**«Воронеж».** На этом уровне в системе работают СЗИ собственной разработки ГК «Астра», входящие в подсистему безопасности PARSEC. В первую очередь это механизмы мандатного контроля целостности и замкнутой программной среды, которые противостоят угрозе целостности информации.

Эти СЗИ существенно повышают защищенность Astra Linux от взлома, заражения вредоносным ПО, внедрения программных закладок, получения несанкционированных прав и т. д. В таком режиме Astra Linux Special Edition обеспечивает формирование основного рубежа обороны от нарушителей (поверхности атаки), и разработчики рекомендуют заказчикам работать с ОС именно на этом или на «Максимальном» уровнях защищенности.

**«Смоленск».** Максимальный уровень защищенности дополняет возможности «Усиленного» режима функциями мандатного управления доступом (МРД) для защиты от угрозы конфиденциальности информации. Суть этого принципа в распределении информации по явно заданным уровням конфиденциальности и выполнении следующих условий:

1. Читать данные из файла или каталога могут только те процессы и пользователи, которые обладают не меньшим уровнем конфиденциальности, чем у запрашиваемых данных.
2. Записывать данные в файл или каталог могут только те процессы с уровнем конфиденциальности, равным или меньшим, чем у этого файла или каталога.
3. Действия процессов в системе не приводят к явной или неявной утечке конфиденциальных данных «сверху-вниз» – с высокого уровня конфиденциальности на низкий (т. е. к созданию так называемых скрытых каналов).

Эти прозрачные правила позволяют пользователям и администраторам систем учитывать человеческий фактор при работе с ОС. Угрозы случайной компрометации или несанкционированных изменений информации значительно сокращаются благодаря возможности четко распределить данные по условным уровням: например, «открытая», «служебная», «важная», «очень важная». А для более тонкой настройки разработчики предусмотрели неиерархические категории, позволяющие привязать информацию к структурным подразделениям: например, «отдел персонала», «бухгалтерия», «отдел продаж», «руководство компании» и т.д.

Есть также базовый уровень защищённости **«Орёл»**(несертифицированной операционной системы), он не может применяться в корпоративных системах, системах критической информационной инфраструктуры, а также для обработки информации ограниченного доступа, к которой предъявляются требования по защите информации.

В Astra Linux в режимах «Воронеж» и «Смоленск» организован контроль целостности системы и ее компонентов. Файлы, процессы, учетные записи пользователей и прочие компоненты ОС Astra Linux Special Edition распределяются по уровням целостности, после чего штатными средствами безопасности можно защищать компоненты более высокого уровня целостности от несанкционированной записи из компонентов с меньшим уровнем.

Мандатный контроль целостности (MAC) и мандатное управление доступом (Mandatory Access Control) являются двумя различными концепциями в области информационной безопасности. Давайте разберемся в разнице между ними:

1. Мандатный контроль целостности (MAC):

- MAC определяет правила доступа к объектам на основе уровня секретности и целостности данных.

- Система MAC назначает уровни секретности и целостности для каждого объекта и субъекта в системе.

- Пользователям присваиваются различные уровни доступа в зависимости от их уровня секретности и целостности.

- Применение MAC обеспечивает строгий контроль над доступом к данным, и пользователи не имеют возможности изменять или нарушать установленные правила без специального разрешения.

2. Мандатное управление доступом (Mandatory Access Control):

- MAC определяет политику безопасности, которая управляет доступом к ресурсам на основе правил, установленных администратором системы.

- В MAC администратор системы определяет права доступа к файлам, каталогам, сетевым ресурсам и другим объектам в системе.

- Пользователи не могут изменять или переопределять эти правила доступа, так как они устанавливаются централизованно и не зависят от действий пользователей.

Замкнутая программная среда

При включенной функции ЗПС запуск исполняемых файлов и загрузка исполняемых библиотек возможна только при наличии электронной цифровой подписи на доверительном ключе. Это значительно усложняет эксплуатацию уязвимостей, а в большинстве случаев делает ее неэффективной, поскольку остающиеся у нарушителя незначительные возможности обойти защиту практически полностью перекрываются включенным МКЦ.

Во-первых, внедрить нелегитимную ЭЦП может только пользователь с высоким уровнем целостности. Во-вторых, даже если «зараженный» файл удастся разместить в системе, а нарушитель смог проэксплуатировать заложенную в этом файле уязвимость и получил, например, root-привилегии, он продолжит работу на том же низком уровне целостности.

Помимо этого, в ОС Astra Linux Special Edition имеются еще дополнительные СЗИ, включая запрет запуска интерпретаторов, ограничение прав непривилегированных пользователей с созданием собственных профилей безопасности. Каждый такой профиль содержит перечень имен каталогов или файлов, права доступа к которым надо дополнительно ограничить.