УДК 004.94

ЗАЩИТА ИНФОРМАЦИИ В СОВРЕМЕННЫХ ОПЕРАЦИОННЫХ СИСТЕМАХ

А. И. ЯКИМОВ, Е. А. ЯКИМОВ, Е. А. ЗАЙЧЕНКО
Белорусско-Российский университет
Могилев, Беларусь

Обеспечение безопасности информационных технологий занимает все более значительное место в учебных планах образовательных систем, например, при подготовке бакалавров по направлениям 09 03 01 «Информатика и вычислительная техника», 09 03 04 «Программная инженерия».

Операционные системы (ОС) используют развитые средства обеспечения безопасности информации, например, аутентификацию и авторизацию пользователей, контроль их действий, криптографическую защиту, защиту от сбоев и атак злоумышленников. Основным механизмом защиты информации является контроль доступа к ресурсам операционной системы, основанный на правилах разграничения доступа к ним для пользователей.

Используется следующая схема: пользователи начинают выполнять операции (чтение/запись/исполнение) с информационными ресурсами, а ОС должна определить, имеют ли они на это право. При этом пользователи являются субъектами доступа, а ресурсы – объектами. Пользователь получает доступ к объектам с помощью прикладных процессов, которые запускаются от его имени. Для каждого типа объектов определяется набор операций, которые с ними можно выполнять. Субъектами доступа могут быть как отдельные пользователи, так и группы. У каждого объекта доступа существует владелец. Система контроля доступа ОС должна предоставлять средства для задания прав пользователей по отношению к объектам дифференцированно по операциям, например, пользователю может быть разрешена операция чтения и исполнения файла, а операция записи – запрещена.

Выделяют два основных подхода к определению прав доступа.

Избирательный доступ – для каждого объекта сам владелец может определить допустимые операции с ними. Между пользователями и группами в системах с избирательным доступом нет жестких иерархических взаимоотношений. Исключение делается только для администратора, по умолчанию наделяемого всеми правами.

Мандатный доступ – система наделяет пользователя определенными правами по отношению к каждому ресурсу в зависимости от того, к какой группе отнесен пользователь. От имени системы выступает администратор, а владельцы объектов лишены возможности управлять доступом к ним по своему усмотрению. Все группы пользователей представляют

иерархию, в которой члены группы не имеют возможности предоставлять свои права членам групп более низких уровней иерархии.

Следует отметить, что большинство ОС общего назначения (Windows 10, macOS, Android) поддерживают только механизм избирательного доступа к ресурсам, что снижает степень защиты информации.

Федеральной службой по техническому и экспортному контролю, Минобороны России сертифицирована ОС Astra Linux Special Edition, в которой реализован механизм мандатного разграничения доступа. Решение о запрете или разрешении доступа субъекта к объекту принимается на основе типа операции (чтение/запись/исполнение), мандатного контекста безопасности, сопряженного с каждым субъектом, и мандатной метки, сопряженной с объектом.

Astra Linux Special Edition является ОС специального назначения, используется для обработки всех видов открытой информации и ограниченного доступа: персональных данных, конфиденциальной, содержащей служебную, банковскую и государственную тайну. Поэтому Astra Linux находит применение не только в государственных и силовых учреждениях, но и в банковском, коммерческом и других секторах экономики.

Все приложения, которые входят в дистрибутив ОС Astra Linux, поддерживают механизмы мандатного контроля доступа. Это позволяет создать единую среду безопасности, включающую ОС и используемое программное обеспечение. Всей информации, попадающей в систему Astra Linux, присваивается уровень конфиденциальности. Носители информации, включая переносимые, также категорируются по уровням конфиденциальности. При выводе документов на печать, документ попадет в защищенный комплекс печати и маркировки документов. По настроенному шаблону формируется штамп, отражающий степень секретности, ФИО, дату и другие данные о печатающем лице. Это позволяет значительно упростить работу с бумажным делопроизводством в соответствии с утвержденными регламентами и политиками безопасности. Данный функционал отвечает современной парадигме управления информационной безопасностью по ISO/IEC серии 27000 и других нормативных актов, специфических для юрисдикций стран СНГ.

Кроме того, ОС Astra Linux поддерживает виртуализацию и терминальные режимы доступа, что дает возможность использовать ее для реализации замкнутой защищенной среды, где в качестве гостевой ОС может выступать любая другая ОС, например, Windows.

Для ЭВМ с процессорами x86-64 разработаны Astra Linux Common Edition (релиз «Орел») и Astra Linux Special Edition (релиз «Смоленск»). Задача приобретения ОС Astra Linux для образовательного процесса может быть решена путем заключения договора с официальным представителем ООО «РусБИТех-Астра» в Республике Беларусь.