Полнофункциональная реализация мандатного контроля целостности в ОССН Astra Linux Special Edition

Девянин П.Н., АО «НПО «РусБИТех», г. Москва, devyanin.peter@yandex.ru
Оружейников А.Л., АО «НПО «РусБИТех», г. Москва, a.oruzheynikov@rusbitech.ru
Соснин Ю.В., АО «НПО «РусБИТех», г. Москва, suv@rusbitech.ru

Обеспечение целостности программно-аппаратной среды является фундаментом, на котором базируются все другие механизмы безопасности операционных систем (ОС). Реализация научно-обоснованных, понятных как для администраторов, так и для пользователей ОС технологий по обеспечению их целостности позволяет использовать другие механизмы защиты (аутентификации, мандатного управления доступом, криптографической защиты и др.), корректность и надёжность функционирования которых будет гарантирована.

В этом смысле мандатный контроль целостности можно считать одним из важнейших механизмов, ориентированных на повышение защищенности современных ОС. Результаты его применения можно сравнить с переходом от часто размытых, администрируемых интуитивно правил дискреционного управления доступом к использованию строгих, имеющих научное обоснование правил мандатного управления доступом.

Вместе с тем целесообразно отметить, что если правила реализации мандатного управления доступом хотя бы в объёме, изложенном в классической модели Белла-ЛаПадулы [6, 2], известны многим разработчикам отечественных защищённых ОС, то в случае с мандатным контролем целостности ситуация обстоит иначе. С одной стороны, мандатный контроль целостности был впервые теоретически описан ещё в 1975 г. в рамках во многом похожей на модель Белла-ЛаПадулы модели Биба [7, 2]. Он с 2007 г. реализуется в механизме *MIC* (*Mandatory Integrity Control*) всех ОС семейства *Microsoft Windows*, где показал свою высокую эффективность при противодействии компьютерным вирусам и атакам, направленным на несанкционированное повышение привилегий. С другой стороны, среди отечественных ОС он практически не применяется. Больше того в новых требованиях безопасности информации к ОС, сформулированных ФСТЭК России в профилях защиты ОС общего назначения (типа «А») [4], на необходимость реализации мандатного контроля целостности явно не указывается.

Можно утверждать, что фактически уникальной отечественной операционной системой, в которой с 2016 г. используется мандатный контроль целостности, является операционная система специального назначения (ОССН) *Astra Linux Special Edition* версии 1.5 [1, 5]. При этом учитывая, во-первых, технические сложности реализации мандатного контроля целостности в ОССН, во-вторых, отсутствие аналогичных решений для других ОС семейства *Linux*, в-третьих, часто неготовность у заказчиков решений на основе ОССН, использующих по существу данный вид управления доступом, мандатный контроль целостности в ОССН до настоящего времени применялся ограниченно. Его активизация требовала выполнения дополнительных действий по конфигурированию ОССН, причём могли быть использованы только два уровня целостности: высокий (доверенный, системный, административный) и низкий (недоверенный, несистемный, пользовательский).

Однако по мере накопления опыта применения мандатного контроля целостности в ОССН стала возможной его полнофункциональная реализация, начиная с версии 1.6, разработка которой будет завершена в ближайшее время. В ней для обеспечения возможности использования мандатного контроля целостности в компьютерных сетях с доменной архитектурой, а также в средствах виртуализации, реализована шкала уровней целостности, имеющая 256 возможных значений. После установки ОССН элементы файловой системы сразу получают требуемые метки целостности, реализованы средства администрирования этих меток целостности, а также уровней целостности учётных записей пользователей. Разработана процедура инициализации меток целостности процессов при штатной загрузке ОССН, при этом традиционно для ОС семейства *Linux* доверенные

процессы (например, от имени суперпользователя) получают по умолчанию низкий уровень целостности и непосредственно не могут нанести ущерб безопасности ОССН.

Понимая несоответствие современным условиям применения защищённых ОС устаревших классических моделей Белла-ЛаПадулы и Биба, научной основой реализации мандатного контроля целостности в ОССН стала имеющая иерархическое представление мандатная сущностно-ролевая ДП-модель безопасности управления доступом и информационными потоками в ОС семейства *Linux* (МРОСЛ ДП-модель) [1-3]. Кроме мандатного контроля целостности эта модель включает мандатное и ролевое управление доступом, описание которых в рамках модели учитывает существенные особенности функционирования как ОССН, так и ОС семейства *Linux* в целом. Модель уже включает все необходимые элементы для использования невырожденной (состоящей из более, чем двух уровней) решётки уровней целостности. При этом в модели строго теоретически сформулированы и обоснованы достаточные условия, выполнение которых гарантирует защиту от возникновения запрещённых информационных потоков (скрытых каналов) по памяти и по времени, а также от несанкционированно захвата недоверенным субъектом (процессом) с низким уровнем уровнем целостности контроля (управления) над доверенным субъектом с высоким уровнем целостности.

Для повышения доверия к МРОСЛ ДП-модели и её реализации в ОССН силами сотрудников ИСП РАН иерархическое представление модели переведено в формализованную нотацию *Event-B* и верифицировано с использованием инструментальных средств дедуктивной верификации платформы *Rodin* [8].

Сложность рассмотренных технологий подтверждает важность подготовки для их применения и развития соответствующих квалифицированных кадров в сферах информационных технологий, системного программирования и, особенно, информационной безопасности. На этом направлении АО «НПО «РусБИТех» в ближайшее время планирует сфокусировать свои усилия, в первую очередь во взаимодействии с образовательными организациями, реализующими программы высшего образования по специальностям и направлениям подготовки 10.00.00 «Информационная безопасность».

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Безопасность операционной системы специального назначения Astra Linux Special Edition. Учебное пособие для вузов / П.В. Буренин, П.Н. Девянин, Е.В. Лебеденко и др.; Под редакцией доктора техн. наук П.Н. Девянина. 2-е издание, стереотипное. М.: Горячая линия – Телеком, 2016. 312 с.
2. *Девянин П.Н.* Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. 2-е изд., испр. и доп. М.: Горячая линия — Телеком, 2013. 338 с.: ил.
3. *Девянин П.Н.* О результатах формирования иерархического представления МРОСЛ ДП-модели // Прикладная дискретная математика. 2016. Приложение № 9. С. 83−87.
4. Документы по сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации. URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/120-normativnye-dokumenty.
5. Операционные системы Astra Linux. URL: http://www.astra-linux.ru/.
6. *Bell D.E., LaPadula L.J.* Secure Computer Systems: Unified Exposition and Multics Interpretation. Bedford, Mass.: MITRE Corp., 1976. MTR-2997 Rev. 1.
7. *Biba K.* Integrity considerations for secure computer systems. MITRE Corp., 1975. MTR-3153.
8. *P.N. Devyanin, V.V. Kuliamin, A.K. Petrenko, A.V. Khoroshilov, I.V. Shchepetkov.* Using Refinement in Formal Development of OS Security Model // In Lecture Notes in Computer Sciences vol. 9609 "Perspectives of System Informatics: 10th International Andrei Ershov Informatics Conference", pp. 107-115. Springer International Publishing, 2016.