# ЛАБОРАТОРНАЯ РАБОТА № 1 (2 часа)

# Установка и настройка операционной системы AstraLinuxSE

# Цель работы – изучение требований к целевому компьютеру и подготовка к установке, установка ОС, настройка дополнительных параметров в Astra Linux SE.

**ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ**

В настоящее время в ходе масштабного перехода госорганов на отечественный софт Департамент развития информационного общества определил 26 исполнительных органов государственной власти (ИОГВ), которые перейдут на операционные системы семейства Astra Linux и другие отечественные программные продукты.

Флагманами перевода своих информационных систем на отечественные IT-решения остаются силовые структуры, более всего подверженные санкционным рискам и предъявляющие повышенные требования к безопасности и защищенности используемых программно-аппаратных платформ, это МВД, МЧС, ФСО, Минобороны, Минюста России и другие организации силового сектора. А также активное включение в процесс импортозамещения госкорпораций входят Росатом, РЖД, РусГидро, Газпром, Роскосмос, РосТех, РосНефть и др.

**1 Введение в ОС AstraLinux**

Операционные системы Astra Linux предназначены для применения в составе информационных (автоматизированных) систем в целях обработки и защиты от несанкционированного доступа информации любой категории доступа (в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», статья 5, пункт 2), общедоступной информации, а также информации, доступ к которой̆ ограничен федеральными законами (информации ограниченного доступа).

Под дистрибутивом понимается набор программного обеспечения на базе ядра Linux, поставляемый как единое целое.

Дистрибутивы Linux различаются как между собой,   
так и версиями дистрибутивов, хотя обладают многими схожими чертами.

Существует огромное количество дистрибутивов, большинство из них относится к одному из пяти семейств:

* Debian (представители: Debian, Ubuntu, Astra Linux);
* Red Hat (представители: Red Hat, Fedora, Centos);
* Slackware (представители: Slackware, Suse);
* Arch Linux (представители Arch Linux, Manjaro);
* Gentoo (представители Gentoo, Chromium).

Astra Linux относится к семейству UNIX-подобных ОС  
GNU/LINUX. Astra Linux базируется на Debian и является официально признанной веткой дистрибутива Debian. В строенные средства защиты ОС разработаны совместно с Академией ФСБ России и Институтом системного программирования РАН.

Операционные системы Astra Linux Common Edition и Astra Linux Special Edition разработаны коллективом открытого акционерного общества «Научно-производственное объединение Русские базовые информационные технологии» и основаны на свободном программном обеспечении. С 17 декабря 2019 года правообладателем, разработчиком и производителем операционной системы специального назначения «Astra Linux Special Edition» является ООО «РусБИТех-Астра».

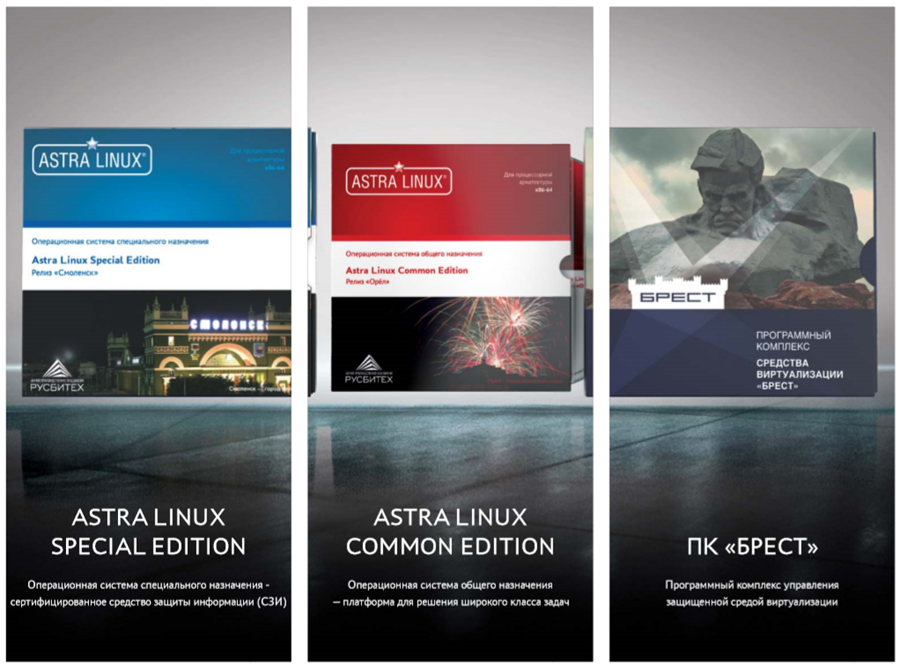
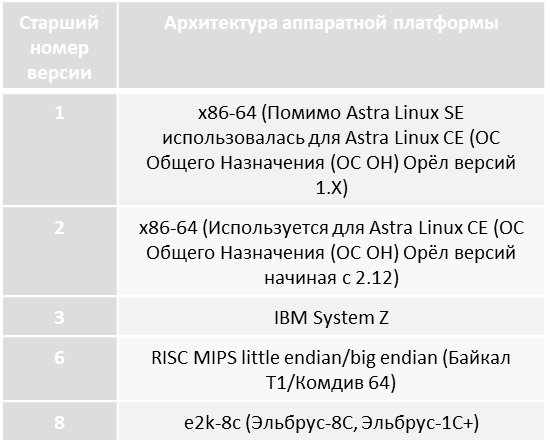


Рисунок 1 – Существующие варианты архитектуры Astra Linux

ОС Astra Linux Common Edition (релиз «Орёл») –версия ОС общего назначения без усиленных средств защиты данных. ОС в полной мере поддерживает стандарт аутентификации Kerberos. Предусмотрены три варианта централизованных систем управления аутентификацией и безопасностью:

* собственный домен Astra Linux Directory;
* Samba DC;
* универсальный open-source домен FreeIPA.

ОС специального назначения Astra Linux Special Edition предназначена для создания на ее основе автоматизированных систем в защищенном исполнении, обрабатывающих информацию со степенью секретности «совершенно секретно» включительно. ОС Astra Linux Special Edition создана и развивается на основе распространенных дистрибутивов Debian и Ubuntu. Виды защищаемой информации:

* коммерческая тайна;
* конфиденциальная информация;
* персональные данные;
* государственная тайна, в том числе с грифом «особой важности» (СВТ классов «3А», «2А» и «1А»)

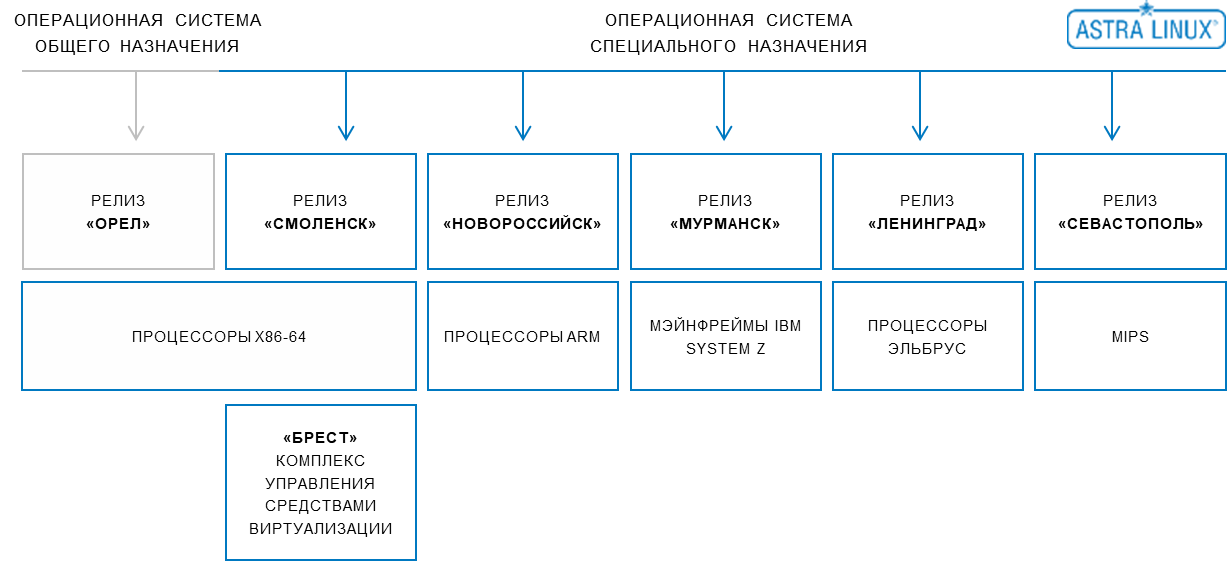


Рисунок 2 – Релизы ОС AstraLinux

Соответствие требованиям регуляторов обеспечивают:

* + встроенная система безопасности PARSEC;
  + мандатное разграничение доступа;
  + изоляция модулей;
  + очистка оперативной и внешней памяти и гарантированное удаление файлов;
  + маркировка документов;
  + регистрация событий;
  + защита информации в графической подсистеме;
  + ограничение действий пользователя (режим «киоск»);
  + защита адресного пространства процессов;
  + контроль замкнутости программной среды и целостности;
  + средства организации единого пространства пользователей;
  + защищенная среда виртуализации;
  + защищенная реляционная СУБД;
  + защищенные комплексы программ электронной почты и гипертекстовой обработки данных;
  + средства для работы с мультимедиа и изображениями.

Продукты Astra Linux входят в реестр отечественного ПО при Минцифры. ОС Astra Linux принята в стандарт ФОИВов и госкорпораций, кроме того, она имеет полный набор сертификатов Минобороны России, ФСТЭК (Федеральная служба по техническому и экспортному контролю) и ФСБ.

**2 Установка ОС AsrtaLinux SE (см. Руководство пользователя РУСБ.10015-01 93 01)**

Минимальные требования:

* аппаратная платформа — процессор с архитектурой x86-64 (AMD, Intel);
* оперативная память — от 4 ГБ;
* объем свободного дискового пространства — от 16 ГБ;
* устройство чтения DVD-дисков;
* стандартный монитор SVGA.

Начало процесса установки:

1. По умолчанию установка начнется графическая установка на русском языке, но при запуске установщика есть возможность выбрать язык. К выбору предлагаются варианты (на русском и английском языке): текстовая установка (Install), графическая установка (Graphical install), режим экспертной установки (Expert Install) и Resque (Режим восстановления).
2. Лицензионное соглашение доступно только на русском языке.
3. Ввести имя машины (hostname)
4. Создание учетной записи пользователя. Будет создана учетная запись пользователя, входящего в группу astra-admin, то есть имеющего выполнять команды от имени суперпользователя с помощью sudo. Будет предложено выбрать имя пользователя и пароль. Если установка производится на сервер, доступный по сети, имя пользователя должно быть не словарное, чтобы уменьшить вероятность взлома сервера с помощью подбора имени пользователя и пароля. Не следует использовать простые, очевидные и легко подбираемые имена пользователей. Независимо от роли компьютера, на который устанавливается операционная система, с целью исключения несанкционированного доступа, не следует использовать короткие простые, легкоподбираемые пароли. Пароль должен иметь размер не менее 8 символов (а лучше – больше), содержать символы латинского алфавита в верхнем и нижнем регистре, цифры, знаки препинания. Пароль не должен использоваться больше нигде, ни на других сервисах, сайтах и т.д.
5. Выберите ваш часовой пояс. Если вашего часового пояса нет, с помощью клавиши «Tab» выберите Go Back и выберите язык, страну и при необходимости регион, чтобы предоставить верный выбор часовых поясов.
6. **Разметка диска - выбирать «Ручная»!!!**

Доступны варианты разметки диска:

* автоматическая – используя весь диск;
* автоматическая – используя весь диск и LVM;
* автоматическая – используя весь диск и зашифрованный LVM;
* ручная.

**Пример разбиения диска емкостью 20Gb.** Он разбивается следующим образом:

* + - * раздел ESP (EFI System Partition) – 512 Mb;
      * основной раздел: файловая система Ext4, точка монтирования /, размер 10Gb;
      * раздел swap – 5 Gb
      * раздел /home: файловая система Ext4, точка монтирования /home, размер 5Gb

В примере разобран случай разбиения диска 20 Gb. Это чуть больше, чем минимальные требования к установке. Можно (и желательно) использовать и более емкий накопитель. Обязательно выделять раздел EFI в случае использования EFI, его размер чуть больше, чем 500 Мб. Под swap выделяется место исходя из объема оперативной памяти. Если планируется гибернация – то объем swap должен быть не меньше, чем объем оперативной памяти (и обладать определенным запасом, +1-2Гб). В случае сервера достаточно под swap выделить 1-3 Гб, и в дальнейшем при необходимости увеличить. Под / и /home выделяется все остальное пространство, при этом большая часть дискового пространства выделяется под /. Отдельный раздел под /home имеет смысл выделять для сохранности документов пользователей в случае переустановки, и не имеет особого смысла для сервера.

**Этапы разбиения диска:**

1. Выбирать диск для разметки – указывается его имя устройства, размер и тип. Чтобы вернуться к выбору типа разметки следует выбрать Guided partitioning.
2. Предупреждение об уничтожении предыдущей разметки. Если выбрано все устройство – это потенциально разрушительное действие. Если на устройстве уже присутствуют разделы они будут стерты. Поэтому по умолчанию стоит отказ от продолжения – No, следует явным образом указать о согласии. Если устройство новое – выбираете Yes. Если на устройстве есть данные, и вы уверены, что они не нужны, также выбираете Yes. Если на устройстве есть важные данные, то следует нажать No и вернуться к предыдущему шагу.
3. Выделить свободное место, чтобы создать раздел.
4. Выбрать – Создать новый раздел и далее ввести размер раздела 512 Мб. Будет предложено два варианта размещения раздела – в начале диска или в конце. Выбираем в начале, нажимаем Enter.
5. Выбирать пункт меню «Use as» и нажать Enter.

По умолчанию установщик предлагает создать раздел как корневой раздел / c файловой системой Ext4. Ннеобходимо создать раздел диска для загрузчика Efi, поэтому выбираем Use as и нажать Enter.

1. Выбать вариант EFI System Partition и нажать Enter.
2. Подтвердить создание раздела - выбрать пункт Done setting up the partition и нажать Enter.
3. Создание следующего раздела - выделить оставшееся свободное пространство и Enter.
4. Создать раздел для корня системы / - действия в интерфейсе аналогичны проделанным для предыдущего раздела: выбираем Create a new partition, размер 10 Gb.
5. Раздел для корневой системы Use as: Ext 4 journaling file system Mount point:/ Оставить по умолчанию и выбрать Done setting up partition, Enter.
6. Создать раздел swap. Для этого:

* выбрать оставшийся свободный раздел;
* Create a new partition, размер 5 Gb – по объему оперативной памяти + 1 Gb (для рабочей станции – резервируем место под гибернацию, для сервера достаточно 1-3Gb);
* размещение Beginning;
* Use as по умолчанию установлен как ext4, выбираем этот пункт, чтобы установить swap.

Создаем swap - выбрать swap area и Enter, оставить Use as: swap area, нажать Done setting up the partition как это было сделано ранее.

1. Раздел для /home - выбрать оставшееся свободное пространство и нажать Enter. Выбрать Create a new partition, размер оставить предложенный. Далее оставить по умолчанию и нажимаем Done setting up the partition. В данном случае нужно оставить параметры по умолчанию:

* Use as: ext4 journaling file system
* Точка монтирования: /home. При необходимости, исправить (если предлагается точка монтирования /usr, следует исправить на /home).

13. Таблица разделов. Если есть ошибки, то выбрать нужный раздел и исправить. Если все верно, выбрать пункт Finish partitioning and write changes on disk.

Цель достигнута, мы имеем:

* Раздел EFI для загрузчика
* Раздел для операционной системы /
* Раздел для swap
* Раздел для /home – может быть полезен, если понадобится переустановить операционную систему, не уничтожая данные пользователя.

Далее необходимо еще раз все проверить. По умолчанию вопрос «Записать изменения на диск?» имеет ответ «No», выбрать вариант «Yes». После того, как подтвердили запись разделов на диск, начинается процесс установки.

14. Выбор ПО - оставить по умолчанию. При необходимости добавить SSH server (нажатием пробела), нажать TAB, выбрать Continue.

При необходимости удаленного доступа к компьютеру можно установить ssh. В этом случае следует учесть, что по ssh доступ к компьютеру может получить и злоумышленник, потому имя пользователя и пароль должны быть нетривиальными, не должно быть у злоумышленника возможности их быстро подобрать.

15. Установка ALD пока не нужна, пропустить, нажать Continue. Ожидаем пока система распаковывает и устанавливает ПО.

**Дополнительные настройки.** Пробел устанавливает или снимает дополнительную опцию, Tab переключает на кнопку Continue. Выбрать Continue и Enter

Доступны для включения следующие опции:

- включить проверку сигнатуры исполняемых файлов – режим замкнутой программной среды, в котором могут быть запущены только те ELF-приложения, исполняемые файлы которых подписаны цифровой подписью разработчика, чей открытый ключ добавлен в перечень ключей, которым доверяет операционная система. Исполняемые файлы и разделяемые библиотеки с неверной цифровой подписью или без нее не могут быть загружены и запущены;

- запретить установку бита исполнения – запрет на установку для файлов права x (chmod +x) для обычных пользователей;

- использовать Hardened-ядро – модифицированную версию ядра с дополнительными механизмами защиты, такими как очистка остаточной информации в стеке и куче ядра, содержит ряд изменений для защиты ядра от внедрения вредоносного кода;

- запретить вывод меню загрузчика – при запуске операционной системы меню загрузчика GRUB выводиться не будет;

- включить очистку swap – разделов страничного обмена (с учетом того, что очистка освобождаемых ресурсов как правило не работает на SSD-дисках;

- включить очистку освобождаемых областей для EXT-разделов. При включенной опции данные любых удаляемых/урезаемых файлов в пределах заданной ФС предварительно очищаются предопределенной или псевдослучайной маскирующей последовательностью. Следует учесть, что очитска освобождаемых ресурсов как правило не работает на SSD-дисках;

- включить блокировку консоли – запрещает обычным пользователям консольный вход в систему;

- включить межсетевой экран uwf – при выборе данного пункта будет включен межсетевой экран ufw и запущена фильтрация сетевых пакетов в соответствии с заданными настройками;

- включить системные ограничения ulimits – при выборе данного пункта будут включены системные ограничения, установленные в файле/etc/security/limits.conf

- отключить возможность трассировки ptrace – при выборе данного пункта будет отключена возможность трассировки и отладки выполнения программного кода.

При включении блокировки интерпретаторов блокируется несанкционированное использование интерпретатора для выполнения кода напрямую из командной строки или из неименованного канала (pipe). При этом сценарии из каталога /usr/bin/, написанные для этих интерпретаторов, выполняются в штатном режиме.

- отключить автоматическую конфигурацию сети – при выборе данного пункта будет отключена автоматическая настройка сети в процессе установки Astra Linux;

-включить 32-битный загрузчик –при выборе данного пункта из системы будет удален 64-х битный загрузчик EFI и установлен 32-х битный загрузчик EFI.

**Обратите внимание!** Выбор данной опции при установке на 64-х битную вычислительную машину с поддержкой EFI может привести к тому, что установленная система не загрузится.

16. Установка GRUB – введите и подтвердите пароль.

17. Система установлена, необходимо выполнить перезагрузку.

18. Войти в систему пользователем, созданным при установке. Терминальный вход пользователем root заблокирован (не установлен пароль). Пользователь, созданный во время установки, входит в группу astra-admin и может выполнять любые команды через sudo (/etc/sudoers).

19. Установить дополнения –Update 6.

20. Включить мандатный контроля целостности на системные каталоги. По умолчанию он выключен, его следует включить. Узнать состояние мандатного контроля целостности

sudo set-fs-ilev status

Включение мандатного контроля целостности на системные каталоги выполняется командой sudo set-fs-ilev

**3 Вход в систему**

Сессия – сеанс взаимодействия пользователя с операционной системой, открывающийся после успешной авторизации в системе и завершающийся после выхода из сессии. Взаимодействие осуществляется благодаря оболочке – программе, предоставляющий интерфейс пользователя, графический или текстовый. Рабочий стол появляется на экране монитора после входа пользователя в графическую среду. Он содержит пространство рабочего стола с фоновым изображением, панель задач и графические элементы интерфейса пользователя. Само пространство рабочего стола и панель задач также являются элементами интерфейса пользователя.

Сессия – сеанс взаимодействия пользователя с операционной системой, осуществляемый благодаря текстовой (как правило bah) или графической (Fly-wm) оболочке. Вход в сессию осуществляется после успешной авторизации пользователя. Сессия включает набор процессов, запущенных пользователем оболочки или автоматически. Запущенные в сессии процесс получают привелегии и идентификатор пользователя, выполнившего вход в систему. Графическая сессия может быть запущена в одном из режимов (декстоп, планшет, мобильный), адаптированном под те или иные типы устройств, на которых запущена операционная система.

В состав Astra Linux входит рабочий стол Fly, который состоит из оконного менеджера и набора графических утилит и программ, как пользовательских, так и административных. После успешного ввода логина и пароля и, при необходимости, указания атрибутов безопасности учетной записи будет запущена сессия вашего пользователя и открыт рабочий стол. Фон рабочего стола сигнализирует о режиме целостности – если он красный, это означает что сессия запущена в высоком режиме целостности и предназначена для администрирования. При низком уровне целостности фон рабочего стола – синий.

Типы сессии:

- десктоп – устанавливается по умолчанию;

- режим восстановления – в графической среде будет запущен только терминал, что позволяет администрировать в режиме командной строки, но при необходимости запускать и графические приложения;

- мобильный;

- планшетный.

Меню:

- сменить пользователям (Alt-I) – позволяет переключаться между активными сеансами пользователей (включая входы на виртуальные терминалы). При выборе этого пункта будут отображаться активные сессии и возможность выбора окна входа;

- перезапустить X Server (Alt-E) – перезапустить графическое окружение;

- виртуальная клавиатура (Alt-K) – откроет виртуальную клавиатуру (такой же эффект достигается щелчком по значку клавиатуры в левом нижнем углу экрана);

- консольный вход (Alt-N) –временно закроет графический режим и переведет в режим терминала, все сессии будут принудительно закрыты;

- завершение работы (Alt-S) – выведет окно завершения работы.

- щелчок по этому значку, в случае корректных имени пользователя и пароля откроет окно выбора уровня конфиденциальности и целостности. В случае неверного ввода имени пользователя и/или пароля на короткое время появится надпись «Login failed».

**Обратите внимание!** на регистр – регистр имеет значение, буква в верхнем и нижнем регистре считаются разными символами.

**2.1 Уровни конфиденциальности, целостности, категории.**

В случае успешного ввода имени пользователя и пароля, если учетная запись пользователя активна, появляется окно выбора уровня конфиденциальности, неиерархического уровня целостности и неиерархической категории целостности. Уровень конфиденциальности задает степень повышающейся секретности. По умолчанию (а также, если уровни конфиденциальности) не заданы – используется самый низкий уровень – **Не секретно**.

Возможные варианты уровней конфиденциальности – Не секретно, Для служебного пользования, Секретно, Совершенно секретно.

Уровень целостности (неиерархический уровень целостности) – атрибут, отвечающий за то, чтобы информацию не могли изменять те, кому ее не положено изменять. По умолчанию, доступны два уровня целостности – Низкий и Высокий.

Для обычного использования ЭВМ применяется низкий уровень целостности, для администрирования – высокий.

Категория (неиерархическая категория) – также, как и уровень конфиденциальности, служит для того, чтобы информация не попадала тому, кто не уполномочен ее получать. Если уровни конфиденциальности – «вертикальная градация» полномочий (с линейным повышением-понижением), то неиерархические категории – это «горизонтальная градация». Например, сотрудники разных отделов могут получить категории согласно их отделам, а руководитель вышестоящей организационной структуры может иметь доступ к категориям всех нижестоящих отделов.

В случае, если выбран высокий уровень целостности, цвет фона рабочего стола, рамок и заголовок окон, панели быстрого запуска и области уведомления, устанавливается красный, что сигнализирует о том, что практически все действия разрешены и могут быть потенциально разрушительны. Высокий уровень целостности следует применять только для администрирования, он не подходит для постоянной работы. При выполнении административных задач требуется крайне внимательно подходить ко всем совершаемым действиям.

В панели уведомлений доступен индикатор мандатных уровней доступа. Он отображает уровень конфиденциальности (по умолчанию 0), также при наведении курсора мыши (во всплывающем информационном поле) либо при щелчке мыши по индикатору мандатных уровней (в отдельном окне) будет показана информация о мандатных уровнях. Уровень конфиденциальности, уровень целостности (63 – высокий уровень целостности), категориях и ролях. Элементы интерфейса (рабочий стол, ярлыки, кнопка и меню «Пуск», панель быстрого запуска, переключатель задач, область уведомлений и т.д.) при работе в низком уровне целостности идентичны (за исключением прав и расцветки).

**4 Завершение работы**

- Блокировка – сессия пользователя будет заблокирована, появится окно блокировки. Для возобновления работы потребуется ввести пароль. Блокировку следует использовать, если требуется отойти от рабочего места.

- Сон – «легкое выключение» компьютера. Компьютер приостанавливает работу, но в оперативной памяти сохраняются данные. Поэтому обратное «включение» – «пробуждение» компьютера происходит очень быстро. В случае отключения питания все несохраненные данные будут потеряны.

- Гибернация – похоже на сон, но в этом случае данные из оперативной памяти сохраняются на диск. Возобновление работы возможно даже при отключении питания.

- Выход из сессии – завершается сессия текущего пользователя и происходит переход в окно входа.

- Перезагрузка – компьютер будет перезагружен.

- Выключение – компьютер будет выключен, все программы будут завершены.

- Планирование – позволяет выполнить любую из вышеперечисленных операций не мгновенно, а запланировать ее на некоторое время. Можно выбрать, как скоро операция будет выполнена, а также когда об этом следует напомнить – предупредить.

-Новый вход – по нажатию на эту кнопку появляются/скрываются две дополнительные кнопки «Отдельный» (Console) и в «Окне». Данная операция может понадобится, когда потребуется временно войти в систему под другим пользователем, не закрывая программы и документы в открытой сессии.

Отдельный (Console)– в этом случае данная сессия будет приостановлена (но не закрыта), и будет открыто окно входа. Чтобы вернуться обратно, нужно воспользоваться на экране входа «Меню»(Menu), выбрать пункт «Смена сессии»(Switch User) и выбрать открытую сессию для перехода в нее (будет открыт экран блокировки для ввода пароля пользователя).

В окне – данная сессия не будет приостановлена а новая сессия будет открыта во вложенном окне.

- Закрыть – закрывает окно «Выход или выключение».

Чтобы переключаться между отдельными сессиями, можно воспользоваться Меню Пуск>Завершение работы (Exit)>Новая сессия(Switch)>Отдельная сессия (Console)>Экран входа>Меню> «Смена сессии» (Switch User) и выбрать нужную сессию. Значительно проще для переключения сессий использовать клавиатурные сокращения. Ctrl-Alt-F1, Ctrl-Alt-F2… Ctrl-Alt-F6 для текстовых сессий, Ctrl-Alt-F7, Ctrl-Alt-F8, Ctrl-Alt-F9 и т.д. для графических.

**Дополнительная информация** <https://wiki.astralinux.ru/pages/viewpage.action?pageId=327739>

**МЕТОДИКА ВЫПОЛНЕНИЯ**

1. Выполнить поэтапную установку Astra Linux SE с **ручной разметкой накопителя!** (уметь рассказать процесс) согласно п. 2 Теоретических сведений
2. Рассмотреть и произвести дополнительные настройки (рассказать о них преподавателю).
3. Установить дополнения.
4. Включить мандатный контроль целостности на системные каталоги.
5. Установить и запустить утилиту GParted (сделать скриншот).
6. Осуществить вход в систему (рассказать типы сессий, меню, все уровни конфидециальности и целостности, категории)
7. Выполнить пользовательские настройки, см. Презентацию к ЛР1.
8. Показать навыки монтирования/размонтирования сьемных носителей, см. Презентацию к ЛР1.
9. Ознакомиться с работой LibreOffice, см. Презентацию к ЛР1.

**КОНТРОЛЬНЫЕ ВОПРОСЫ**

1. Назначение ОС AstraLinux SE.
2. Сравнительная характеристика AstraLinux SE и AstraLinux CE.
3. Виды защищаемой информации AstraLinux SE.
4. Какой раздел необходимо создать обязательно при EFI-установке?
5. В какую группу будет включен созданный при установке пользователь?
6. Какое действие следует сделать после установки для включения мандатного контроля целостности на системные каталоги?
7. Что означает цвет Рабочего стола AstraLinux SE?
8. Какие вAstraLinux SE уровни конфидециальности и целостности, категории?
9. Как открыть новую сессию не используя режим окна?
10. Как вернуться в одну из предыдущих запущенных сессий с помощью элементов интерфейса?
11. Как вернуться в одну из предыдущих запущенных сессий, используя клавиатурные сокращения?