редактировать Меню, что может пригодится для доступа к программам, установленным со сторонних ресурсов. Далее подключаем репозитории Whonix, как мы это делали в шлюзе и устанавливаем пакет anon-apps-config, а если ранее у вас получилось синхронизировать время с помощью sdwdate, то и его.

Закрываем Synaptic. По уже знакомой методике, в редакторе Mousepad открываем файл slim.conf с правами суперпользователя и отключаем ввод пароля при каждом входе в систему.

После этого идем в Меню, категория «Избранное» и выбираем «Эмулятор терминала». Запускается терминал. Набираем su, вводим пароль, затем sudo

bash, после чего необходимо прописать правила файервола для рабочей станции. Ниже представлен их полный набор. Эти правила взяты из системы Whonix. Жирным шрифтом выделено пространство адресов виртуальной сети, которое нужно заменить на ваше, если оно отличается.

```
iptables -A INPUT -m conntrack --ctstate INVALID -j DROP
iptables -A INPUT -m state --state INVALID -j DROP
iptables -A INPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG FIN,SYN,RST,ACK -j DROP
iptables -A INPUT -p tcp -m tcp --tcp-flags FIN,SYN FIN,SYN -j DROP
iptables -A INPUT -p tcp -m tcp --tcp-flags SYN,RST SYN,RST -j DROP
iptables -A INPUT -f -j DROP
iptables -A INPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG FIN,SYN,RST,PSH,ACK,URG -j DROP
iptables -A INPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG NONE -j DROP
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -j REJECT --reject-with tcp-reset
iptables -A INPUT -j REJECT --reject-with icmp-port-unreachable
iptables -A FORWARD -j DROP
iptables -A OUTPUT -m conntrack --ctstate INVALID -j REJECT --reject-with icmp-admin-prohibited
iptables -A OUTPUT -m state --state INVALID -j REJECT --reject-with icmp-admin-prohibited
iptables -A OUTPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG FIN,SYN,RST,ACK -j REJECT --reject-with icmp-admin-prohibited
iptables -A OUTPUT -p tcp -m tcp --tcp-flags FIN,SYN FIN,SYN -j REJECT --reject-with icmp-admin-prohibited
iptables -A OUTPUT -p tcp -m tcp --tcp-flags SYN,RST SYN,RST -j REJECT --reject-with icmp-admin-prohibited
iptables -A OUTPUT -f -j REJECT --reject-with icmp-admin-prohibited
iptables -A OUTPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG FIN,SYN,RST,PSH,ACK,URG -j REJECT --reject-with icmp-admin-prohibited
iptables -A OUTPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG NONE -j REJECT --reject-with icmp-admin-prohibited
iptables -A OUTPUT -o lo -j ACCEPT
iptables -A OUTPUT -d 192.168.100.0/24 -p udp -m udp --dport 53 -j ACCEPT
iptables -A OUTPUT -d 192.168.100.0/24 -p udp -m udp --dport 53 -j ACCEPT
iptables -A OUTPUT ! -p tcp -j REJECT --reject-with icmp-port-unreachable
iptables -A OUTPUT -j ACCEPT
iptables -A OUTPUT -j REJECT --reject-with icmp-port-unreachable
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT DROP
ip6tables -P INPUT DROP
ip6tables -P FORWARD DROP
```

```
ip6tables -P OUTPUT DROP
```

После того, как правила заданы, закрываем терминал, снова открываем Synaptic и устанавливаем пакет iptables-persistent. Во время установки появится окно с вопросом сохранить ли правила IPv4? Нажимаем «Да». Затем, сохранить ли правила IPv6? Снова «Да». После окончания установки, закрываем Synaptic.

Затем настраиваем браузер по уже знакомой методике, с учетом правил, указанных в настройке шлюза — отключение WebRTC, передачи данных о времени загрузки страницы, возможности отправки геоданных. При этом в настройках приватности оставляем «Стандартная», для большей гибкости в работе с сайтами. Расширения также устанавливаем. При этом может быть рациональным вместо тех, что мы использовали в публичной активности, установить другие с аналогичными функциями. Насколько мне известно, расширения не влияют на уникальность цифрового отпечатка браузера. Однако полной уверенности нет. Впрочем, здесь стоит заметить, что не стоит преувеличивать опасность отпечатков, как это часто делают. Наличие уникального отпечатка не раскрывает пользователя, при условии, что он не пользуется тем же браузером для неанонимной активности. Хотя, конечно, его неотличимость от других пользователей только повысит анонимность, поскольку не позволит утверждать, что та или иная активность принадлежит одному и тому же человеку, пусть и остающемуся скрытым.

Расширения http to https и noscript на момент написания пособия не имеют полноценных аналогов, их ничем не заменишь.

Расширения ublock и privasy badger можно заменить одним расширением ghostery. Оно блокирует как рекламу, так и различные трекеры. Однако рекламу оно блокирует менее эффективно, чем ublock, по этой причине, возможно этот блокировщик рекламы кто-то захочет оставить.

В таком случае можно заменить только privasy badger. Замена ему privasy possum.

Для расширения canvas defender figerprinting мне также не известно полноценных замен.

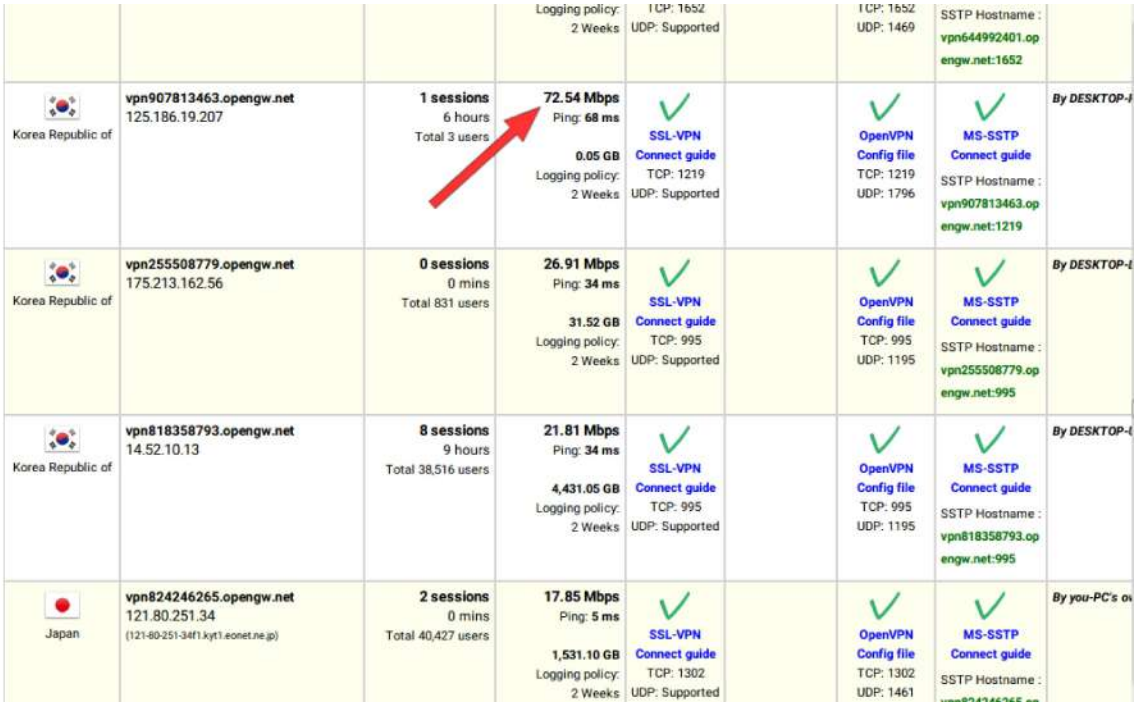
Расширение же user agent switcher можно заменить на другое с таким же названием.

После настройки перезагружаем систему.

44 Работа с VPN-сервисами

Как уже было сказано, использование VPN за Tor позволяет скрыть от сайтов факт использования Tor, позволяя обойти возможную блокировку и дополнительно повышая безопасность. Поскольку VPN-соединения требуют настройки и кроме того, те что предлагаются в данном пособии для использования, как правило, недолговечны, целесообразно настроить сразу несколько соединений, чтобы иметь возможность подключаться и менять их по мере необходимости.

Для этого идем на уже знакомый ресурс и скачиваем несколько (а лучше сразу несколько десятков) конфигурационных файлов OpenVPN. При этом есть несколько нюансов. Во-первых, Tor умеет работать только по TCP-протоколу, поэтому скачивайте конфигурационные файлы, у которых в названии фигурирует TCP, а не UDP. Во-вторых, если предполагайте пропускать через соединение тяжелый трафик, требующий высокой скорости (например видео), то необходимо позаботится о скорости VPN. Для этого смотрите в четвертом столбце скорость.



В третьем столбце указано количество соединений (sessions), и иногда их предлагают учитывать, деля величину скорости на это количество, и полученный результат, якобы, будет той скоростью, которую получите вы. На самом деле, опыт показывает, что это не так. Во-первых, данные о скорости и

количестве подключений могут быть недостоверны. Во-вторых, если большинство пользователей за этими соединениями, просто просматривают страницы с текстом или вообще не работают в сети, просто соединение установлено, то остаток скорости будет больше, чем если бы они все использовали его на полную. И наоборот, они могут забить своим трафиком канал так, что для вас в нем найдется настолько узкое место, что страницы будут грузится так долго, словно соединения с ними вообще нет. При таком раскладе, указанная величина скорости может показаться также бесполезной. Однако, в первом приближении, это очень хороший ориентир. Я рекомендую на соединения со скоростью менее 30 Мбит/с не обращать внимания. Лучше, конечно, вообще ориентироваться на соединения 100 Мбит/с и больше. Но если их будет не очень много, то можно понизить планку.

После скачивания настраиваем VPN-соединения по методике, описанной в настройке шлюза. Если необходимы высокоскоростные соединения, то каждое необходимо проверить на скорость. Сделать это можно через специальные сервисы.[2] Однако они в подавляющем большинстве для выполнения своих функций требуют активации тучи скриптов. Мы, конечно, хорошо защищены от негативных последствий их возможных вредоносных особенностей, однако само разрешение их одного за другим в ожидании, что после очередной перезагрузки страницы, сайт все-таки заработает корректно, может быть очень утомительным. Поэтому альтернативным вариантом проверки может быть запуск какого-нибудь видеохостинга (например YouTube) и запуск на нем видео в HD качестве. Также запуск Системного монитора, где отображается трафик и скорость, которую можно увидеть, пока идет видео (при проверке через специальные сайты, лучше тоже смотреть скорость в системном мониторе, а не на самом сайте). Я уже говорил, что лично для меня планкой приемлемой скорости являются 4 Мбит/с, поскольку при такой скорости можно смотреть видео в хорошем качестве без тормозов. Я не рекомендую поднимать планку выше, иначе вы рискуете потратить на поиски приемлемого VPN очень долгое время. Я не припомню, чтобы за Tor какой-либо VPN выдавал больше 10 Мбит/с. Однако 5 Мбит/с найти вполне реально. Имейте ввиду, что на системном мониторе скорость сети отображается не в Мбит/с, а в Мбайт/с. 1 Мбайт = 8 Мбит. Соответственно скорость, скажем, в 10 Мбит/с, на мониторе отобразится как 1,2 Мбайт/с. Кроме того, при активном VPN-соединении системный монитор почему-то показывает скорость вдвое больше действительной. То есть

показанию в 1,2 Мбайт/с, будет соответствовать 5 Мбит/с. Таким образом, если скорость с VPN на системном мониторе 1 Мбайт/с и выше, то можете смело оставлять такое соединение для использования. Впрочем, иногда бывает, что скорость отображается правильная или наоборот, вдвое меньшая. В свою очередь, без VPN-соединения скорость вообще не отображается, идет лишь непонятный график входящего трафика на небольшой скорости, при реальном входящем трафике. Это какой-то баг. В этом случае можно смотреть графики системного монитора шлюза. Там, соответственно, нужный уровень скорости в районе 600 Кбайт/с и выше.

Я рекомендую сохранить хотя бы несколько, а лучше десяток VPN, чтобы ими можно было пользоваться достаточно продолжительное время. Конечно существует вероятность, что все VPN, конфигурационные файлы которых вы скачали, перестанут работать на следующий день или в течении недели, но как правило 7–10 VPN хватает на месяц или даже дольше. Статистически среди такого количества находятся более-менее долгоживущие. Таким образом, обновление списка VPN, замену старых неработающих новыми рабочими вы сможете осуществлять при ежемесячном обновлении системы. Стоит иметь ввиду, что использование какого-либо VPN на постоянной основе продолжительное время позволит этому VPN собрать статистику по вашей активности, хоть вы для него и останетесь анонимным. Поэтому лучше прибегать к такому шагу только действительно в тех случаях, когда сайт отказывается открываться непосредственно через Tor.

Теперь мне хотелось бы рассказать о дополнительных браузерах. Я уже рассказывал о браузере Falkon. Сейчас хотелось бы поведать об иных, возможно они кому-то приглянутся.

45 Настройка браузера LibreWolf

Пожалуй наилучшим, с точки зрения приватности, браузером на сегодняшний день является LibreWolf.[3] Он основан на Firefox, но из него удалены многие неприятные особенности, характерные для браузера от Mozilla. Также в нем изначально выставлены более серьезные настройки безопасности. При этом, он остается полностью совместим с расширениями Firefox. К сожалению, в репозиториях Devuan его нет. Его репозитории необходимо подключать отдельно.

Открываем терминал и от суперпользователя вводим следующую строку

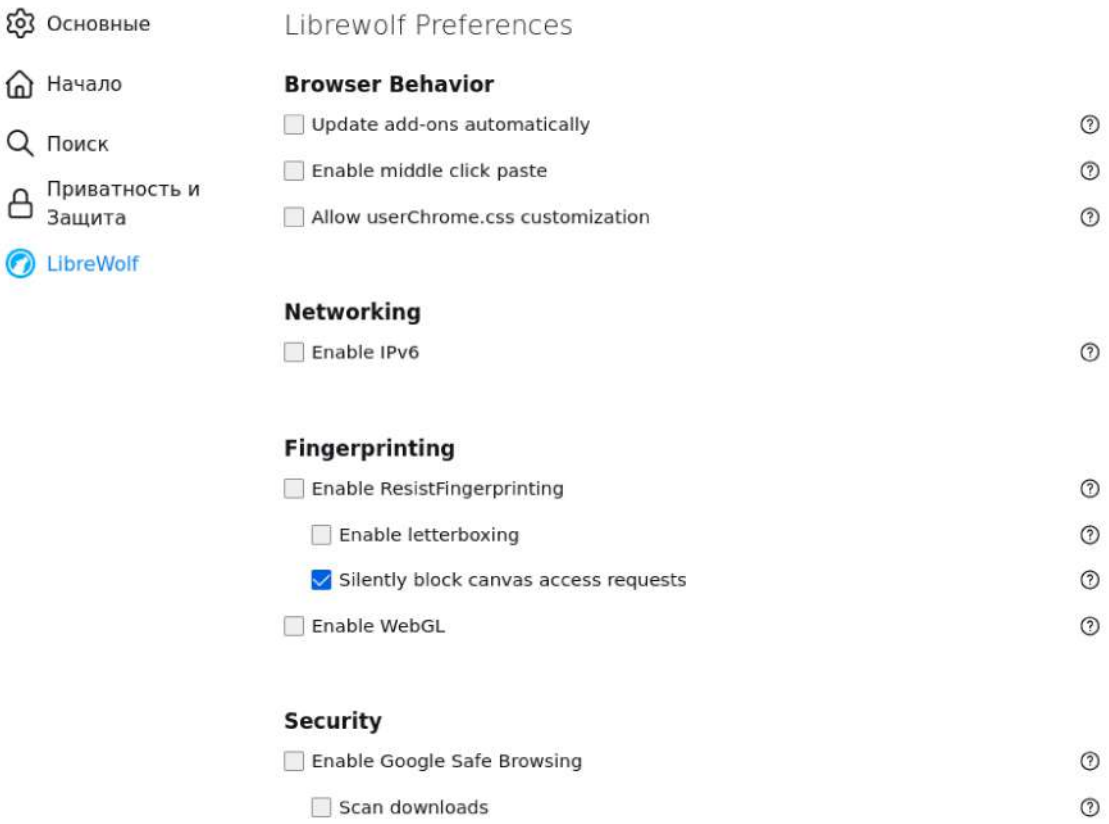
```
echo "deb [arch=amd64] http://deb.librewolf.net $(lsb_release -sc) main" | tee /etc/apt/sources.list.d/librewolf.list
```

Затем вводим строку

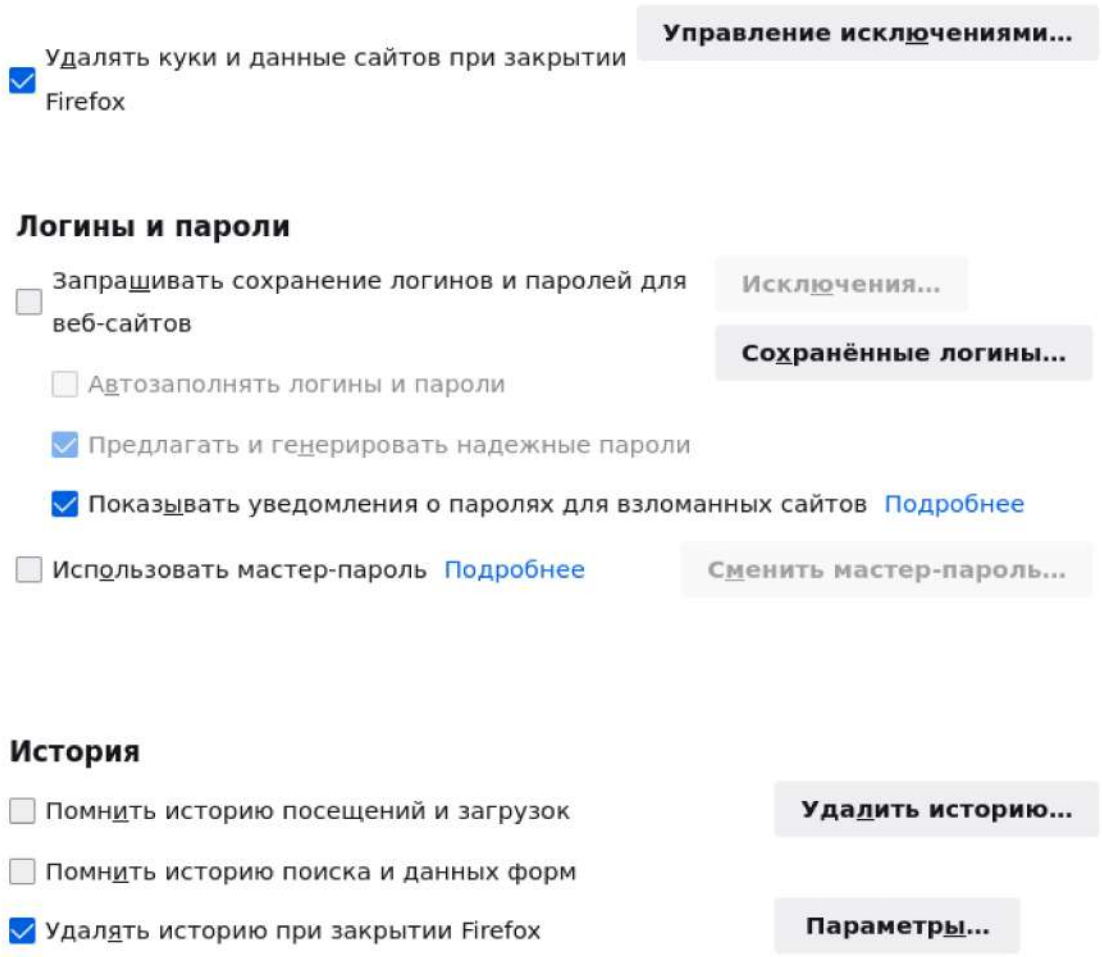
```
wget https://deb.librewolf.net/keyring.gpg -O /etc/apt/trusted.gpg.d/librewolf.gpg
```

После этого идем в Synaptic и затем в репозитории, где меняем название дистрибутива с chimaera на bullseye. Поскольку версии именно для Devuan нет, необходимо устанавливать пакеты для той версии Debian, на которой основана конкретная версия Devuan, чье название прописывается автоматически. Потому его и необходимо сменить.

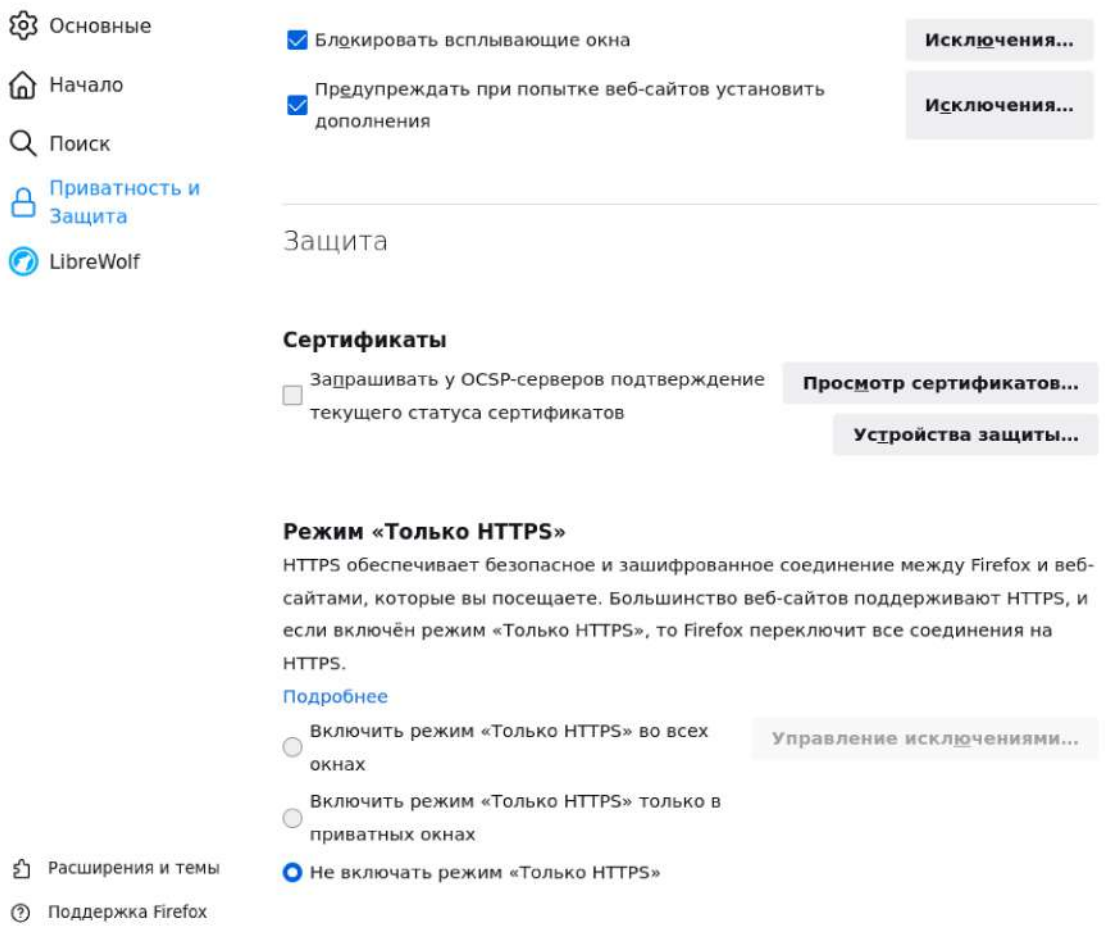
После этого обновляем список пакетов, ищем и устанавливаем LibreWolf. Перезагружаем систему и открываем браузер. Идем в «Настройки». Во вкладке «LibreWolf» снимаем все галочки, кроме «Silently block canvas access requests».



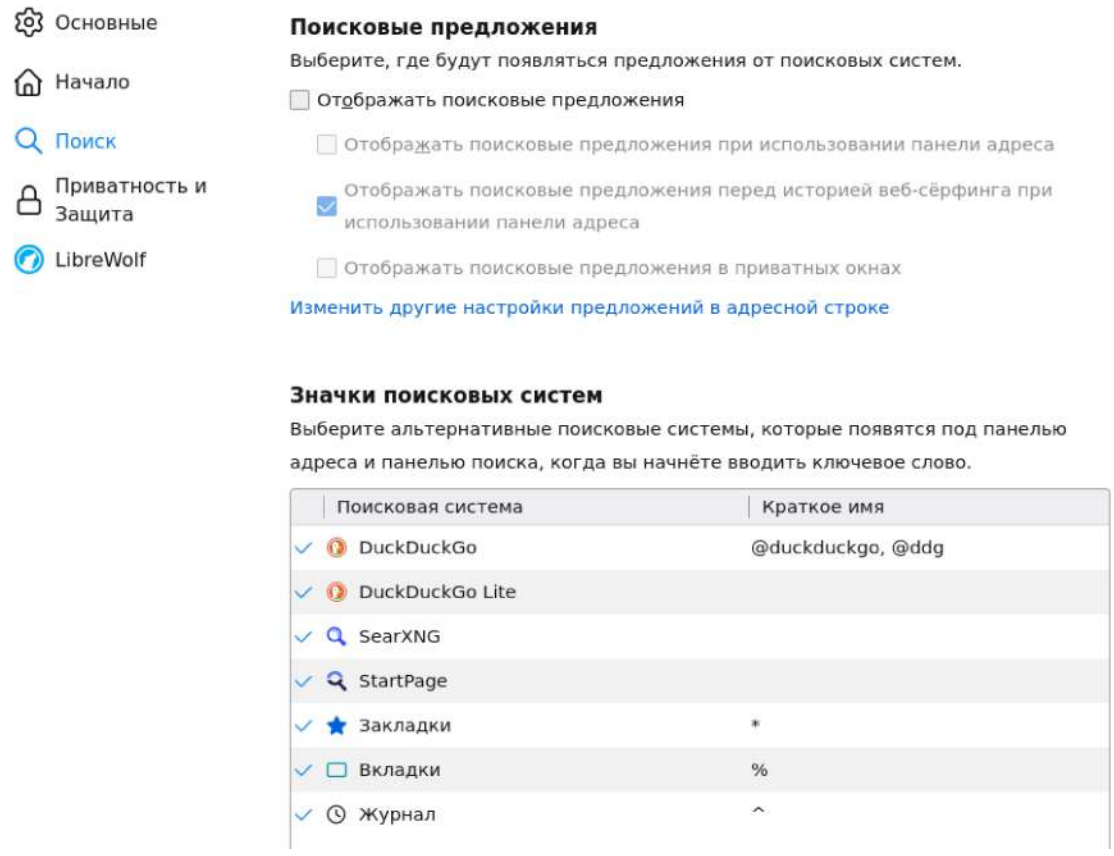
Во вкладке «Приватность и защита» проставляем удаление cookie и истории.



Также, если для вас важно удобство, можете внизу указать не включать режим «Только HTTPS».

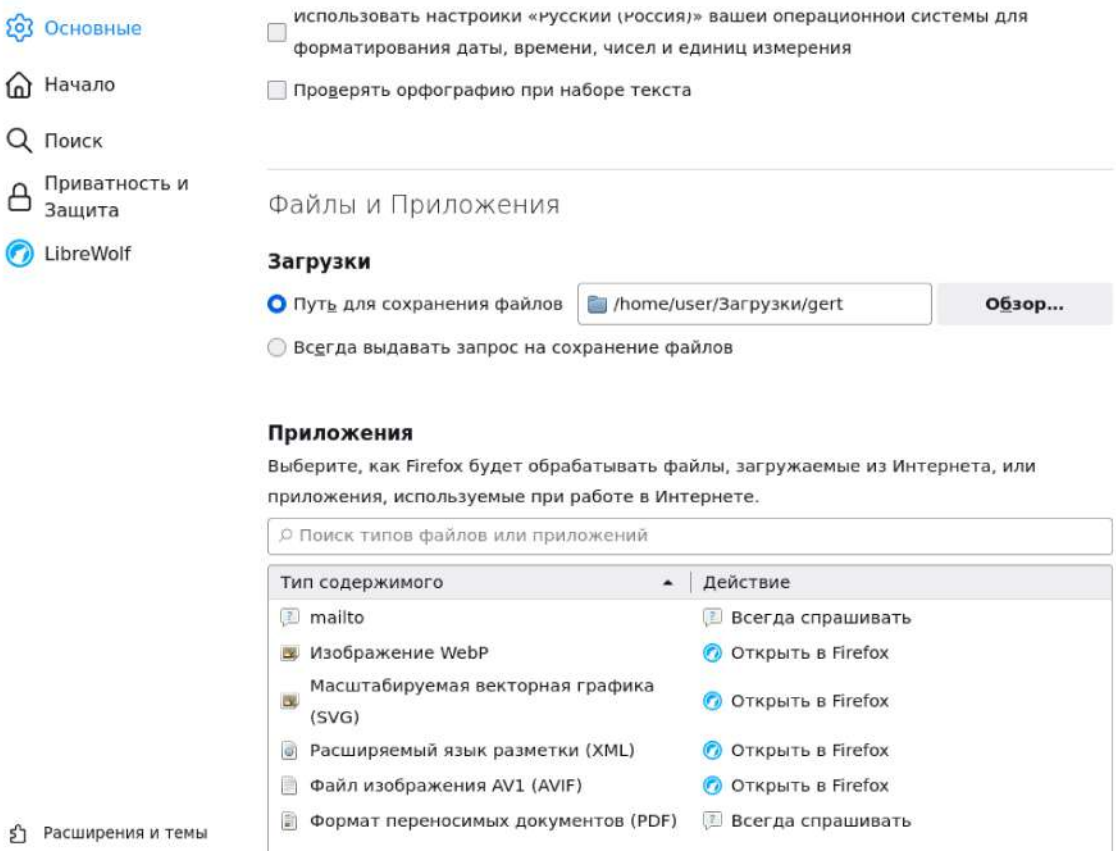


Во вкладке «Поиск» отключаем отображение поисковых запросов и удаляем все неэтичные поисковики.

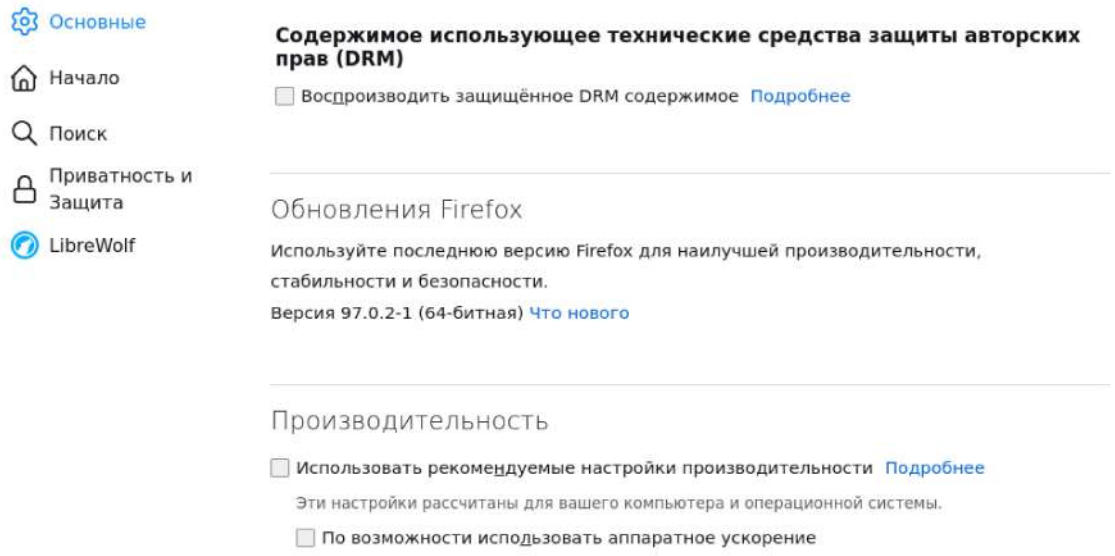


Во вкладке «Начало» все выставляем по своим нуждам.

Во вкладке «Основные» отключаем проверку орфографии и отображение PDF в браузере.



Также отключаем использование аппаратного ускорения.



Перезапускаем браузер. Заходим в about:config и производим те же настройки, что и в Firefox.

После этого идем на сайт расширений Mozilla и устанавливаем уже знакомые нам дополнения. Могу в добавок порекомендовать, например, Disconnect, блокирующий слежку жучков соц. сетей, а также Decentralise, пропускающую запросы через различные CDN-сервера, там самым затрудняя идентификацию. Также могу обратить внимание на расширение Chameleon. Это тоже подмена браузера и операционной системы, только более надежная чем та, что обеспечивается расширениями, которые мы устанавливали до этого.

Также на определенном этапе может возникнуть окно с вопросом, стоит ли запрашивать страницы на английском языке. Если ответить «Да», это также повысит анонимность.

На этом настройка LibreWolf закончена. Данный браузер я рекомендую использовать в качестве основного в этой виртуалке.

Настройки его также можно скопировать и использовать в дальнейшем.

В качестве альтернативы вы можете также использовать браузер Waterfox. Браузер Firefox с 57 версии перешел на движок Quantum. При этом для того, чтобы его расширения работали, им также необходимо было перейти на этот движок. Однако не все смогли это сделать. Проект Waterfox появился как ответвление от Firefox, этот браузер продолжает развиваться на движке, который был у Firefox ранее.[4] За счет этого в нем могут работать старые расширения, ныне не поддерживаемые в Firefox. Данного браузера также нет в репозиториях Devuan, потому его придется скачивать отдельно.

Конечно, если вам нужно, вы можете установить и браузер Falkon. Всех этих браузеров более чем достаточно.

46 Инструмент Интернет-поиска Searx

Я уже рассказывал об этичных Интернет-поисковиках. Все они являлись централизованными, т.е. все запросы в них проходят через какой-то центральный единый сервер. Однако существует поисковый инструмент, который позволяет любому поднять свой собственный поисковый сервер. Таким образом формируется распределенная сеть серверов. Называется этот инструмент Searx.[5]

В отличие от популярных централизованных этичных поисковиков, этот инструмент осуществляет метапоиск не по ограниченному количеству

поисковых баз, а по всем, какие есть. Таким образом, используя его, вы можете повысить широту охвата Интернет-пространства при поиске информации.

Чтобы воспользоваться им, перейдите на сайт, где есть ссылки на страницы различных серверов Searx и перейдите по одной из них.[6] Предложить вам сразу какой-то конкретный сервер я не могу, поскольку иногда они перестают работать. Но зато появляются новые. Такая распределенная сеть еще более снижает возможность для слежки, поскольку нет единого центра, который можно было бы скомпрометировать.

47 Настройка децентрализованного поисковика YaCy

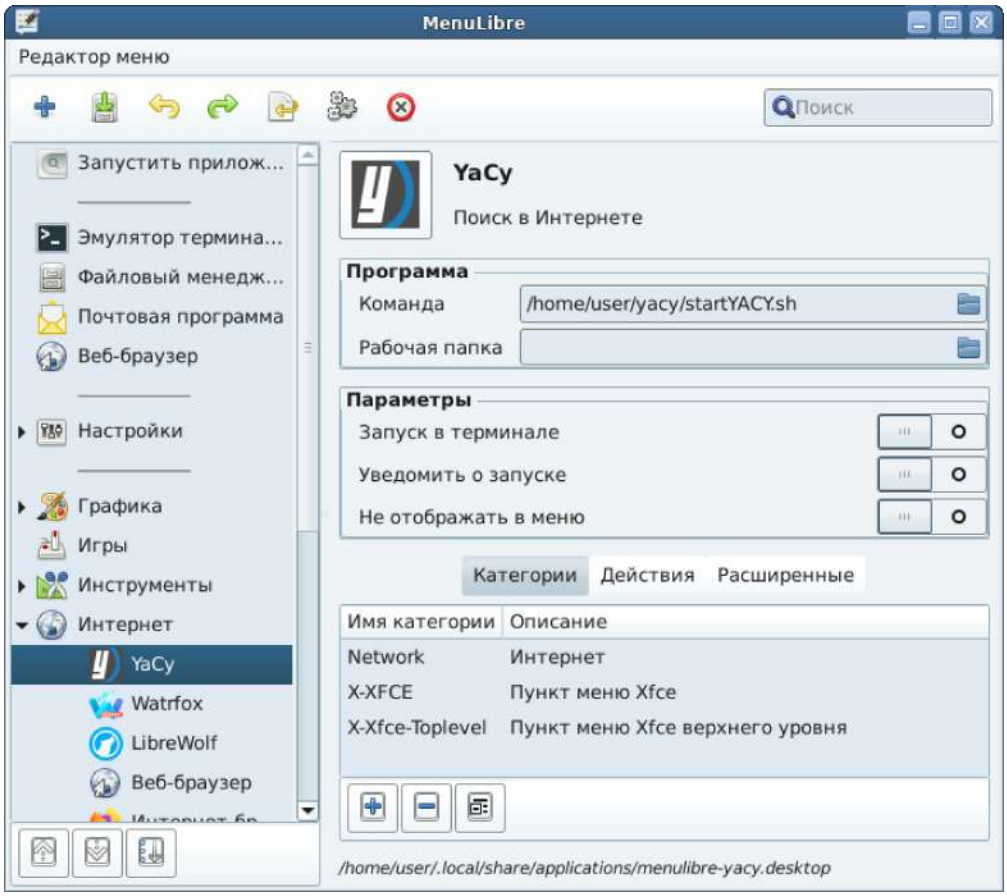
Для Интернет-поиска можно, безусловно, пользоваться этичными поисковиками, о которых уже говорилось. Однако, они являются серверными, и хотя их политика уважает пользователей, это все же потенциальная проблема. Гораздо надежнее было бы, если бы поиск не зависел от сервера, а был распределен. Если бы пользователи сами индексировали страницы и, по сути, сами были бы поисковиками. Такой децентрализованный поисковик существует.

Инструмент YaCy создает локальную поисковую машину на компьютере пользователя, благодаря которой посещенные страницы индексируются, и к ним может получить доступ через поиск таким же инструментом другой пользователь YaCy. Конечно, там довольно сложная структура предоставления индексированных страниц в общий доступ, но принцип примерно такой. Страницы, содержащие cookie или другие данные, которые могут быть классифицированы, как конфиденциальные, личные, не индексируются. Это гарантирует, что приватная информация не попадет в общий доступ.[7]

Безусловно, релевантность ответов и широта охвата Интернета у YaCy не такая, как у серверных поисковиков. Однако проект развивается.

Чтобы воспользоваться данным инструментом, как уже было сказано, необходимо установить специальное ПО. Его нет в хранилищах Devuan, поэтому скачивать придется с официального сайта.[8] После скачивания, распаковываем его в отдельную папку, идем в нее и запускаем файл startYACY.sh. С некоторой задержкой откроется страница в браузере, установленном по-умолчанию. Данную страницу можно поставить в закладки (адрес localhost:8090/index.html). Это не сайт в сети, это интерфейс локальной поисковой машины, которая теперь работает на вашем устройстве. Сама работа с YaCy осуществляется также, как и с обычным поисковиком. В дальнейшем,

после перезапуска, войдя в эту вкладку, вы не попадете на эту страницу, для этого необходимо также запустить поисковик. Поэтому добавляем ярлык программы в Меню. Значок YaCy находим следующим образом. В пользовательской папке идем в yacy, затем в addon и там выбираем YaCy_TrayIcon.png.



Можно также создать отдельный ярлык на панели. Теперь вы можете осуществлять поиск по Интернету распределенно.

48 Работа с картами OpenStreetMap

Пришло время рассказать о том, чем воспользоваться заместо несвободных сервисов карт от Google, Яндекс и т.п. Существует свободный сервис OpenStreetMap.[9] Я уже говорил о нем. Это свободный сервис карт, не принадлежащий никакой корпорации, создаваемый энтузиастами по всему миру. Если говорить о его точности, то в некоторых местах она даже превосходит точность таких сервисов как карты Google. Хотя, справедливости ради, необходимо признать, что немало мест, где их точность наоборот уступает несвободным аналогам. Тем не менее проект развивается и он во вполне

достаточной мере способен заменить шпионящие инструменты от корпораций.

Чтобы воспользоваться им перейдите на сайт.[10] Для работы необходимо разрешить скрипт. Здесь присутствует функция прокладки маршрутов. Также можно активировать дополнительные слои карты, например, схему транспорта. В целом, работа с сервисом похожа на работу с другими подобными.

49 Сервисы языкового перевода

Еще одним важным для широкого пользователя сервисом, является сервис перевода с одного языка на другой. Опять же, сервисы от крупных корпораций не подходят. Существует свободный сервис перевода. Он называется LibreTranslate. Данный проект предлагает свободное ПО для поднятия своего сервиса языкового перевода. Если вы хотите быть полностью независимыми от сторонних серверов, то можете скачать его и установить свой сервер с переводчиком. Для тех же, для кого такое проблематично, существуют уже поднятые сервисы на этом ПО. На одном из них, к сожалению, присутствует скрипт от Google.[11] Но на другом, известном мне, такая неприятность отсутствует, однако при этом он позволяет переводить за раз текст со значительно меньшим количеством символов.[12] Для работы необходима активация скрипта. В графе над левым полем выбирается язык с которого нужно осуществить перевод, над правым полем — язык, на который нужно осуществить перевод, в левое поле вводится текст для перевода. Работа с этим сервисом похожа на работу с другими переводчиками. Качество перевода отстает от более крупных сервисов. Но все же сносное.

Еще один сервис, придерживающийся относительно этичной политики Systran. Сервис перевода от Systran не хранит вводимые пользователями тексты для перевода и не собирает идентификационные данные на них. Единственное что, они используют файлы cookie, но при нашей настройке системы они не страшны.[13]

Чтобы воспользоваться переводчиком, перейдите на сайт.[14] Для работы необходима активация скрипта. В графе над правым полем выбирается язык, на который нужно осуществить перевод (по-умолчанию, скорее всего, стоит «English»), в левое поле вводится текст для перевода. По-умолчанию стоит автоматическое определение вводимого языка («Auto-Detect»), поэтому его над левым полем специально можно не указывать. В принципе, работа с этим сервисом очень похожа на работу с другими переводчиками. Касательно

качества перевода, то мои личные тесты не выявили существенных отличий от других похожих сервисов. Как и все они, на уровень профессионального перевода, который не стыдно публиковать, они не тянут. Но чтобы просто понять суть того, что написано на незнакомом языке, их вполне достаточно. И переводчик Systran в этом отношении хороший инструмент.

50 Сервис Internxt

Кому-то может понадобиться безопасное удаленное хранение файлов. Выше уже рассказывалось о сервисе MEGA, но для по-настоящему высокой приватности он может оказаться не очень удачным решением. Более приглядным выглядит сервис Internxt. Также как и MEGA он шифрует все данные непосредственно на вашем устройстве перед загрузкой на сервер. В отличие от MEGA, в нем отсутствуют инструменты общения и просмотра многих видов файлов. Зато нет и сомнительной функции восстановления доступа к аккаунту при утрате пароля. Есть отдельная программа для установки на компьютер, позволяющая осуществлять синхронизацию файлов. Также присутствует галерея и некоторые другие функции.

Помимо удаленного хранилища, Internxt предоставляет и некоторые другие услуги, например временную электронную почту, с помощью которой можно, например, произвести регистрацию на каком-то ресурсе не паля свои личные данные. К слову, на момент написания пособия, с помощью этой почты удается завести аккаунт и в самом Internxt. Временный почтовый ящик существует до тех пор, пока открыта вкладка с ним, или пока не будет нажата кнопка удаления почты. Также он удаляется по прошествии определенного количества времени.

Также Internxt предоставляет сервис конвертации величин информации, проверку надежности пароля и проверку фалов на вирусы. Возможно, эти функции кому-то пригодятся.

51 Сервис онлайн-документации CryptPad

Для некоторых важной может оказаться онлайн-документация. На замену таким сервисам как Google Docs существует свободный инструмент CryptPad. [15] Данный сервис позволяет создавать онлайн-документы различных типов — текст, электронные таблицы, презентации, рисунки, документы составления опросов, канбан, файлы редактирования программного кода. Помимо этого, CryptPad предоставляет удаленное хранилище, размером 1 Гб. Существует

возможность за плату расширить объем хранилища до 75 Гб. Также платные пакеты позволяют помещать в криптодиск файлы, размером до 150 Мб; в бесплатной версии ограничение составляет 25 Мб.

Все создаваемые и загружаемые на сервис файлы шифруются непосредственно на вашем устройстве, таким образом, даже сам сервис не сможет узнать содержимое ваших файлов.

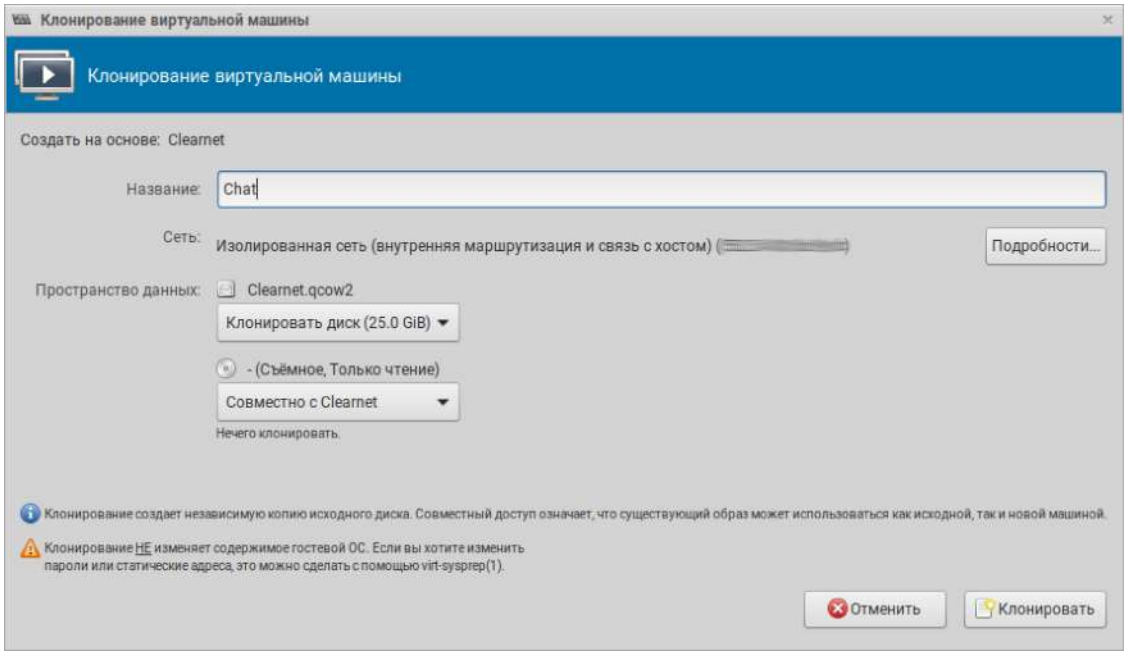
Онлайн-документацией можно пользоваться даже не создавая аккаунта. В этом случае информация о доступе к анонимной учетной записи хранится непосредственно в браузере. И соответственно, если очистить браузер после выхода из него, то вы уже не сможете получить доступ к своим документам. Информация, созданная таким способом, хранится на сервере в течении нескольких месяцев. В полноценных же аккаунтах информация хранится неопределенно долго. При этом для регистрации не требуется предоставление каких-либо личных данных. Учитывая это, я конечно же, рекомендую завести себе полноценный аккаунт в CryptPad, и тогда вы сможете, как я и предлагал, очищать браузер и производить откат виртуалки после каждого сеанса.

7 Виртуальная машина для приватного общения

52 Настройка виртуалки для приватного общения

Чтобы облегчить себе работу, мы не будем производить полноценную установку операционки на виртуальную машину, а просто скопируем и настроим уже имеющуюся. Для этого в основном окне Менеджера виртуальных машин выделяем виртуалку для приватной Интернет-активности, нажимаем наверху «Открыть», в открывшемся окне нажимаем наверху «Виртуальная машина» и выбираем «Клонировать». В появившемся окне забиваем новое имя виртуалки, нажимаем кнопку «Подробности» и проверяем, чтобы MAC-адрес

отличался от того, что был в клонируемой машине. Все остальное оставляем без изменений. Нажимаем кнопку «Клонировать» внизу справа.



Когда процесс клонирования закончится, запускаем виртуалку. После запуска нажимаем на значок Интернета на панели и удаляем появившееся новое подключение. Оно возникло из-за адаптера с новым MAC-адресом. Нажимаем на соединение «VLAN» и открываем его настройки нажатием на значок колеса внизу слева. Во вкладке «VLAN» указываем в графе «Родительский интерфейс» новый адаптер. Во вкладке «Параметры IPv4» нажимаем на ip-адрес системы и меняем его на один. То есть, если у виртуалки для приватной Интернет-активности был ip 192.168.100.2, то ставим 192.168.100.3. Это необходимо, чтобы виртуалки могли работать без конфликтов в виртуальной локальной сети при одновременном запуске. Ведь вполне может возникнуть ситуация, когда вам нужно будет одновременно запустить обе виртуалки, чтобы в одной производить Интернет-поиск или работу с какими-то другими Интернет-сервисами, и параллельно общаться. Нажимаем «Сохранить» внизу справа.

Теперь открываем файловый менеджер с правами суперпользователя, идем в коревую папку, затем в папку etc, там открываем файл hosts и в нем меняем имя компьютера, которое вписано под «localhost» на новое. Это также нужно, чтобы машины различались между собой в локальной сети за шлюзом.

Сохраняем и закрываем, после чего открываем там же файл hostname и в нем также меняем имя компьютера на тоже, которое задали в предыдущем файле. Сохраняем и закрываем.

После этого удаляем все лишние приложения, например дополнительные браузеры, оставив только один, и другие программы для работы с какими-либо Интернет-сервисами, поскольку данная виртуалка предназначена только для общения. Общение и Интернет-серфинг необходимо разграничивать по разным машинам поскольку именно Интернет-серфинг, когда вы ходите по неизвестным сайтам, представляет наибольшую угрозу. И лучше держать ваше общение, — деятельность принципиально связанную с конфиденциальными данными — от него подальше. Кроме того, инструменты, которые мы будем использовать, хранят переписку непосредственно на устройствах пользователей, и если вы не хотите ее потерять, придется отказаться от отката виртуалки к предыдущему снапшоту после каждого сеанса, тогда как при Интернет-серфинге этот откат производить необходимо. Также удаляем закладки из браузера и можно заменить некоторое расширения на аналоги по причинам о которых я уже говорил выше.

После этого перезагружаем виртуалку. После перезагрузки опять могло появиться новое Интернет-соединение в настройках сети. Проверяем это, и если так, то удаляем его.

Пора поговорить об этичных инструментах для общения.

53 Почтовые сервисы

Начнем с сервисов электронной почты. Обычные сервисы почты от корпораций, эксплуатирующих пользователей, понятное дело, не подходят. Хоть по сегодняшним временам они и не требуют привязки к номеру телефона в обязательном порядке, но только если не обнаружат признаки использования туннелирования в вашей активности или иных способов повышения безопасности с вашей стороны, например, ограничения скриптов. В этом случае они могут отказать в регистрации, или же потребовать «подтверждения личности» позже.

Существуют сервисы защищенной почты, где все письма шифруются на устройствах пользователей, и даже владельцы сервера не могут получить доступ к содержимому. Сразу скажу, что я не рекомендую пользоваться почтой, пусть и защищенной, для приватного общения. Есть более перспективные технологии, о которых я расскажу далее. Тем не менее, я все же поведаю об известных мне сервисах защищенной почты.

Самым известным из таких сервисов является ProtonMail.[16] Его я не рекомендую. Дело в том, что при регистрации требуется предоставить адрес другой электронной почты, либо номер телефона. Разработчики уверяют, что этот номер нужен только при регистрации для проверки не является ли пользователь роботом, и что он не хранится и не привязывается к аккаунту. Однако пользователями было замечено, что если воспользоваться одним из доступных в сети сервисов с виртуальными номерами, то ProtonMail, скорее всего, откажет в регистрации, заявив, что номер уже использовался. Но откуда он может знать это? Только если кто-то уже таким номером воспользовался, а ProtonMail привязал этот номер к аккаунту. Как верно заметил пользователь, отметивший это, «Не советую пользоваться сервисом, где тебя не просто обманывают, а держат за идиота уже на стадии регистрации».[17] Я сам проверил этот факт, попытавшись создать аккаунт. Также воспользовался сервисом с виртуальными номерами и столкнулся с тем же самым. Так что эта проблема никуда не делась. Некоторое время ProtonMail не требовал указания номера телефона или адреса почты в обязательном порядке, но требовал введения капчи, через сервис reCapcha, принадлежащий Google и нацеленный на шпионаж. При нашей организации подключения, мы надежно защищены от

возможных сливов в этом случае, но теперь такая возможность исчезла. В качестве варианта, остается возможность создания почты на каком-нибудь ширпотребном сервисе, использование его для подтверждения аккаунта при регистрации в ProtonMail. Но учитывая сомнительные моменты данного сервиса, сомнительно, что он стоит этих усилий.

Следующим сервисом, о котором хотелось бы сказать, является Riseup.[18] Этот сервис, в отличие от предыдущего, не имеет подводных камней. Хотя на него и оказывалось давление со стороны ФБР, в результате чего разработчикам пришлось убрать информирование о том, что в отношении пользователей не поступало запросов от властных структур.[19] Тем не менее, нет свидетельств, что чьи-то данные в этой почте были скомпрометированы. Это действительно надежный защищенный сервис. Однако вряд ли кому-то доведется им воспользоваться. Дело в том, что для регистрации нужно получить инвайт — эдакий залог от уже действующего пользователя Riseup. И таким образом, если у вас нет знакомого криптоанархиста, путь на данный сервис вам закрыт.

Также существует сервис Mailbox.[20] Он достаточно надежный и, пожалуй, именно его стоит рассматривать в качестве первостепенной рекомендации. Правда стоит отметить, что мне так и не удалось произвести на нем регистрацию. С перерывом примерно в месяц я дважды пытался это сделать, но на странице регистрации всякий раз появлялось уведомление, что регистрация временно приостановлена и стоит попробовать позже.

Ну и последний известный мне сервис, это Tutanota.[21] По информации в сети, он представляется достаточно безопасным и удобным. Правда есть информация, что правительство Германии через суд принудило разработчиков внести в него бэкдор.[1] Разработчики собирались оспаривать это решение. К сожалению, мне не удалось выяснить, чем закончилась эта история. Это повод поставить под сомнение безопасность и этой почты. Кроме того и здесь я столкнулся с проблемой при регистрации. Если несколько лет назад удавалось спокойно создать учетную запись, заходя через Tor, то сейчас уже после внесения всех данных, сервис заявляет, что регистрация с данного ip приостановлена. Это проявляется не только при использовании Tor, но и при использовании VPN. Похоже Tutanota все же взялась за идентификацию пользователей, хотя продолжает писать о желательности использования средств анонимизации. Тем не менее, если кому-то очень нужна защищенная почта, то Tutanota можно рекомендовать.

54 Сервисы VoIP

Обычные сервисы IP-телефонии для приватного общения не подходят. Все они централизованные, и в подавляющем большинстве требуют при регистрации адрес почты или номер телефона. Но есть пара инструментов, на которые я хотел бы обратить внимание.

Во-первых, это Mumble — инструмент аудиосвязи для гейминга.[2] Несмотря на то, что разрабатывается он с ориентиром на геймеров, пользоваться им может любой желающий. Отличительной чертой Mumble является отсутствие центрального сервера. Пользователи сами поднимают сервера, маршрутизирующие связь между теми, кто к ним подключен. Таким образом создаются комнаты для общения, к которым каждый может присоединиться. Несмотря на достаточно хорошую реализацию, с точки зрения безопасности, рекомендовать этот инструмент широкому пользователю нельзя, поскольку присоединяться к серверам, доступ к которым открыт, плохая идея. Ведь связь в них осуществляется всех со всеми, и скорее всего, там вы натолкнетесь на безостановочный говор других людей. А настройка своего сервера достаточно сложна и неискушенный человек вряд ли станет этим заниматься. Тем не менее, как дополнительный вариант, Mumble потенциально можно рассматривать, как достойное средство связи.

Во-вторых, это Jitsi Meet.[3] Этот инструмент использует протокол WebRTC, благодаря чему видеосвязь с помощью него можно осуществлять через обычный браузер.[4] Для этого, конечно, WebRTC в нем должен быть включен. При нашей организации Интернет-подключения слива ip при этом произойти не должно, поэтому такую связь можно считать безопасной. Само общение, происходит со сквозным шифрованием. Первоначальное формирование каналов связи между устройствами происходит с помощью сервера, однако далее связь осуществляется непосредственно между участниками, если их всего двое. В случае большого числа общающихся, при видеоконференциях, связь маршрутизируется через сторонний сервер. Однако, в данном случае невозможно формировать базу контактов. Каждый сеанс связи происходит в одноразовой комнате. Подобная организация подойдет, конечно, не всем. Однако, это весьма хороший инструмент. Сам сервис очень функционален. К сожалению, там есть некоторое пересечение с несвободными инструментами, например, предлагается использовать календари от Google и

Microsoft, чего делать категорически не следует. Несмотря на это, данное средство связи можно рекомендовать тем, кому нужна безопасная организация видеоконференций. Необходимо, правда, отметить, что у сервиса на сегодняшний день, к сожалению, нет средств эхоподавления, и при использовании колонок, вы можете получить очень неприятное пищание и скрежет, обусловленное возникновением аккустической обратной связи.[5] То есть, когда ваш голос исходит из колонок собеседника, его микрофон это улавливает, выдает в ваши колонки, их звук улавливает ваш микрофон и т.д., таким образом, эхо беспрерывно нарастает, сливается в жуткий писк и треск, что не только губит качество связи, но и может даже повредить аудиосистему. Для предотвращения этого, собеседником желательно использовать вместо колонок гарнитуру.

Использование данного сервиса осуществляется через сайт.[6]

Подобные средства связи, безусловно, можно рекомендовать, однако, как уже было сказано, они подойдут далеко не всем. А о том, что подойдет, я расскажу далее.

55 Безопасные инструменты для общения

Существует много свободных и безопасных средств для общения. Некоторые из них являются федеративными, в них сервер может поднять любой, и нет какой-то одной корпорации, которая бы контролировала их. Таковым является, например, протокол XMPP.[7] Существует большая распределенная сеть серверов, работающая на данном протоколе.[8] С помощью него возможно общаться используя различные технологии сквозного шифрования, OpenPGP,[9] OTR[10] и OMEMO.[11] Последний сочетает в себе преимущества первых двух.[12]

Для того, чтобы воспользоваться услугами того или иного сервера, необходима специальная программа, например Gajim[13] или Dino.[14]

Существуют, правда сведения, что есть возможность расшифровать переписку, ведущуюся с использованием OMEMO, если сервер хранит логи.[15]

Есть иные инструменты для общения, более современные и удобные, реализация сквозного шифрования которых, возможно, более удачная, и безопасность которых, соответственно, выше.

Таким относительно новым протоколом общения является Matrix. Эта технология также позволяет поднимать собственный сервер, что дает возможность строить федеративную сеть, и обеспечивает сквозное шифрование. [16]

Существуют разные клиенты для общения через данный протокол. В репозиториях Devuan присутствует клиент Quaternion.[17] Его к сожалению, никак нельзя рекомендовать, поскольку он до сих пор чрезвычайно сырой. Работает нестабильно, имеет крайне ограниченный функционал, позволяя только обмениваться сообщениями, а также не позволяет производить регистрацию. То есть, для его использования, вам уже необходимо иметь аккаунт Matrix.

Еще один клиент Nheko Reborn.[18] Он также присутствует в репозиториях Devuan — название пакета nheko. В отличии от Quaternion, данный клиент имеет полный функционал. В том числе присутствует функция регистрации. К сожалению, нормально поработать в данном клиенте у меня не получилось, поскольку он всякий раз вылетал через несколько секунд после запуска. В чем причина сбоя, я так и не разобрался. Также разработчики предупреждают, что хотя текущая реализация сквозного шифрования функционирует вполне корректно, она может иметь некоторые ошибки, которые, в свою очередь могут негативно сказаться на безопасности. Кроме того, может потребоваться загрузка ключей перекрестной подписи в другом клиенте. Также могут иметься проблемы с резервным копированием ключей.[19]

Наиболее функциональным и стабильным клиентом является Element.[20] Стоит, однако, отметить, что сервера, которые предлагает команда Element для поднятия своих узлов Matrix принадлежат Amazon, о чем сказано в их Политике конфиденциальности.[1] Данная корпорация известна различными пакостями в отношении пользователей.[2] Этот неприятный момент, однако, не несет рисков для пользователей самого клиента.

Существует еще один федеративный инструмент для общения — Status. На

самом деле, Status, это не только инструмент общения, но также электронный кошелек со своей криптоволютой и Web3-браузер.[3] Однако приложение для компьютера располагает функционалом только для общения.[4] Связь в Status может осуществляться через ноды, которые поднимают энтузиасты. При этом возможно осуществлять оффлайн-отправку. Но также можно и отказаться от использования каких-либо нод, и производить общение, связываясь с собеседниками напрямую. Также можно поднять собственную ноду, и осуществлять оффлайн-отправку сообщений через подконтрольный вам самим узел. Сообщения, передаваемые через ноды, хранятся на них в течении месяца, после чего удаляются.

Клиент для компьютера сейчас, к сожалению, не развивается, поскольку разработчики Status сосредоточились на мобильном приложении и развитии своей инфраструктуры. Но его все же можно скачать и использовать.[5]

Существуют средства заточенные сугубо на децентрализованную связь, т.е. осуществляемую непосредственно между собеседниками.

Одним из таких инструментов является Tox.[6] Для общения по этому протоколу можно использовать клиенты qTox[7] или uTox.[8] Они есть в репозиториях Devuan и в целом очень похожи.

Еще одним децентрализованным средством для общения является Jami.[9] Он достаточно стабильный. Если версия в репозиториях Devuan не слишком свежая, можно подключить отдельные с сайта.[10]

Также существует инструмент Briar.[11] В отличии от Tox и Jami он имеет высокую стабильность связи. В него уже интегрированы функции пропускания трафика через Tor, поэтому нет необходимости подключать виртуалку с ним к шлюзу. К сожалению, в нем пока не реализован функционал подключения к сети Tor через мосты, что является серьезной проблемой. Кроме этого, в отличии от мобильной версии, в нем отсутствуют и некоторые другие функции, например блоги.[12] В общем, хоть Briar является весьма перспективным инструментом, на данный момент его использование может быть проблемой.

Также существует комплексный децентрализованный инструмент коммуникации со сквозным шифрованием. Помимо обмена сообщениями, голосовой и видеосвязи, файлообмена, в нем также присутствует децентрализованный почтовый сервис, возможность открывать свои каналы, форумы, выкладывать публикации. Называется он RetroShare.[13] Необходимо

отметить, что RetroShare имеет довольно ощутимые проблемы безопасности. Независимые проверки выявили высокую поверхность атак и большую плотность уязвимостей в коде.[14] Однако, RetroShare продолжает развиваться, и возможно, проблемы уже во многом устранены. Данное средство связи возможно интегрировать с Tor.

Существует репозиторий для подключения и скачивания RetroShare,[15] однако в нем находятся только нестабильные версии для 32-битной архитектуры, что нам не подходит. Поэтому скачивать лучше отдельным файлом.[16]

Функционал RetroShare крайне широк. К сожалению, он не всегда работает стабильно, поэтому данный инструмент подойдет далеко не всем.

56 Настройка виртуалки для общения через Session

Наиболее стабильным инструментом для приватного общения является Session. Его я считаю наиболее оптимальным для простого пользователя. Этот инструмент формирует свою собственную сеть серверов, и подключение в нем организуется по принципу Tor, — трафик пропускается последовательно через три узла.[17] При этом он подключается к слушающему серверу, который координирует пересылку сообщений собеседникам, а также некоторое время хранит их, что позволяет осуществлять оффлайн-отправку. То есть, связь между собеседниками осуществляется следующим образом — один посылает зашифрованное сквозным шифрованием сообщение, оно проходит через цепочку узлов и попадает на слушающий сервер собеседника, а оттуда пересылается через цепочку узлов ему. Если собеседника на данный момент нет в сети, то сообщение может некоторое время храниться на сервере. Когда же собеседник появится в сети, сообщение будут отослано с сервера ему. Слушающий сервер не является как таковым сервером координации, на нем не осуществляется регистрация, как это происходит в XMPP или Matrix. И узлы для построения анонимизирующей цепочки, и слушающий сервер выбираются случайным образом из общего роя.[18]

Поскольку данный инструмент имеет свои встроенные функции анонимизации трафика, его не имеет смысла использовать в сочетании с Tor, а значит для общения через него нужна отдельная виртуалка. При такой организации отсутствует разделение между средой подключения и той в которой осуществляется активность. Однако, поскольку здесь речь идет не о

Интернет-серфинге, риски крайне незначительны и связаны в основном с опасностью активировать вредоносный код, полученный при общении. Поэтому стоит с крайней осторожностью скачивать и тем более открывать файлы от незнакомых контактов.

Создание виртуалки аналогично созданию машины для публичной Интернет-активности. Установка же операционной системы больше похожа на установку системы для приватной активности — локализацией указываем Соединенное Королевство (чтобы время в системе соответствовало нулевому часовому поясу).

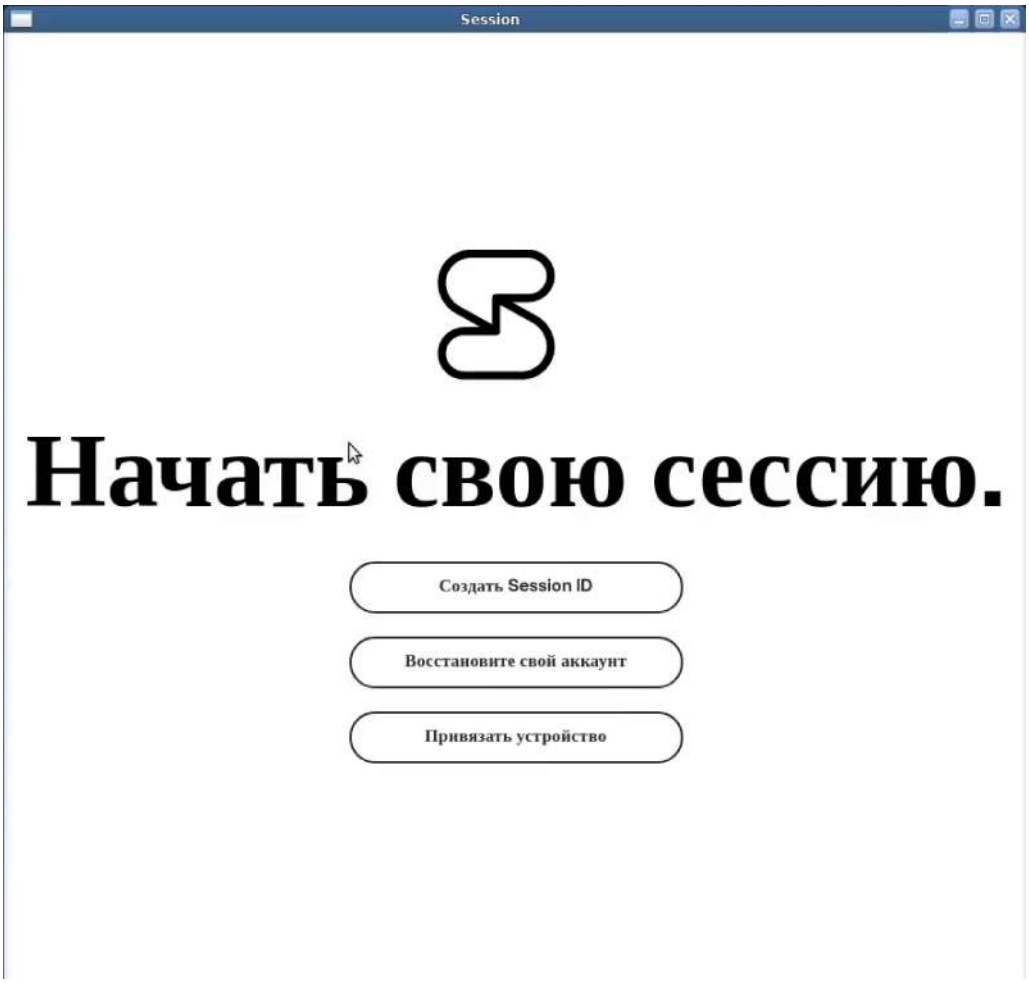
Настройка системы после установки также по уже известной методике. Настраиваем внешний вид, обновляем, удаляем пакет telnet, устанавливаем Bleachbit, GDebi, gnome-system-monitor, gnome-system-tools, libreoffice-l10n-ru, firefox-esr-l10n-ru, curl, ecj, caja, menulibre. Настраиваем автовход в систему.

Настройку браузера можно не проводить, поскольку он в этой системе не понадобится. На всякий случай можно только по уже знакомой методике все выставить в меню настроек.

После того, как система настроена, скачиваем клиент Session с официального сайта.[19] Скачивается он единым файлом, который и запускается. Можно с помощью редактора меню по уже знакомой методике создать его ярлык. После этого запускаем клиент. Если запуск не удастся, то откройте свойства файла, пройдите во вкладку «Права» и отметьте галочкой

«Позволять выполнение файла как программы».

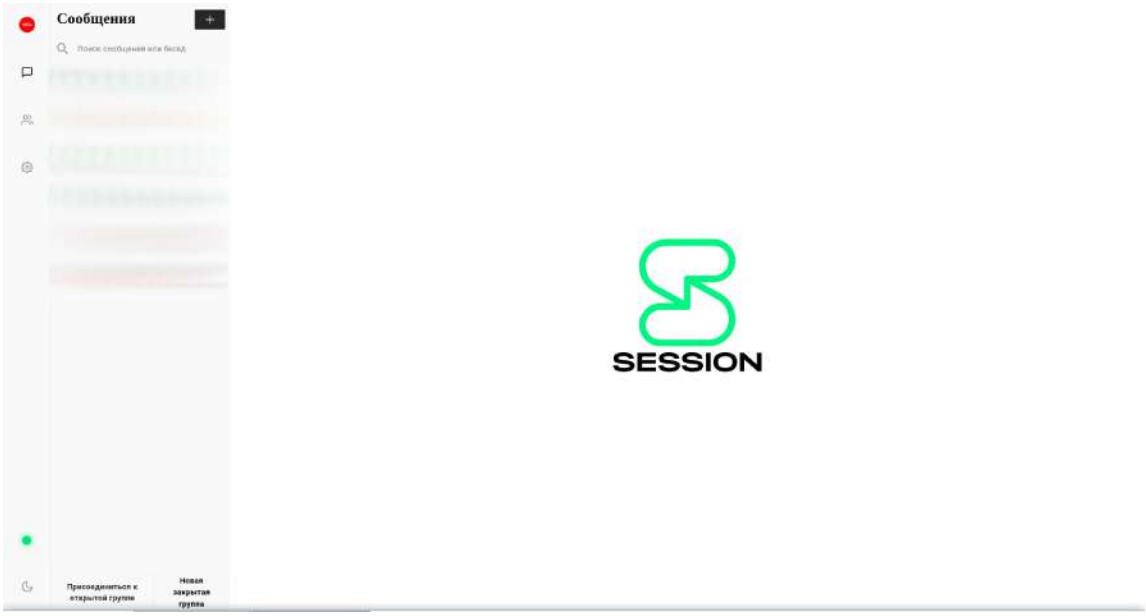
Открывается окно в котором предлагается создать либо восстановить аккаунт.



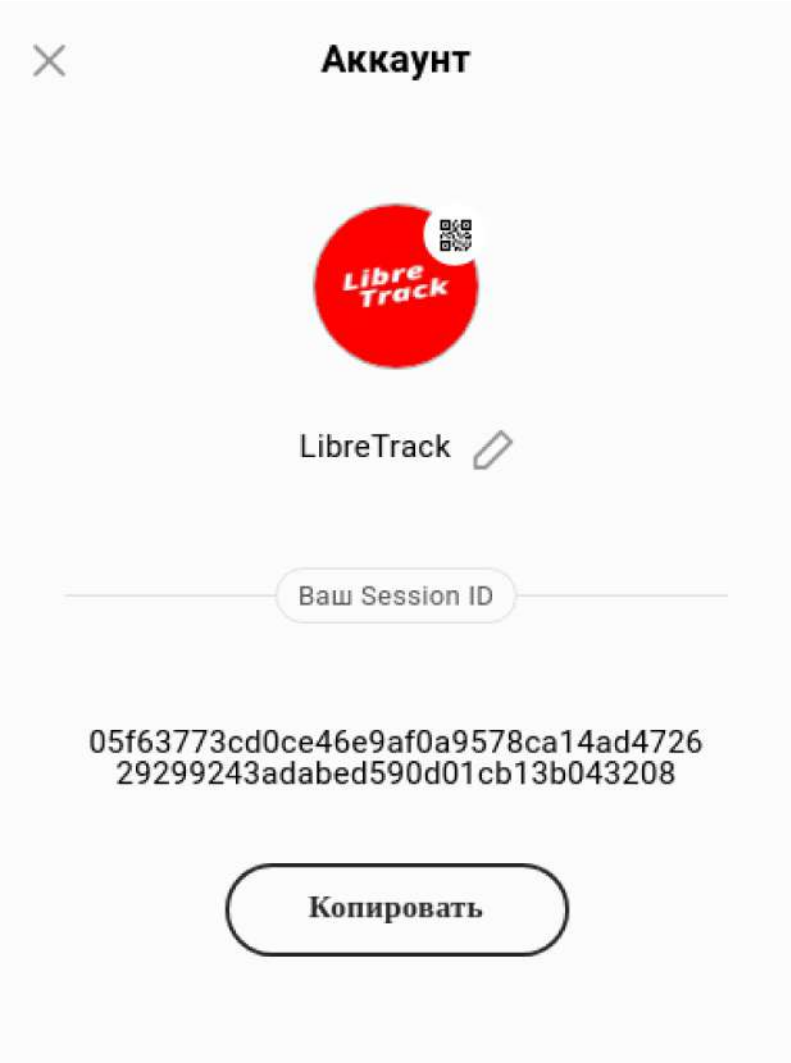
Если у вас есть учетная запись на устройстве, где вы сохраняли секретную фразу, то можете нажать «Привязать устройство». После этого необходимо ввести секретную фразу и нажать «Восстановить Session ID». После этого откроется основное окно клиента. Кнопка «Восстановите свой аккаунт», это по сути, то же самое, только при введении секретной фразы необходимо также указать ник.

Если аккаунта еще нет, то нажимаем «Создать Session ID». Высветится наш идентификатор, который лучше скопировать в менеджер паролей. После этого нажимаем «Продолжить». Вводим ник и нажимаем «Продолжить».

Открывается основное окно клиента.



Если нажать на значок вверху слева, откроются данные нашего аккаунта. Здесь можно изменить ник, фото, скопировать идентификатор, который нужно передать собеседникам для установления канала связи.



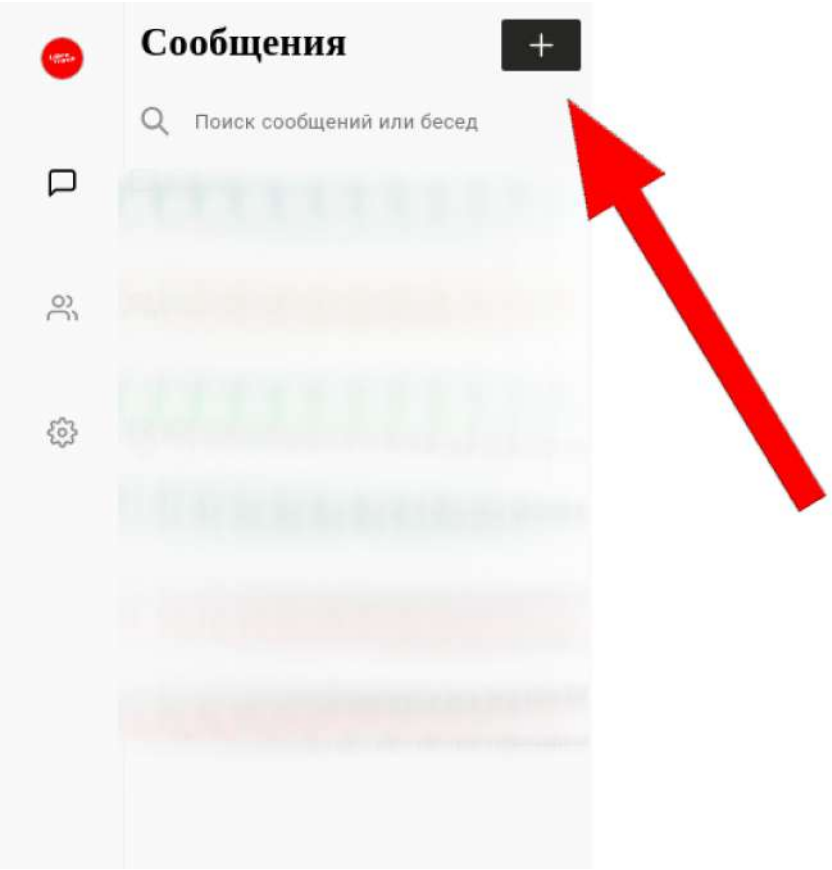
В самом низу слева в основном окне находится кнопка быстрой смены темы. Над ней точка, при нажатии на которую выскакивает окно, отображающее цепочку подключения с указанием стран узлов. При наведении мыши на узлы, отображаются их ip.

Под значком аккаунта в основном окне находятся еще три значка. Самый нижний, это настройки. Здесь во вкладке «Конфиденциальность», если хотите отправлять голосовые сообщения, необходимо активировать «Микрофон». Если хотите осуществлять звонки, то активируйте «Голосовые и видеозвонки». Во вкладке «Посмотреть запросы на переписку» отображаются запросы в контакты. Если кто-то вам напишет, его сообщение попадет сюда, пока вы ему не ответите и не примите в контакты. Пока вы этого не сделаете, вы также не сможете видеть его ник, только идентификатор. Аналогично и если вы кому-нибудь напишите, пока он вам не ответит, он не увидит вашего ника.

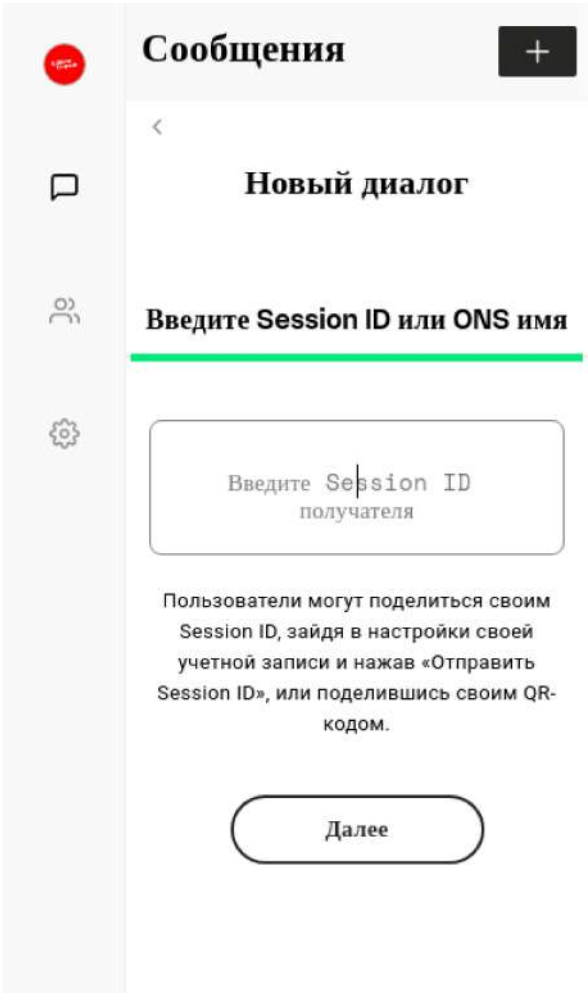
Первый значок сверху под иконкой аккаунта, это список диалогов. Если на него нажать, рядом отобразится список чатов и групповых чатов. Также

присутствует строка поиска, чтобы легко можно было найти нужный диалог. Второй значок сверху под иконкой аккаунта, это контакты, где отображаются, соответственно, контакты.

Чтобы добавить новый чат, во вкладке разговоров нажимаем на черный значок «плюс» вверху справа от надписи «Сообщения».



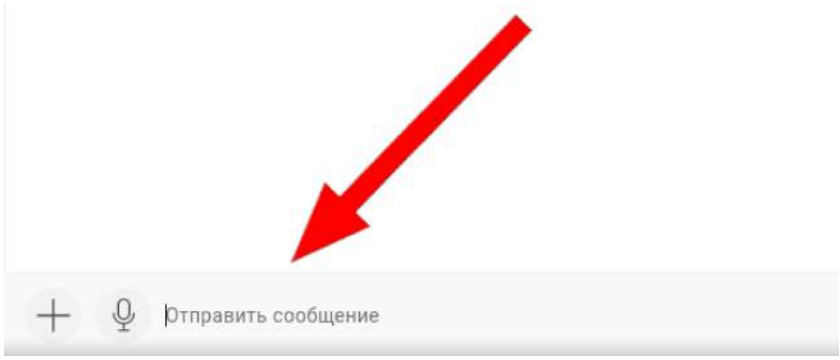
Откроется окно, где необходимо ввести идентификатор собеседника, после чего нажать «Далее».



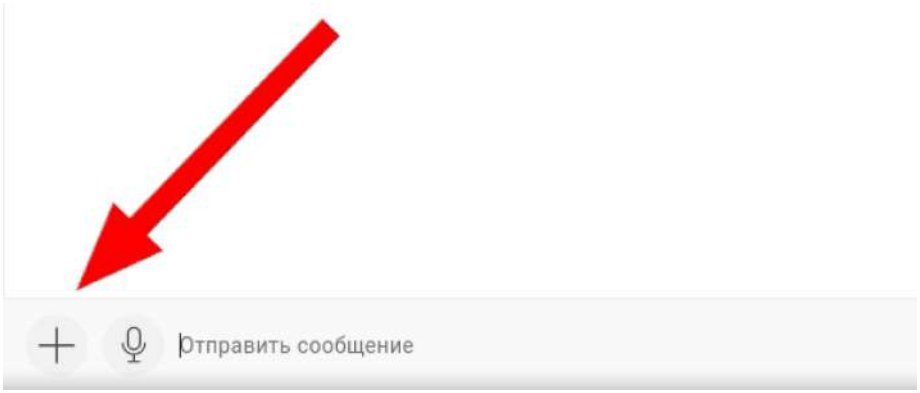
Появится новый контакт и можно будет отправить ему сообщение. Как уже было сказано, пока он вам не ответит, его имя видно не будет. После ответа подпись контакта смениться с идентификатора на ник.

Если в окне диалога нажать на иконку справа сверху, то откроется окно настроек диалога, где можно указать, через какое время сообщения будут исчезать из переписки, выставив «Исчезающие сообщения». Также можно посмотреть медиафайлы, присутствующие в диалоге и другие типы файлов. Кроме этого, некоторые настройки диалога можно открыть нажав на три точки вверху слева.

Чтобы отправить сообщение, набираем его текст в поле «Отправить сообщение» внизу и нажимаем Enter.

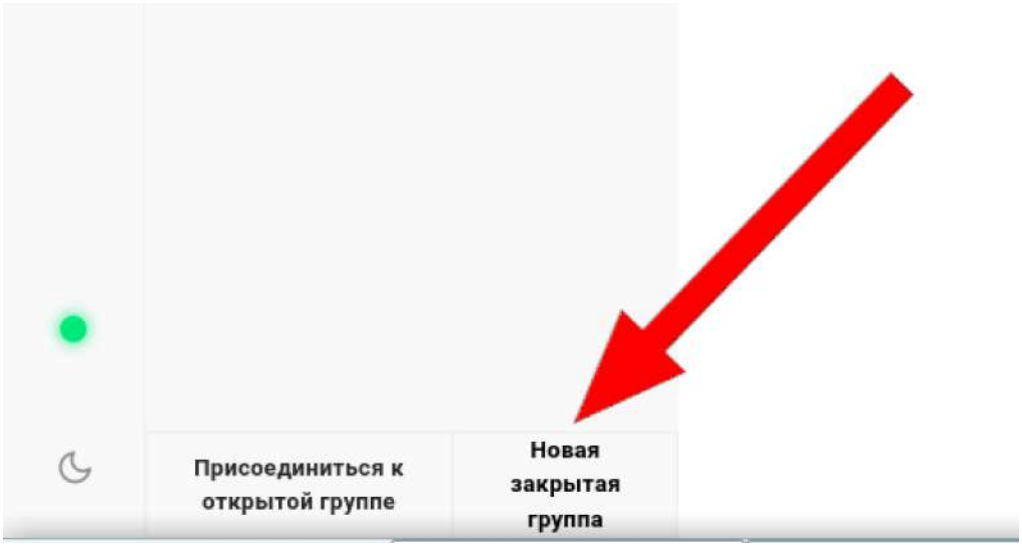


Чтобы отправить файл, нажимаем на значок «плюс» слева от поля ввода и выбираем нужный файл.

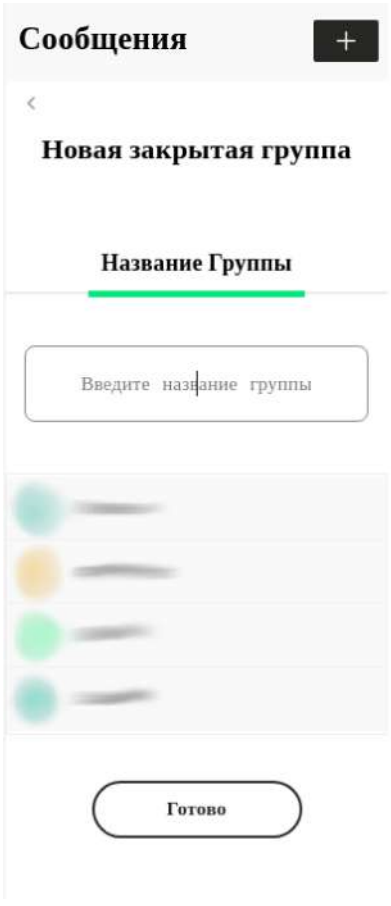


Чтобы осуществить звонок, нажимаем на значок трубки вверху справа.

Такого общение в чате. Чтобы создать групповой чат, нажимаем на кнопку «Новая закрытая группа» внизу слева.



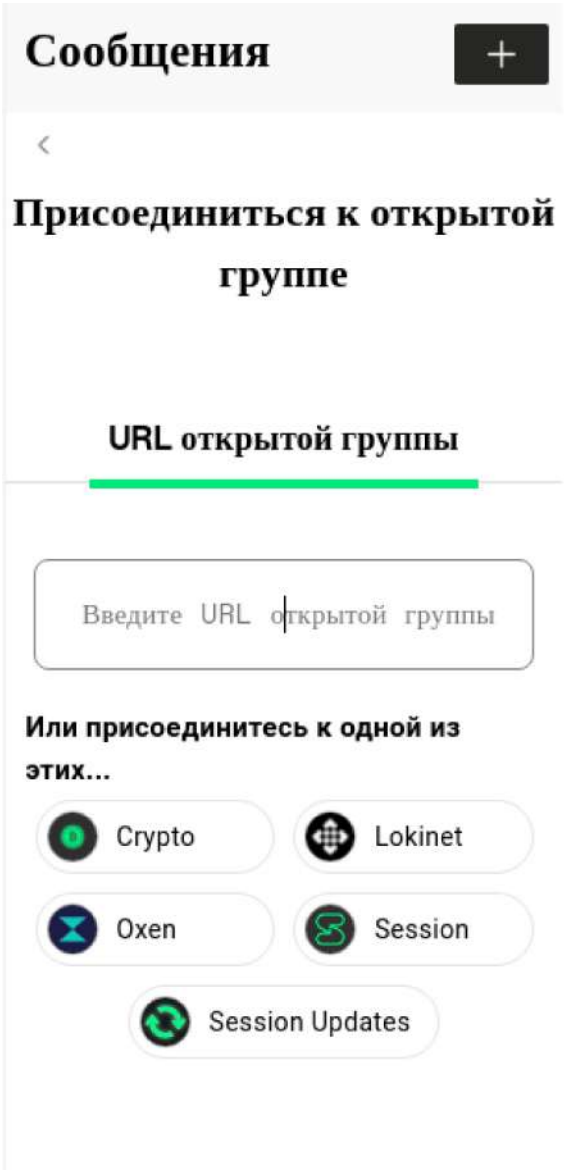
После этого необходимо ввести название группы, отметить ее участников из контактов и нажать «Готово».



Общение в группе такое же, как в обычном чате, только отсутствует возможность совершать звонки.

Чтобы присоединиться к открытой группе, нажимаем «Присоединиться к открытой группе» внизу слева.

После этого необходимо указать адрес группы и нажать «Далее».



Общение в открытой группе аналогично общению в закрытой.

Вот и вся методика работы с Session.

Далее стоит рассказать об этичных социальных сетях и сервисах микроблогинга.

57 Социальные сети и сервисы микроблогинга

Существует довольно много социальных сетей функционирующих без центрального сервера. В них свой узел может поднять любой, и пользователи вольны выбирать на каком узле создать свой аккаунт. Такие федеративные социальные сети формируют объединение Fediverse.[20] Пользователи ресурсов, входящих в это объединение, могут обмениваться информацией с другими пользователями, как того ресурса, которым пользуются они, так и других.

Одной из наиболее развитых таких социальных сетей является Friendica.[1] Она обладает широким функционалом и хорошей интеграцией с другими ресурсами. Помимо нее существуют также GNU social,[2] Funkwhale,[3] Hubzilla[4], Pixelfed.[5] и Mastadon.[6] Еще есть соц. сеть Diaspora.[7] Не знаю, как у остальных упомянутых, но у последней есть серьезная проблема. Дело в том, что владельцу сервера, на котором вы создаете свой аккаунт, может быть доступно содержимое этого аккаунта, в том числе личная переписка.

Из отдельных федеративных проектов можно упомянуть сеть Movim, основанную на XMPP.[8]

Вообще федеративная организация, как уже говорилось, не самая надежная с точки зрения безопасности. Существует, однако, полностью децентрализованная социальная сеть Pandora.[9] Она обеспечивает связь непосредственно между пользователями. Информация, которую вы передаете определенному человеку, поступит только ему. Это позволяет организовывать безопасное общение. Для того, чтобы воспользоваться данной сетью, необходимо установить на компьютер специальное ПО.[10]

При такой организации не реализуется одна из главных функций социальной сети, возможность демонстрировать публикации широкой аудитории.

Эти функции, однако, реализуются в свободном сервисе микроблогинга Twister.[11] Также, как и Pandora, он полностью децентрализованный. Следствием этого, к сожалению, является то, что если у вас мало подписчиков, то при выходе из сети, ваши посты могут стать недоступными для просмотра. Тем не менее, это очень хороший сервис, не подверженный цензуре и контролю каких-то организаций.

58 Сервисы самоуничтожающихся сообщений

В определенных ситуациях могут пригодится сервисы, с помощью которых возможна отправка сообщений, которые будут удалены сразу же после прочтения. Например, для обмена ключами других инструментов общения.

Одним из таких сервисов является TMWSD.[12] Он не требует для работы java-скриптов, все сообщения шифруются. После создания сообщения, необходимо по какому-либо каналу связи передать ссылку на него тому, кому сообщение предназначено. После того, как ссылка будет открыта, сообщение

удалится с сервера, и после закрытия страницы браузера, его уже нельзя будет увидеть.

Еще один подобный сервис OneTimeSecret.[13] Его функционал и реализация идентичны. Обращаю внимание, что в Интернете есть ресурсы с похожим названием и даже идентичным оформлением. Ни в коем случае не перепутайте. Такие сервисы могут оказаться мошенническими. Работа же с данным сервисом такая же как и с предыдущим.

Сервисы самоуничтожающихся сообщений могут выполнять очень широкий спектр задач. Я указал наиболее важные.

---

1 Полное пособие по вычислительной свободе https://share.internxt.com/d/sh/file/329ff2c9358a0da0535f/8d5a8b6123e3182e0c5749cbb929d60862238fdece8ec125413821badd519776

2 Об аппаратных закладках можно почитать в Википедии https://ru.wikipedia.org/wiki/%D0%90%D0%BF%D0%BF%D0%B0%D1%80%D0%B0%D1%82%D0%BD%D0%B0%D1%8F_%D0%B7%D0%B0%D0%BA%D0%BB%D0%B0%D0%B4%D0%BA%D0%B0. Также этот вопрос освещается в статье по этой ссылке https://servernews.ru/995720

3 Об инструменте Intel Management Engin можно прочитать в Википедии https://ru.wikipedia.org/wiki/Intel_Management_Engine

4 О технологии Active Management можно прочитать в Википедии https://ru.wikipedia.org/wiki/Active_Management_Technology

5 Подробнее этот вопрос разобран здесь https://www.techrepublic.com/article/is-the-intel-management-engine-a-backdoor/. Об этом же говорится здесь https://www.fsf.org/blogs/sysadmin/the-management-engine-an-attack-on-computer-users-freedom

6 О них сказано здесь https://www.securitylab.ru/blog/company/pt/345157.php. А также здесь https://xakep.ru/2017/11/21/intel-me-flaws/. О более свежей и фундаментальной уязвимости сказано здесь https://www.ixbt.com/news/2020/03/06/ahillesova-pjata-processorov-intel-najdena-samaja-opasnaja-i-neustranimaja-ujazvimost.html

7 Об этом можно прочитать здесь https://xakep.ru/2017/06/10/intel-amt-sol/

8 Об этом сказано здесь https://www.heise.de/newsticker/meldung/AMD-Secure-Processor-PSP-wohl-bei-einigen-Ryzen-Mainboards-abschaltbar-3913635.html

1 bezopasnye-proczessory/. А также здесь https://aspektcenter.ru/tablitsa-sootvetstviya-protsessorov-intel-amd/. Более свежие сведения приводятся в этой статье https://www.cnews.ru/news/top/2022-02-04_intel_v_nebezopasnosti_nashih. Еще об одной свежей уязвимости в Intel, отсутствующей в AMD, сказано здесь https://www.cnews.ru/news/top/2022-03-09_protsessorykotoryh_intel_lishila. О процессорных уязвимостях можно почитать эту работу https://safe-surf.ru/specialists/article/5265/648025/?sphrase_id=45542, а также ее продолжение https://safe-surf.ru/specialists/article/5265/650521/

2 Единственное найденное свидетельство, подкрепляющее данное утверждение касается одной уязвимости, о которой сказано здесь https://overclockers.ru/blog/TEXHAPb/show/70654/v-processorah-intel-i-amd-obnaruzhena-kriticheskaya-uyazvimost-retbleed-patch-zamedlyaet-pk-do-28

3 О производительности процессоров можно прочитать здесь http://www.thg.ru/cpu/amd_vs_intel/index.html. А также здесь https://www.moyo.ua/news/kakoy-protsessor-luchshe-dlya-igr-amd-ili-intel-vybiraem-iz-2-proizvoditeley.html

4 Одним из них является этот сайт https://h-node.org

5 Например о видеокартах можно почитать здесь https://www.dz-techs.com/ru/use-amd-nvidia-gpus-linux. Также подборку информации о наилучшем взаимодействии тех или иных видеокарт с системами GNU/Linux можно посмотреть здесь https://myroad.club/luchshaya-videokarta-dlya-linux-v-2021-godu-obzory/

6 Компании продающие чистые устройства с предустановленным свободным ПО https://ryf.fsf.org/

7 Подробнее о BIOS https://ru.wikipedia.org/wiki/BIOS

8 Подробнее о UEFI https://ru.wikipedia.org/wiki/Extensible_Firmware_Interface

9 Об одной из таких можно прочитать здесь https://www.kaspersky.ru/blog/mosaicregressor-uefi-malware/29215/. Технические подробности этой атаки даны в этой статье https://securelist.com/mosaicregressor/98849/. Еще об одной атаке рассказано здесь https://www.kaspersky.ru/blog/cosmicstrand-uefi-rootkit/33702/. Более подробно она описана в данной статье https://arstechnica.com/information-technology/2022/07/researchers-unpack-unkillable-uefi-rootkit-that-survives-os-reinstalls/3/. Технические подробности

1 данной атаки описаны в этой статье https://securelist.com/cosmicstrand-uefi-firmware-rootkit/106973/

2 Сайт Libreboot https://libreboot.org/, также о нем можно прочитать в Википедии https://ru.wikipedia.org/wiki/Libreboot

3 Сайт Coreboot https://www.coreboot.org/, также о нем можно прочитать в Википедии https://ru.wikipedia.org/wiki/Coreboot

4 О системе GNU/Linux можно почитать по этой ссылке https://www.gnu.org/gnu/about-gnu.ru.html

5 О ядре Linux https://ru.wikipedia.org/wiki/%D0%AF%D0%B4%D1%80%D0%BE_Linux

6 Данный вопрос о правильности названия разобран в этой статье https://www.gnu.org/gnu/gnu-users-never-heard-of-gnu.ru.html. Также на вопросы по данный теме можно найти ответы по данной ссылке https://www.gnu.org/gnu/gnu-linux-faq.ru.html

7 Подробнее об Ubuntu https://ru.wikipedia.org/wiki/Ubuntu. О ее проблемах можно почитать на этой странице https://www.gnu.org/distros/common-distros.ru.html. Также существует отдельная статья о слежке в Ubuntu. Функция, о которой в ней говорится, в последующих выпусках была отключена, но проблема во многом осталась, о чем также сказано в статье https://www.gnu.org/philosophy/ubuntu-spyware.ru.html

8 Подробнее о Mint https://ru.wikipedia.org/wiki/Linux_Mint. О его проблемах также можно прочесть в этой статье https://www.gnu.org/distros/common-distros.ru.html

9 Подробнее о семействе операционных систем BSD https://ru.wikipedia.org/wiki/BSD

10 Об одном из дистрибутивов BSD, рассчитанном на домашнее использование https://ru.wikipedia.org/wiki/TrueOS

11 Об этих проблемах также можно прочесть на этой странице https://www.gnu.org/distros/common-distros.ru.html

12 Полностью свободные дистрибутивы GNU/Linux https://www.gnu.org/distros/free-distros.ru.html

13 О полностью свободном ядре Linux-libre https://ru.wikipedia.org/wiki/Linux-libre

14 Сайт проекта Dragora https://dragora.org/en/index.html

15 Сайт проекта Giks https://guix.gnu.org/. Также о нем можно прочитать в

1 Википедии https://ru.wikipedia.org/wiki/Guix_System_Distribution

2 Сайт операционной системы Dyne:bolic https://algosov.org/. Также о нем можно прочитать в Википедии https://ru.wikipedia.org/wiki/Dyne:bolic

3 Об операционной системе Arch можно прочесть в Википедии https://ru.wikipedia.org/wiki/Arch_Linux

4 Сайт операционной системы Hiperbola https://www.hyperbola.info/

5 Сайт операционной системы Parabola https://www.parabola.nu/. Также о ней можно прочитать в Википедии https://ru.wikipedia.org/wiki/Parabola_GNU/Linux-libre

6 Сайт проекта PureOS https://pureos.net/. Также о нем можно прочитать в Википедии https://ru.wikipedia.org/wiki/PureOS

7 Сайт операционной системы Trisquel https://trisquel.info/. Также о нем написано в Википедии https://ru.wikipedia.org/wiki/Trisquel

8 Сайт Utito http://www.ututo.org/. О ней также есть статья в Википедии https://ru.wikipedia.org/wiki/Ututo

9 Сайт Debian https://www.debian.org/index.ru.html. Также о нем можно прочесть в Википедии https://ru.wikipedia.org/wiki/Debian

10 Об этой проблеме также говориться на этой странице https://www.gnu.org/distros/common-distros.ru.html

11 Статья с историей спора о systemd https://habr.com/ru/post/431202/. Статья о проблемах systemd https://sohabr.net/habr/post/242495/. Обсуждение проблем systemd https://www.linux.org.ru/forum/general/13519919. Комментарий с констатацией проблем systemd https://www.linux.org.ru/news/opensource/11344526/page4#comment-11352917. Статья с разоблачением мифов о systemd https://www.opennet.ru/base/sys/systemd_myth.txt.html

12 Статья с указанием на наличие DNS от Google в конфигурации systemd https://isc.sans.edu/forums/diary/Systemd+Could+Fallback+to+Google+DNS/22516/

13 Обсуждение проблем наличия DNS от Google в конфигурации systemd https://github.com/systemd/systemd/issues/8782. Еще одно обсуждение https://github.com/systemd/systemd/issues/12499

14 Со статьей, отстаивающей преимущества systemd, можно ознакомиться здесь https://habr.com/ru/post/325792/

15 Сайт Devuan https://www.devuan.org/. Также о Devuan можно прочитать эту статью http://helpexe.ru/linux/linux-bez-systemd-pochemu-vy-dolzhny-

1 ispolzovat

2 Ссылка на страницу, где можно скачать iso-образа Trisquel https://trisquel.info/en/download

3 Подробнее о Rufus https://ru.wikipedia.org/wiki/Rufus_(%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)

4 Скачать программу для записи образов ОС Rosa можно на этой странице https://www.rosalinux.ru/rosa-linux-download-links/. Если ссылка не работает, можете попробовать эту http://wiki.rosalab.ru/ru/index.php/ROSA_ImageWriter

5 Сайт LibreOffice https://ru.libreoffice.org/. Также о нем можно прочитать в Википедии https://ru.wikipedia.org/wiki/LibreOffice

6 Сайт GIMP https://www.gimp.org/. Также о нем можно прочитать в Википедии https://ru.wikipedia.org/wiki/GIMP

7 Отличия в функционале между GIMP и Photoshop описаны на этой странице https://askentire.net/q/kakie-klyuchevye-funkcii-photoshop-svyazannye-s-fotografiei-otsutstvuyut-v-24271418321

8 Сайт VLC https://www.videolan.org/vlc/. Также о нем можно прочитать в Википедии https://ru.wikipedia.org/wiki/VLC_(%D0%BC%D0%B5%D0%B4%D0%B8%D0%B0%D0%BF%D0%BB%D0%B5%D0%B5%D1%80)

9 Репозитории с драйверами для графического оборудования указаны здесь http://linuxoidblog.blogspot.com/2015/12/linux_4.html

10 Сайт GParted https://gparted.org/. Также о нем можно прочитать в Википедии https://ru.wikipedia.org/wiki/GParted

11 Подробнее про отрицаемое шифрование https://ru.wikipedia.org/wiki/%D0%9E%D1%82%D1%80%D0%B8%D1%86%D0%B0%D0%B5%D0%BC%D0%BE%D0%B5_%D1%88%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5

12 Подробнее о Virtual Mashine Manager https://ru.wikipedia.org/wiki/Virtual_Machine_Manager

13 Сайт Flowblade https://jliljebl.github.io/flowblade/. Также о нем можно прочитать в Википедии https://ru.wikipedia.org/wiki/Flowblade

14 Сайт Audacity https://www.audacityteam.org/. Также о нем можно прочитать

1 в Википедии https://ru.wikipedia.org/wiki/Audacity

2 Сайт MuseScore https://musescore.org/. Также о нем можно прочитать в Википедии https://ru.wikipedia.org/wiki/MuseScore

3 Видео о кодеках и контейнерах можно посмотреть по этой ссылке https://www.youtube.com/watch?v=hQcHq0XJfQA

4 О свободном кодеке видео Theora написано в Википедии https://ru.wikipedia.org/wiki/Theora

5 О кодеке Dirac есть статья в Википедии https://ru.wikipedia.org/wiki/Dirac

6 О кодеке VP9 https://ru.wikipedia.org/wiki/VP9

7 Об аудиокодеке Vorbis https://ru.wikipedia.org/wiki/Vorbis

8 О кодеке Opus https://ru.wikipedia.org/wiki/Opus_(%D0%BA%D0%BE%D0%B4%D0%B5%D0%BA)

9 О кодеке FLAC https://ru.wikipedia.org/wiki/FLAC

10 О контейнере Ogg https://ru.wikipedia.org/wiki/Ogg. Также есть видео о нем https://www.youtube.com/watch?v=lfeyPy14NrM

11 О контейнере Matroska https://ru.wikipedia.org/wiki/Matroska. Также видео https://www.youtube.com/watch?v=eJ85bLfrr9Y

12 О контейнере WebM https://ru.wikipedia.org/wiki/WebM. Также видео https://www.youtube.com/watch?v=oRT-jHgnH-8

13 Сайт LibreCAD https://librecad.org/. Также о нем можно прочитать в Википедии https://ru.wikipedia.org/wiki/LibreCAD

14 О программе для 3D-моделирования Blender https://ru.wikipedia.org/wiki/Blender

15 Сайт CalculiX http://calculix.de/. Также о нем можно прочитать в Википедии https://ru.wikipedia.org/wiki/CalculiX

16 Сайт OpenFOAM https://openfoam.org/. Также о нем можно прочитать в Википедии https://ru.wikipedia.org/wiki/OpenFOAM

17 Страница программы TimeShift https://github.com/teejee2008/timeshift. Также о ней можно прочитать здесь https://info-comp.ru/drugieopersistemi/709-create-system-snapshot-in-linux-mint.html

18 Об Интернет-браузере Firefox https://ru.wikipedia.org/wiki/Mozilla_Firefox

19 Статья о методе Гутмана в Википедии https://ru.wikipedia.org/wiki/%D0%9C%D0%B5%D1%82%D0%BE%D0%B4_%D0%93%D1%83%D1%82%D0%BC%D0%B0%D0%BD%D0%B0

20 Подробнее про OpenBSD https://ru.wikipedia.org/wiki/OpenBSD

1 Devuan https://www.devuan.org/get-devuan. Лучше использовать полный образ последней стабильной версии, помеченный как desktop, например по этой ссылке https://ftp.nluug.nl/pub/os/Linux/distr/devuan/devuan_chimaera/installer-iso/devuan_chimaera_4.0.0_amd64_desktop.iso

2 Проприетарная лицензия плагина VirtualBox https://www.virtualbox.org/wiki/VirtualBox_PUEL

3 Подробнее о KVM https://ru.wikipedia.org/wiki/KVM

4 Подробнее о Xen https://ru.wikipedia.org/wiki/Xen

5 Подробнее о Qemu https://ru.wikipedia.org/wiki/QEMU. А также об инструменте Libvirt https://ru.wikipedia.org/wiki/Libvirt

6 Методика настройки конфигурации браузера исходит из информации, представленной в этой статье https://gist.github.com/Guest007/e3a09aa97a827916b0b91b726a8c2c66. А также в этой https://cryptopunks.org/article/firefox-secure-tweak/. И в этой https://habr.com/ru/post/435876/. Еще в этой https://www.pf.team/articles/tor-browser---nastroika-na-anonimnost%2527__bhq21i3w

7 О проблеме java-скриптов можно почитать в этой статье https://www.gnu.org/philosophy/javascript-trap.ru.html

8 О XSS-атаках можно прочитать в Википедии https://ru.wikipedia.org/wiki/%D0%9C%D0%B5%D0%B6%D1%81%D0%B0%D0%B9%D1%82%D0%BE%D0%B2%D1%8B%D0%B9_%D1%81%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%B8%D0%BD%D0%B3

9 Об этом сказано в этой статье http://en.hackdig.com/?442.htm. Еще об одной функции, позволяющей эксплуатировать уязвимость сказано здесь https://www.opennet.ru/opennews/art.shtml?num=54727

10 Страница со списком шифрующих DNS-серверов https://dnscrypt.info/public-servers/

11 О поисковике DuckDuckGo можно почитать в Википедии https://ru.wikipedia.org/wiki/DuckDuckGo

12 О технологии «Пузырь фильтров», используемой неэтичными поисковиками https://ru.wikipedia.org/wiki/%D0%9F%D1%83%D0%B7%D1%8B%D1%80%D1%8C_%D1%84%D0%B8%D0%BB%D1%8C%D1%82%D1%80%D0%BE%D0%B2

13 Об Ixquick и StartPage можно прочитать в Википедии https://ru.wikipedia.org/wiki/Ixquick

1 https://ru.wikipedia.org/wiki/Chromium

2 Подробнее об Интернет-браузере SRWare Iron можно прочитать в Википедии https://ru.wikipedia.org/wiki/SRWare_Iron

3 Увидеть это можно по следующей ссылке https://www.srware.net/forum/viewtopic.php?f=27&t=44996. А также по этой https://www.srware.net/forum/viewtopic.php?f=27&t=19809

4 Страница Ungoogled Chromium https://ungoogled-software.github.io/

5 Сайт Vivaldi https://vivaldi.com/ru/

6 Статья с объяснением отличий Vivaldi от Chromium https://vivaldi.com/blog/vivaldi-browser-vs-google-chrome/

7 Статья о поддержке Vivaldi блокировщиков рекламы https://habr.com/en/company/vivaldi/blog/456048/. Статья о новом способе отслеживания пользователей, внедряемом Google и отказе его использования Vivaldi https://habr.com/en/company/vivaldi/blog/552408/

8 Статья о том, как Google препятствует распространению Vivaldi https://habr.com/en/post/406461/

9 Статья с разъяснением политики публикации исходного кода и лицензирования Vivaldi https://habr.com/en/company/vivaldi/blog/526300/. Страница с разъяснениями открытости Vivaldi https://jon.vivaldi.net/a-few-words-about-open-source-vivaldi/

10 Политика конфиденциальности Vivaldi https://vivaldi.com/ru/privacy/browser/

11 Подробнее об Интернет-браузере Falkon https://ru.wikipedia.org/wiki/Falkon

12 О веб-маяках можно почитать в Википедии https://en.wikipedia.org/wiki/Web_beacon

13 Сайт Sylpheed https://sylpheed.sraoss.jp/en/, также о нем можно прочитать в Википедии https://ru.wikipedia.org/wiki/Sylpheed

14 Об этом сказано здесь https://directory.fsf.org/wiki/Icedove

15 Об этом рассказано в статье в Википедии https://ru.wikipedia.org/wiki/Iceweasel

16 Сайт Thunderbird https://www.thunderbird.net/, также о нем можно почитать в Википедии https://ru.wikipedia.org/wiki/Mozilla_Thunderbird

17 Страница об Evolution https://wiki.gnome.org/Apps/Evolution, также о нем можно почитать в Википедии https://ru.wikipedia.org/wiki/Evolution

18 Сайт Claws Mail https://www.claws-mail.org/, также о нем можно прочитать

1 в Википедии https://ru.wikipedia.org/wiki/Claws_Mail

2 Сайт Mailpile https://www.mailpile.is/, также о нем можно прочитать в Википедии https://ru.wikipedia.org/wiki/Mailpile

3 О VoIP можно почитать в Википедии https://ru.wikipedia.org/wiki/VoIP

4 О SIP можно почитать в Википедии https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%83%D1%81%D1%82%D0%B0%D0%BD%D0%BE%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D1%81%D0%B5%D0%B0%D0%BD%D1%81%D0%B0

5 Сайт Linphone https://www.linphone.org/, также о нем можно почитать в Википедии https://ru.wikipedia.org/wiki/Linphone

6 Сайт Twinkle http://twinkle.dolezel.info/

7 Сайт MEGA https://mega.nz. О MEGA можно почитать в Википедии

8 Страница со ссылками на исходные коды инструментов MEGA https://mega.io/sourcecode

9 С расценками и сравнением с другими сервисами можно ознакомится на этой странице https://mega.io/pro

10 О таких уязвимостях говорится здесь https://unixforum.org/viewtopic.php?t=122400. А также здесь https://xakep.ru/2011/07/19/56270/

11 О таких вирусах можно прочитать эту статью https://losst.ru/opasnye-virusy-dlya-linux. Также о более свежем вирусе говорится здесь https://www.intezer.com/blog/linux/evilgnome-rare-malware-spying-on-linux-desktop-users/

12 О них говорится здесь https://www.technodor.info/2019/02/4-linux.html. Из всех приведенных неприемлем для использования только Comodo, поскольку он несвободный. Остальные вполне годятся.

13 Об этих инструментах есть эта статья https://losst.ru/pesochnitsa-programm-linux

14 О видах и функциях прокси можно узнать на этой странице https://techlist.top/proksi-vidy-proksi/. Также о прокси можно прочитать в Википедии https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%BA%D1%81%D0%B8-%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80

15 О VPN можно прочитать в Википедии https://ru.wikipedia.org/wiki/VPN

16 Такое заявление звучит, например, в этом видео https://www.youtube.com/

1 watch?v=2QNKtyVwUDo, которое вообще апофеоз некомпетентности. В нем также говориться, что прозрачные прокси не скрывают ip, что неверно. При этом заявляется, что они подменяют тип браузера и операционки, что также не соответствует действительности.

2 О слежке со стороны VPN-провайдеров можно почитать это исследование https://research.csiro.au/ng/wp-content/uploads/sites/106/2016/08/paper-1.pdf

3 О SSH можно почитать в Википедии https://ru.wikipedia.org/wiki/SSH

4 Это описано в данной статье https://thesafety.us/ru/what-is-double-triple-quad-vpn

5 Принципы такой схемы описаны здесь https://thesafety.us/ru/parallel-vpn

6 Официальный сайт проекта Tor https://www.torproject.org/ru/. О принципах использования Tor можно узнать из этого видео https://www.youtube.com/watch?v=3Qa0-OcBF0w. Также о нем можно почитать в Википедии https://ru.wikipedia.org/wiki/Tor

7 История проекта Tor изложена на официальном сайте https://www.torproject.org/ru/about/history/

8 Эти структуры указаны на официальном сайте в разделе «Спонсоры» https://www.torproject.org/ru/about/sponsors/. На это также указано в статье https://www.washingtonpost.com/news/the-switch/wp/2013/09/06/the-feds-pays-for-60-percent-of-tors-development-can-users-trust-it/?arc404=true. А также https://www.vedomosti.ru/technology/articles/2019/04/03/798234-tor-ne-dolzhen-zaviset-ot-pravitelstva

9 Лицензия Tor опубликована по ссылке https://gitweb.torproject.org/tor.git/tree/LICENSE

10 Это можно увидеть в уже не раз упомянутом видео Ивана Глазкова https://www.youtube.com/watch?v=rsO_ofHTfEA

11 Об этом можно узнать в Википедии https://ru.wikipedia.org/wiki/Tor#.D0.A1.D1.82.D0.BE.D1.80.D0.BE.D0.B6.D0.B5.D0.B2.D1.8B.D0.B5_.D1.83.D0.B7.D0.BB.D1.8B_.28guard_node.29

12 Методы деанона эксплуатирующие подобные инструменты описаны в этой статье https://xakep.ru/2015/06/25/tor-197/

13 Одно из наиболее крупных исследований этого метода можно найти по ссылке http://www.cs.columbia.edu/~sc2516/papers/pam2014-tor-nfattack.pdf

14 О разработке такого инструмента рассказано в этой статье https://xakep.ru/2016/02/29/sybilhunter/

1 %D0%90%D1%82%D0%B0%D0%BA%D0%B0_%D0%BF%D0%BE_%D0%B2%D1%80%D0%B5%D0%BC%D0%B5%D0%BD%D0%B8

2 Аргументы в пользу безопасности Tor, в том числе критику эффективности тайминг-атак можно найти в этой статье https://intsystem.org/security/pochemu-tor-bezopasen/

3 Такие случаи описаны в этой статье http://odminblog.ru/tor-operators-cases/

4 О мостах Tor можно узнать в Википедии https://ru.wikipedia.org/wiki/Tor#.D0.9C.D0.BE.D1.81.D1.82.D0.BE.D0.B2.D1.8B.D0.B5_.D1.83.D0.B7.D0.BB.D1.8B_.28bridge_relay.29

5 О различных технологиях противодействия глубокой инспекции пакетов, используемых Tor, можно почитать в Википедии https://ru.wikipedia.org/wiki/Tor#.D0.9F.D1.80.D0.BE.D1.82.D0.B8.D0.B2.D0.BE.D0.B4.D0.B5.D0.B9.D1.81.D1.82.D0.B2.D0.B8.D0.B5_.D0.B1.D0.BB.D0.BE.D0.BA.D0.B8.D1.80.D0.BE.D0.B2.D0.BA.D0.B5_.D0.B8_.D0.B3.D0.BB.D1.83.D0.B1.D0.BE.D0.BA.D0.BE.D0.B9_.D0.B8.D0.BD.D1.81.D0.BF.D0.B5.D0.BA.D1.86.D0.B8.D0.B8_.D0.BF.D0.B0.D0.BA.D0.B5.D1.82.D0.BE.D0.B2

6 Об этой технологии можно узнать по ссылке https://2019.www.torproject.org/docs/pluggable-transports

7 Об этой технологии можно узнать по ссылке https://trac.torproject.org/projects/tor/wiki/doc/meek

8 О технологиях обфускации можно также почитать на этой странице https://tb-manual.torproject.org/ru/circumvention/. Также о них рассказывается в этой статье https://spy-soft.net/unblock-tor/

9 По этой теме может оказаться полезным почитать рекомендации на сайте прокта Tor https://support.torproject.org/ru/faq/staying-anonymous/. А также на сайте проекта Whonix https://www.whonix.org/wiki/DoNot. Также сборник рекомендаций можно почитать здесь https://www.pf.team/articles/rekomendatsii-pol%2527zovateliu-tor__bKgrzPAq. Хотя некоторые предостережения можно считать чрезмерными, а от некоторых опасностей нас защищает организация соединения, все же эти рекомендации стоит учитывать. Кроме этого может оказаться полезным ознакомиться с этой статьей https://www.pf.team/articles/anonimnost%2527-v-seti__bsGNzXmS. А также с этой https://www.pf.team/articles/protivniki-anonimnosti-i-ikh-metody__bwgaomcc

1 можно почитать в Википедии https://ru.wikipedia.org/wiki/TAILS

2 Об этом говорится в этой статье https://www.gnu.org/distros/common-distros.ru.html#Tails

3 Официальный сайт Whonix https://www.whonix.org/. Также об этой системе можно почитать в Википедии https://ru.wikipedia.org/wiki/Whonix

4 Официальный сайт Qubes https://www.qubes-os.org/. Также об этой системе можно почитать в Википедии https://ru.wikipedia.org/wiki/Qubes_OS

5 Официальный сайт Subgraph https://subgraph.com/. Также о нем можно почитать в Википедии https://ru.wikipedia.org/wiki/Subgraph_OS

6 Страница данного пакета https://gitlab.com/whonix/anon-apps-config. Здесь же дана методика подключения репозиториев Whonix.

7 Страница данного пакета https://gitlab.com/whonix/sdwdate

8 Обо всем этом сказано на сайте проекта Whonix https://www.whonix.org/wiki/Alternative_DNS_Resolver

9 Сайт с конфигурационными файлами VPN https://www.vpngate.net/en/

10 О протоколе IPv4 можно почитать в Википедии https://ru.wikipedia.org/wiki/IPv4

11 Об исчерпании адресов IPv4 и способах его замедления есть статья в Википедии https://ru.wikipedia.org/wiki/%D0%98%D1%81%D1%87%D0%B5%D1%80%D0%BF%D0%B0%D0%BD%D0%B8%D0%B5_IPv4-%D0%B0%D0%B4%D1%80%D0%B5%D1%81%D0%BE%D0%B2

12 О протоколе IPv6 можно прочитать в Википедии https://ru.wikipedia.org/wiki/IPv6

13 Мосты Tor https://bridges.torproject.org/options

14 Сайт одного из таких Web-прокси https://www.sudoproxy.net/. Еще один сайт https://proxybrowser.xyz/. И еще один https://proxy-123.com/

15 Конфигурация взята с https://trac.torproject.org/projects/tor/wiki/doc/TransparentProxy

16 Список кодов стран можно посмотреть здесь https://countrycode.org

17 Методика настройки взята с https://cryptopunks.org/article/forward+all+the+traffic+to+tor/

18 Они также находятся на этой странице https://trac.torproject.org/projects/tor/wiki/doc/TransparentProxy

19 Его можно посмотреть по этой ссылке https://lists.torproject.org/pipermail/

1 tor-talk/2014-March/032507.html

2 Например этот сервис https://www.speedtest.net/

3 Сайт LibreWolf https://librewolf.net/

4 Официальный сайт Waterfox https://www.waterfox.net/. Также о нем можно почитать в Википедии https://ru.wikipedia.org/wiki/Waterfox

5 Официальный сайт Searx https://searx.me/

6 Страница с ссылками на сервера Searx, осуществляющие Интернет-поиск https://searx.space/.

7 Официальный сайт YaCy https://yacy.net/. Также об этом поисковике можно почитать в Википедии https://ru.wikipedia.org/wiki/YaCy

8 Страница с образами для скачивания https://yacy.net/download_installation/. Необходима ссылка под надписью «Linux».

9 Об OpenStreetMap можно почитать в Википедии https://ru.wikipedia.org/wiki/OpenStreetMap

10 Карты OpenStreetMap https://www.openstreetmap.org

11 Сайт LibreTranslate https://libretranslate.com/

12 Еще один сайт LibreTranslate https://libretranslate.de/

13 Политика конфиденциальности Systran https://www.systransoft.com/systran/policies/privacy-policy/. О том, что ip и другие идентификаторы не привязываются к вводимым для перевода текстам, сказано в 10 пункте.

14 Переводчик Systran https://www.systran.net/en/translate/

15 Сайт CryptPad https://cryptpad.fr/

16 Официальный сайт ProtonMail https://protonmail.com/ru/. Также о нем можно прочитать в Википедии https://ru.wikipedia.org/wiki/ProtonMail

17 Комментарий можно посмотреть по ссылке https://spy-soft.net/zashhishhennaya-pochta-protonmail/#comment-9244

18 Страница сервиса почты Riseup https://riseup.net/ru/email. Также о нем можно посмотреть вот это видео https://www.youtube.com/watch?v=AJYuvP1fM_Y&disable_polymer=true

19 Об этом можно узнать здесь https://web.archive.org/web/20170304164306/http://horizontalhostility.net/post/001/

20 Сайт Mailbox https://mailbox.org/en/

21 Официальный сайт Tutanota https://www.tutanota.com/ru/. Также об этом сервисе можно почитать в Википедии https://ru.wikipedia.org/wiki/Tutanota

22 Об этом говорится в этой статье https://habr.com/ru/company/globalsign/blog/

1 532238/

2 Официальный сайт Mumble https://www.mumble.info/. Также о нем можно прочитать в Википедии https://ru.wikipedia.org/wiki/Mumble

3 Страница Jitsi Meet https://jitsi.org/jitsi-meet/

4 О WebRTC можно прочитать здесь https://ru.wikipedia.org/wiki/webrtc

5 Об акустической обратной связи можно прочитать в Википедии https://ru.wikipedia.org/wiki/%D0%90%D0%BA%D1%83%D1%81%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F_%D0%BE%D0%B1%D1%80%D0%B0%D1%82%D0%BD%D0%B0%D1%8F_%D1%81%D0%B2%D1%8F%D0%B7%D1%8C

6 Сайт сервиса Jitsi Meet https://meet.jit.si/

7 Об XMPP можно почитать в Википедии https://ru.wikipedia.org/wiki/XMPP

8 Посмотреть их список можно по этой ссылке https://xmpp-servers.404.city/

9 Официальный сайт OpenPGP https://www.openpgp.org/. Об этой технологии также можно прочитать в Википедии https://ru.wikipedia.org/wiki/OpenPGP

10 Страница OTR https://otr.cypherpunks.ca/. Об этой технологии также можно прочитать в Википедии https://ru.wikipedia.org/wiki/Off-the-Record_Messaging

11 О шифровании OMEMO можно почитать в Википедии https://ru.wikipedia.org/wiki/OMEMO

12 Сравнение функций этих технологий шифрования можно посмотреть здесь https://ru.bmstu.wiki/OMEMO#C.D1.80.D0.B0.D0.B2.D0.BD.D0.B5.D0.BD.D0.B8.D0.B5_.D1.84.D1.83.D0.BD.D0.BA.D1.86.D0.B8.D0.B9_OMEMO

13 Официальный сайт Gajim https://gajim.org/. Также о нем можно почитать в Википедии https://ru.wikipedia.org/wiki/Gajim

14 Официальный сайт Dino https://dino.im/

15 Об этом сказано в этой статье https://www2.bdf-club.hk/threads/ostorozhno-jabber-servera-wwh-vedut-polnoe-logirovanie.23794/. В ней же указывается, какие серверы хранят логи, а какие нет.

16 Сайт Matrix https://matrix.org/. О Matrix можно прочитать в Википедии https://ru.wikipedia.org/wiki/Matrix

17 Страница Quaternion https://github.com/quotient-im/Quaternion

18 Страница Nheko Reborn https://github.com/Nheko-Reborn/nheko

1 использовании серверов Amazon сказано в пункте 2.10.

2 Подборку фактов по данному вопросу можно посмотреть здесь https://www.gnu.org/proprietary/malware-amazon.html

3 Сайт Status https://status.im/ru

4 Страница мессенджера Status https://status.im/ru/private-messenger/

5 Страница с образами скачивания клиента Status https://status.im/ru/get/

6 Официальный сайт Tox https://tox.chat/. Также о нем можно почитать в Википедии https://ru.wikipedia.org/wiki/Tox

7 Страница qTox https://wiki.tox.chat/clients/qtox

8 Страница uTox https://wiki.tox.chat/clients/utox

9 Официальный сайт Jami https://jami.net/. Также об этой программе можно почитать в Википедии https://ru.wikipedia.org/wiki/Jami_(%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0)

10 Страница с версиями для скачивания и репозиториями https://jami.net/download-jami-linux/

11 Официальный сайт Briar https://briarproject.org/

12 Страница с образом Briar для компьютера https://briarproject.org/download-briar-desktop/

13 Официальный сайт RetroShare https://retroshare.cc/. Также об этой программе можно почитать в Википедии https://ru.wikipedia.org/wiki/RetroShare

14 Об этом сказано на странице проекта Whonix https://www.whonix.org/wiki/Chat, со ссылкой на эту страницу https://www.elttam.com.au/blog/a-review-of-the-eff-secure-messaging-scorecard-pt1/, а также на эту https://scan.coverity.com/projects/retroshare-retroshare

15 Методика подключения этих репозиториев указана здесь https://retroshare.cc/downloads.html#debian

16 Ссылка на скачивание находится здесь https://retroshare.cc/downloads.html#appimage. Нажимать необходимо на ссылку AppImage.

17 Сайт Session https://getsession.org/

18 Статья о маршрутизации Session https://getsession.org/whitepaper

19 Страница с образами для скачивания Session https://getsession.org/download

20 О fediverse можно прочитать в Википедии https://ru.wikipedia.org/wiki/Fediverse

1 в Википедии https://ru.wikipedia.org/wiki/Friendica

2 Официальная страница GNU social https://gnu.io/social

3 Сайт Funkwhale https://funkwhale.audio/

4 Сайт Hubzilla https://hubzilla.org

5 Сайт Pixelfed https://pixelfed.org/

6 Официальный сайт Mastadon https://joinmastodon.org/. Также о нем можно прочитать в Википедии https://ru.wikipedia.org/wiki/Mastodon_(%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)

7 Официальный сайт Diaspora https://diasporafoundation.org/. Также о ней можно прочитать в Википедии https://ru.wikipedia.org/wiki/Diaspora_(%D1%81%D0%BE%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C)

8 Официальный сайт Movim https://movim.eu

9 Страница Pandora https://github.com/Novator/Pandora. То, как работает данная социальная сеть, описано в этой статье https://github.com/Novator/Pandora/wiki/P2P-social-network-Pandora

10 Инструкцию, как подключить репозитории из которых устанавливается нужное ПО, а также, как производить его настройку, можно посмотреть здесь https://github.com/Novator/Pandora/wiki/Install-and-first-run

11 Официальный сайт Twister http://twister.net.co/. Также о нем можно почитать здесь https://habr.com/ru/post/208472/

12 Сайт TMWSD https://xn--uih.ws

13 Сайт OneTimeSecret https://onetimesecret.com/