64: Комплексная система защиты в операционной системе ASTRA

Актуализация опорных знаний **1**
Понятие информационной безопасности 1
Контроль доступа 2
Общая характеристика операционной системы ASTRA **2**
Обзор дистрибутивов системы 3
Основные общесистемные компоненты 5
Основные элементы комплексной системы защиты ОС ASTRA ... 6
Контроль доступа и целостности **7**
Управление доступом 7
Изоляция процессов и защита памяти 8
Фильтрация сетевого потока **9**
Другие элементы системы защиты **9**
Доверенная аутентификация Kerberos 9
Контроль подключения съемных машинных носителей информации 10
Очистка виртуальной и внешней памяти 10
Контрольные вопросы **10**

Информационное обеспечение:

ОИ4. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей/В.Ф. Шаньгин. – М.: ИД Форум, 2021. – 416 с. – С. 179-190 (Глава 8. Обеспечение безопасности операционных систем).

Операционная система специального назначения ASTRA Linux. Руководство по КСЗ. – М.: 2021. – 220 с.

Операционная система специального назначения «ASTRA Linux Special edition». Руководство администратора. – М.: 2021. – 334 с.

Актуализация опорных знаний

Понятие информационной безопасности

В соответствии с наиболее популярными моделями безопасности информационная система находится в состоянии безопасности, если она защищена от нарушений конфиденциальности, целостности и доступности, где:

- **конфиденциальность** (confidentiality) — состояние ИС, при котором информационные ресурсы доступны только тем пользователям, которым этот доступ разрешен;
- **целостность** (integrity) — состояние системы, при котором информация, хранящаяся и обрабатываемая этой ИС, а также процедуры обработки информации не могут быть изменены, удалены или дополне-

ны неавторизованным образом;
- **доступность** (availability) — состояние системы, при котором услуги, оказываемые системой, могут гарантированно и с приемлемой задержкой быть предоставлены пользователям, имеющим на это право.

При этом

Успех в области информационной безопасности может принести только системный подход,

при котором средства защиты разных типов применяются совместно и под централизованным управлением.

Общепризнанным является представление множества разных средств защиты в виде четырех иерархически организованных уровней:
- законодательного,
- административного,
- процедурного и
- технического уровней.

Операционные системы предоставляют базовые средства технического уровня.

Контроль доступа

Большинство реализуемых на практике способов управления доступом может быть отнесено к одной из следующих категорий:
- **дискреционный** метод доступа (Discretionary Access Control1, DAC), называемый также избирательным или произвольным;
- **мандатный** метод доступа (Mandatory Access Control2, MAC), называемый также принудительным;
- **ролевой** доступ (Role-based Access Control, RBAC), называемый также недискреционным методом доступа (nondiscretionary access control).

Общая характеристика операционной системы ASTRA

Вопрос импортозамещения на российском рынке обсуждается уже достаточно давно, однако в последние месяцы он заиграл новыми красками. На фоне приостановки в России деятельности Microsoft, Adobe, Autodesk и других крупных разработчиков вопрос создания отечественного программного обеспечения актуален как никогда.

Наиболее остро стоит вопрос касательно замещения операционных систем, а именно – Windows, серии самых популярных ОС в мире. Среди всех отечественных ОС наиболее узнаваемые и обсуждаемые Astra Linux и «Альт» ОС (ALT).

Обзор дистрибутивов системы

Astra Linux это российская ОС, основанная на базе популярного открытого дистрибутива Linux под названием Debian.

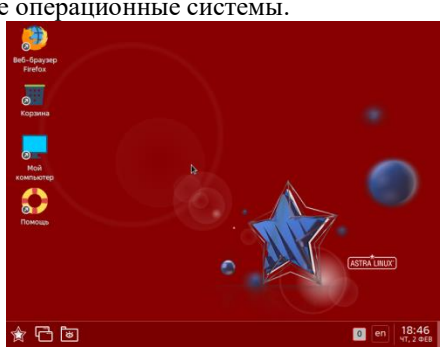
Изначально предназначалась как безопасная система для силовых структур, но на фоне санкций и шквала кибератак на российские инфраструктуры именно о ней сейчас всё больше говорят, когда дело доходит до поиска замены Microsoft Windows.

Позиционируется как единственная операционная система в стране, соответствующая требованиям безопасности информации всех регуляторов: ФСБ, Минобороны, ФСТЭК

Официальный сайт:
https://astralinux.ru/products/astra-linux-special-edition/

ОС имеет две версии – Special Edition, ориентированная на корпоративных заказчиков и Common Edition для общего пользования.

На рисунках ниже показаны обе операционные системы.



Special Edition

Среди компаний ОС Astra Linux распространяется в основном по временной лицензии, хотя в некоторых ревизиях всё же имеется возможность приобрести бессрочную подписку.

Версия Special Edition сертифицирована различными ведомствами и обладает встроенными средствами защиты информации (СЗИ).
Система имеет 3 редакции с разными уровнями защищённости:

- **Базовый** уровень защищенности «Орел»;
- **Усиленный** уровень защищенности «Воронеж»;
- **Максимальный** уровень защищенности «Смоленск».

Уровень «Орел» рекомендуется для обработки и зашиты общедоступной информации и информации ограниченного доступа, в том числе в составе значимых объектов КИИ, ГИС 3 класса защищенности и в информационных системах персональных данных 3-4 класса защищенности.

Уровень «Воронеж» рекомендуется для обработки конфиденциальной информации в ГИС, информационных системах персональных данных, а также в составе значимых объектов КИИ любого класса защищенности.

Уровень «Смоленск» рекомендуется для обработки информации любой категории доступа в ГИС, в информационных системах персональных данных, в составе значимых объектов КИИ, иных информационных системах, обрабатывающих информацию ограниченного доступа, в том числе содержащую сведения, составляющие гостайну, до степени «особой важности» включительно.

Существует полностью бесплатная несертифицированная версия Astra Linux – Common Edition .

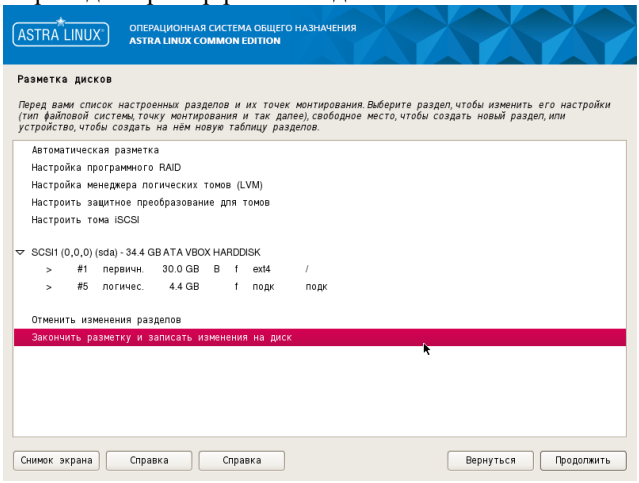
Именно она как раз ориентирована на рядового пользователя. И о ней будем говорить далее.

Для установки требуется немного времени (~15-20 минут) и минимум 20 ГБ свободного места на диске.

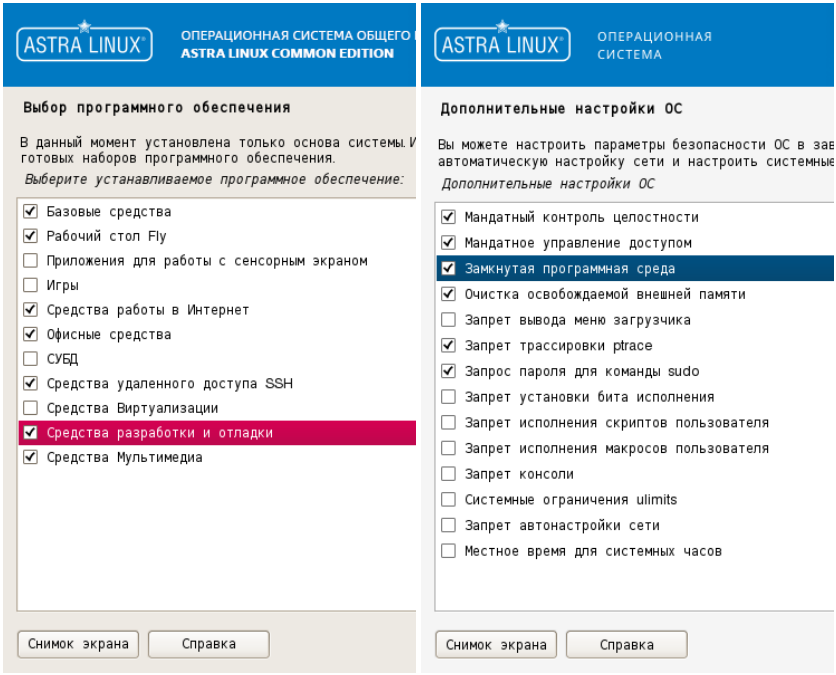
Порядок установки операционной системы вынесен для самостоятельного изучения. По окончании процесса установщик попросит задать имя и пароль учётной записи в системе.

При установке следует обратить внимание на два важных этапа: разметка диска и выбор программного обеспечения.

Ниже приведен пример разметки диска:



Выбор программного обеспечения зависит от редакции. На рисунках ниже приведены скриншоты выбора программного обеспечения для редакции Common Edition и для редакции Special Edition. Обратите внимание, что мандатный доступ предусмотрен только в Special Edition.



Основные общесистемные компоненты

За интерфейс системы отвечает графическая оболочка Fly, фирменная разработка компании «Русбитех».

Дизайн Fly максимально напоминает Windows XP, поэтому для многих Astra Linux будет интуитивно понятной.

Из коробки предусмотрен стартовый набор необходимых драйверов и программ. Это:

- Базовый набор офисных приложений – LibreOffice (аналог Microsoft Office);
- Доступ в интернет из коробки, никаких дополнительных драйверов не нужно;
- По умолчанию в системе уже имеется 2 браузера: Mozilla Firefox и Chromium;
- Файловый менеджер, способный выступать в роли архиватора;

Имеются также прочие свободные программы: Blender и qBittorrent, поддержка планшетных и мобильных функций, популярные видео- и аудио-редакторы: Audacity, VLC.

По умолчанию Astra Linux использует офисный пакет LibreOffice.

В ОС используются программные пакеты (далее по тексту — пакеты) в формате «**.deb**».

Для управления пакетами в режиме командной строки (или в эмуляторе терминала в графическом режиме) предназначены набор команд нижнего уровня **dpkg** и комплекс программ высокого уровня **apt-get**, **apt-cache** и **aptitude**. В графическом режиме управлять пакетами можно с помощью программы **synaptic** (универсальная графическая оболочка для **apt**).

По умолчанию обычный пользователь не имеет права использовать эти инструменты. Для всех операций с пакетами (за исключением некоторых случаев получения информации о пакетах) необходимы права суперпользователя, которые администратор может получить через механизм **sudo**.

Основные элементы комплексной системы защиты ОС ASTRA

В состав КСЗ входят следующие основные подсистемы:

- ❑ - модули подсистемы безопасности PARSEC, входящие в состав ядра ОС;
- ❑ - библиотеки;
- ❑ - утилиты безопасности;
- ❑ - подсистема протоколирования (регистрации);
- ❑ - модули аутентификации;
- ❑ - графическая подсистема;
- ❑ - консольный вход в систему;
- ❑ - средства контроля целостности;
- ❑ - средства восстановления;
- ❑ - средства разграничения доступа к подключаемым устройствам.

Эти подсистемы позволяют решить основные задачи по информационной безопасности.

КСЗ обеспечивает реализацию следующих функций ОС по защите информации от несанкционированного доступа:

- ❑ - идентификацию и аутентификацию;
- ❑ - дискреционное и мандатное управление доступом;
- ❑ - регистрацию событий безопасности;
- ❑ - ограничение программной среды;
- ❑ - изоляцию процессов и защиту памяти;
- ❑ - контроль целостности;
- ❑ - фильтрацию сетевого потока;
- ❑ - маркировку документов;
- ❑ - контроль подключения съемных машинных носителей информации (защиту ввода-вывода на отчуждаемый физический носитель информации).

Контроль доступа и целостности

Управление доступом

Функция идентификации и аутентификации пользователей в ОС ASTRA основывается на использовании механизма PAM.

PAM (Pluggable Authentication Modules, подключаемые модули аутентификации) представляют собой набор разделяемых библиотек (т.н. модулей), с помощью которых системный администратор может организовать процедуру аутентификации (подтверждение подлинности) пользователей прикладными программами. Каждый модуль реализует собственный механизм аутентификации. Изменяя набор и порядок следования модулей, можно построить сценарий аутентификации.

По умолчанию в операционной системе установлено дискреционное управление доступом.

При этом для каждого объекта в системе установлен набор атрибутов «чтение/запись/исполнение» - rwx. Права задаются отдельно для владельца, группы пользователей и прочих пользователей.

Дополнительно в ОС механизмом дискреционных ПРД поддерживаются списки контроля доступа ACL (Access Control List), реализованные на основе расширенных атрибутов файловых систем.

С использованием ACL можно дополнительно для каждой сущности задавать права на доступ субъектов к ней.

ACL состоит из набора записей. Права доступа к сущности для пользователя-владельца, группы-владельца и всех остальных имеют соответствующее представление в ACL в виде отдельных записей. ACL, соответствующий базовым правилам разграничения доступа (ПРД), называется минимальным ACL. Таким образом, каждой сущности всегда сопоставляется минимальный ACL, включающий три записи: для пользователя-владельца, группы-владельца и всех остальных.

Права доступа для дополнительных субъектов определяются в дополнительных записях ACL.

При реализации политики мандатного управления доступом субъектам и сущностям задаются **классификационные метки (уровни конфиденциальности и категории конфиденциальности**).

Уровень конфиденциальности определяет степень секретности сущности и соответствующий уровень доступа к ней, назначенный субъекту.

Он представляет собой числовое значение от 0 до 255 (включительно). Каждой классификационной метке в каждый момент времени может быть назначен только один уровень конфиденциальности. Классический пример – уровни «для служебного пользования», «секретно», «совершенно секретно» и т.д.

Для более точного управления доступом, в дополнение к разделению по уровням конфиденциальности, СЗИ предоставляет возможность разделить материалы по **категориям конфиденциальности**. Например, два проекта «Танки» и «Самолеты» могут иметь одинаковый уровень конфиденциальности «секретно», но разные категории конфиденциальности. В этом случае персонал проекта «Танки» не должен обмениваться информацией с персоналом проекта «Самолеты» и наоборот. Руководитель же может иметь обе категории конфиденциальности.

Итак, с помощью параметров **уровень конфиденциальности** и **категории конфиденциальности** СЗИ обеспечивает защиту от несанкционированной передачи информации:

- Невозможность прочитать информацию, к которой не предоставлен доступ: "нижним" уровням запрещено читать информацию с "верхних" уровней; всем запрещено читать информацию, на которую нет разрешенной категории конфиденциальности;
- Невозможность передать информацию тому, кому не предоставлен доступ: "верхним" уровням запрещено записывать свою информацию на "нижние" уровни; всем запрещено передавать информацию тем, у кого нет соответствующей категории конфиденциальности.

Мандатное управление доступом и мандатный контроль целостности могут быть включены в процессе установки ОС путем выбора соответствующих пунктов программы установки ОС.

Включение мандатного управления доступом после установки ОС выполняется с помощью инструмента **`astra-mac-control`** или графической утилиты **`fly-admin-smc`**.

В операционной системе ASTRA также предусмотрен мандатный контроль целостности.

Уровень целостности сущности отражает степень уверенности в целостности содержащейся в ней информации. Пользователь не может изменять информацию, если уровень целостности не соответствует заданному для документа.

Изоляция процессов и защита памяти

Ядро ОС обеспечивает для каждого процесса в системе собственное

изолированное адресное пространство.

Данный механизм изоляции основан на страничном механизме защиты памяти, а также механизме трансляции виртуального адреса в физический, поддерживаемый модулем управления памятью. Одни и те же виртуальные адреса (с которыми и работает процессор) преобразуются в разные физические для разных адресных пространств.

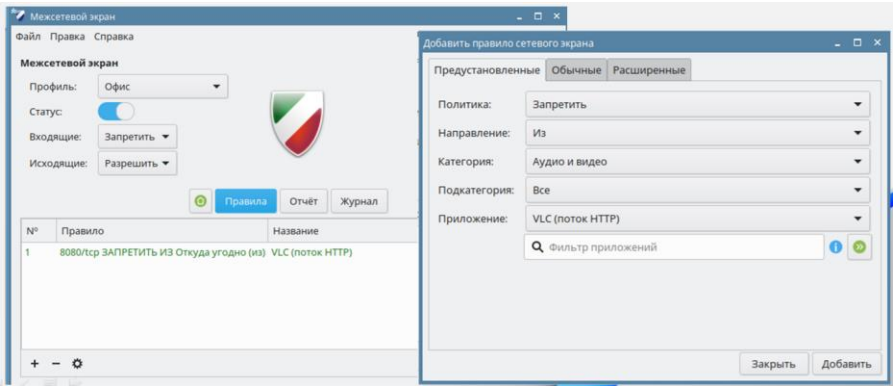
Процесс не может несанкционированным образом получить доступ к пространству другого процесса,

т.к. непривилегированный пользовательский процесс лишен возможности работать с физической памятью напрямую. Ядро ОС гарантирует, что обычный непривилегированный процесс не получит данные чужого процесса.

Фильтрация сетевого потока

При помощи фильтра сетевых пакетов можно осуществлять контроль сетевого трафика, проходящего через компьютер. Запуск фильтрации пакетов обеспечивается межсетевым экраном **`ufw`**. Межсетевой экран позволяет создавать правила фильтрации используя технологию iptables.

Управление межсетевым экраном осуществляется с помощью графической утилиты **`gufw`** или с помощью инструмента командной строки **`astra-ufw-control`**.



Другие элементы системы защиты

Доверенная аутентификация Kerberos

Kerberos является протоколом, обеспечивающим централизованную аутентификацию пользователей и применяющим техническое маскирование данных для противодействия различным видам атак.

Основным компонентом системы Kerberos является центр распределения ключей (KDC). Программы, настроенные на взаимодействие с Kerberos, называются «кербиризованными приложениями». KDC отвечает за аутентификацию в некоторой области Kerberos.

В процессе работы система Kerberos выдает билеты (tickets) на использование различных служб.

Контроль подключения съемных машинных носителей информации

Съемные машинные носители информации могут рассматриваться относительно ОС с двух точек зрения:

- как блочные или символьные устройства ввода-вывода;
- как блочное устройство, которое может быть смонтировано.

В первом случае устройство представляет собой специальный файловый объект, доступ к которому контролируется мандатными и дискреционными правилами разграничения доступа обычным образом и, следовательно, ввод-вывод остается в рамках контроля этих правил.

Во втором случае съемный машинный носитель информации содержит в себе образ файловой системы, которая и хранит данные. Данный носитель может быть смонтирован в заданный каталог, и при этом ФС носителя становится частью (представленной в виде поддерева) корневой ФС. Доступ к объектам данной ФС подчиняется мандатным и дискреционным ПРД обычным образом и, следовательно, ввод-вывод на съемный машинный носитель информации остается в рамках контроля этих правил.

В качестве файловых систем на съемных машинных носителях информации должны использоваться только файловые системы ext2/ext3/ext4/xfs, поддерживающие расширенные (в т.ч. мандатные) атрибуты файловых объектов и обеспечивающие гарантированное уничтожение (стирание) информации.

Очистка виртуальной и внешней памяти

В ОС реализован механизм очистки освобождаемой внешней памяти. Механизм очистки очищает неиспользуемые блоки файловой системы непосредственно при их освобождении, а также очищает разделы страничного обмена. Работа данного механизма снижает скорость выполнения операций удаления и усечения размера файла.

Данные любых удаляемых/урезаемых файлов в пределах заданной ФС предварительно очищаются предопределенной или псевдослучайной маскирующей последовательностью.

Контрольные вопросы

1. На базе какого дистрибутива разработана ОС ASTRA?
2. Перечислите основные редакции ОС ASTRA.

3. Назовите бесплатную несертифицированную редакцию ASTRA.

4. На чем основана идентификации и аутентификации пользователей в ОС ASTRA?

5. Перечислите известные методы доступа. Какие из них реализованы в ОС ASTRA?

6. Что такое уровень и категория конфиденциальности?

7. Какой метод доступа установлен в ОС ASTRA по умолчанию?

8. Дайте характеристику мандатного метода доступа.