ОТЗЫВ

официального оппонента кандидата технических наук, доцента
Коллерова Андрея Сергеевича
на диссертацию и автореферат диссертации Каннер Андрея Михайловича
на тему «Модель и алгоритмы обеспечения безопасности управления доступом в операционных системах семейства Linux», представленные на соискание ученой степени кандидата технических наук по специальности 2.3.6 — Методы и системы защиты информации, информационная безопасность

Актуальность темы диссертационного исследования

В настоящее время безопасность компьютерных систем является одной из наиболее актуальных и важных проблем, которые требуют постоянного внимания и решения. Одним из ключевых аспектов обеспечения безопасности является управление доступом к ресурсам системы.

В операционных системах (далее — ОС) GNU/Linux существует множество правил доступа, которые определяют, какие пользователи имеют право на доступ к файлам и каталогам. Однако, несмотря на то, что эти правила являются достаточно эффективными, они могут быть искажены при проведении компьютерных атак.

Разработка алгоритмов обеспечения безопасности управления доступом, представленная в диссертационном исследовании Каннер Андрея Михайловича, является **актуальной** задачей для организации надежной защиты данных пользователей от несанкционированного доступа (далее — НСД). Такие алгоритмы должны учитывать особенности работы ОС GNU/Linux и обеспечивать высокую степень защиты от возможных атак. Кроме того, разработка таких алгоритмов должна основываться на современных методах анализа и моделирования угроз безопасности информации.

Степень обоснованности научных положений, выводов и рекомендаций

Научные положения диссертационной работы соответствуют основной цели и задачам исследования по разработке алгоритмов обеспечения безопасности управления доступом, исключающих возможность обхода действующих правил доступа в ОС GNU/Linux.

Обоснованность выводов и рекомендаций основывается на доказательном характере их формирования, учете предшествующих достижений и разработок в области защиты данных от НСД, на согласованности и непротиворечивости с имеющимся данными по результатам исследований российских и зарубежных исследователей в сфере компьютерной безопасности сложных информационных систем.

Достоверность и новизна исследования

К основным результатам диссертационного исследования, обладающим **научной новизной**, следует отнести:

– модель безопасности для ОС GNU/Linux, основанную на положениях субъектно-ориентированной модели изолированной программной среды (СО-модели ИПС), которая обеспечивает реализацию заданной политики управления доступом различных пользователей и системных субъектов, а также одновременный контроль непрерывного выполнения функций защиты для всех действующих в системе правил доступа;

– алгоритм обеспечения доверенной загрузки загрузчика и ОС GNU/Linux, использующий процедуры ограничения и контроля загрузчиков, обеспечивающий невозможность нарушения целостности компонентов системы и позволяющий устранить возможность блокировки процесса активации средства разграничения доступа;

– алгоритм встраивания функций защиты от НСД на начальном этапе загрузки ОС GNU/Linux, использующий процедуры обеспечения активации функций безопасности и блокировки их отключения, что исключает нарушение функционирования средства разграничения доступа.

Достоверность полученных результатов обеспечивается корректным использованием теорий моделирования и автоматов, математической логики и теоретических основ компьютерной безопасности, а также положительными результатами использования разработанного средства разграничения доступа в реальных проектах.

Значимость для науки и практики полученных результатов

Теоретическая значимость диссертационного исследования заключается в том, что обоснованы необходимые и достаточные условия достижения безопасного состояния на начальной фазе работы ОС и условия последующего непрерывного выполнения заданных правил доступа, а также в разработке соответствующих им алгоритмов обеспечения безопасности управления доступом.

Практическая значимость результатов диссертации заключается в их реализации в подсистеме управления доступом программно-аппаратного комплекса средства защиты от НСД «Аккорд-X», обладающего сертификатами соответствия требованиям ФСТЭК России и удовлетворяющий требованиям нормативных документов в области защиты информации РФ для 3/5 класса защищенности СВТ и 2/4 уровня контроля отсутствия недекларированных возможностей.

Содержание и завершенность диссертационного исследования

Диссертация состоит из введения, четырех глав, заключения, списка литературы, содержащего 110 наименований, списков сокращений и наименований, иллюстративного материала, четырех приложений. Рукопись имеет общий объем 166 страницы и включает 19 рисунков, 7 таблиц. Порядок изложения материала в рукописи соответствует логике достижения поставленной научной цели.

Во введении обоснована актуальность тематики исследования, сформулированы цели, научная и частные задачи, показаны научная новизна и практическая значимость полученных результатов, представлены основные положения, выносимые на защиту.

В первой главе диссертации представлен анализ состояния предметной области, в том числе: требований нормативно-правовых документов к средствам защиты информации от несанкционированного доступа: средств управления доступом в ОС GNU/Linux и используемых в них механизмов защиты информации; результатов исследований, посвященных совершенствованию алгоритмов разграничения доступом в ОС GNU/Linux. Определена СО-модель ИПС в качестве наиболее соответствующей существующим требованиям.

Вторая глава диссертации посвящена описанию модели безопасности ОС GNU/Linux, в которой исключается возможность обхода действующих правил разграничения доступа системы. Обосновывается использование дополнительных алгоритмов, обеспечивающих активацию и выполнение внедряемых функций безопасности.

В третьей главе приводятся обоснования требований и рекомендаций по практическому использованию предложенных алгоритмов обеспечения безопасности управления доступом в ОС GNU/Linux.

Четвертая глава диссертации посвящена экспериментальному исследованию разработанных алгоритмов обеспечения безопасности и средств разграничения доступа ОС GNU/Linux, для которых приводится верификация на соответствие инвариантам безопасности с использованием темпоральной логики действий Лэмпорта. Отдельные параграфы посвящены анализу опыта апробации и внедрения результатов исследования на различных аппаратных платформах и в операционных системах, отличных от ОС GNU/Linux.

В заключении изложены итоги выполненного исследования, сформулированы основные выводы по диссертационной работе, обозначены направления дальнейших исследований.

В приложениях приводятся перечень объектов контроля целостности ОС GNU/Linux и правил разграничения доступа к ним для создания изолированной программной среды субъектов, листинги разработанной подсистемы

управления доступом к данным и спецификаций для системы ИПС субъектов на языке темпоральной логики действий, документы, подтверждающие внедрение результатов диссертации в практику.

Качество оформления диссертационной работы

Следует отметить соответствие оформления диссертации и автореферата требованиям ГОСТ Р 7.0.11-2011 «Система стандартов по информации, библиотечному и издательскому делу. Диссертация и автореферат диссертации. Структура и правила оформления».

Чтению и восприятию материала диссертации способствует наличие иллюстративного материала (графиков, схем) и таблиц с результатами экспериментов.

Текст, математические формулы, изложение алгоритмов, оформление табличного и иллюстративного материала, за исключением отдельных недочетов, соответствуют требованиям к научным текстам.

Опубликованность основных результатов

Результаты диссертации опубликованы в 24 печатных работах, в том числе 17 — в рецензируемых изданиях.

Полученные соискателем научные результаты прошли апробацию на 13 научно-практических и научно-технических конференциях.

Соответствие автореферата основным идеям и выводам диссертации

Автореферат диссертации **соответствует** требованиям п. 25 «Положения о присуждении учёных степеней», утверждённого постановлением Правительства РФ от 24.09.2013[1] № 842, отражает содержание работы, вклад автора в проведенное исследование, степень новизны и практическую значимость приведенных результатов исследования, содержит основные идеи и выводы диссертации.

Автореферат диссертации является самостоятельным авторским научным трудом Каннер А.М., его содержание соответствует основным положениям выполненного диссертационного исследования.

Отдельные замечания по диссертации

1. Не определены границы исследования, что приводит к необоснованным утверждениям о возможности использования результатов для широкого спектра средств вычислительной техники.

---

[1] С изменениями и дополнениями от:30 июля 2014 г., 21 апреля, 2 августа 2016 г., 29 мая, 28 августа 2017 г., 1 октября 2018 г., 20 марта, 11 сентября 2021 г., 26 сентября 2022 г., 26 января, 18 марта 2023 г.

2. В диссертации анализ предметной области выполнен (представлен) весьма поверхностно. Не учтены положения Государственных стандартов Российской Федерации ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования», ГОСТ Р 59383-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Основы управления доступом», ГОСТ Р 59453.1-2021 «Защита информации. Формальная модель управления доступом» и др. Используются термины и определения не соответствующие стандартам по защите информации.

3. Во второй главе автор описывает новую модель безопасности, основанную на ОС-модели ИПС, при этом вводятся новые сущности. Однако анализ для новой модели скрытых каналов утечки информации не проводится, адекватность модели не оценивается.

4. Представленные в третьей главе требования обоснованы только с позиции работы средства защиты, без учета каналов и видов компьютерных атак.

5. Не обоснован выбор подхода и инструмента для верификации, приведенной в четвертой главе. Метод TLA+ представлен как единственный, при том, что существуют методы: VDM, Z, B, Event-B, Alloy, ASM, PROMELA, сети Петри (которые, в том числе, применялись для верификации существующих на рынке средств доверенной загрузки Dallas Lock и верификации модели Харрисона-Руззо-Ульмана). В тоже время, метод TLA+ чаще используют для верификации параллельных и распределенных систем, что учтено только частично.

6. В текстах диссертации и автореферата имеются неточности, стилистические ошибки, снижающие качество рукописей.

Так, рисунок 4.3 назван «графом», однако подписи вершин и ребер отсутствуют и на рисунке и в тексте описания.

В рукописи используются жаргонизмы (ванильное ядро), разное обозначение одинаковых свойств («право на выполнение» и «право на исполнение»).

В качестве актуальных на сегодняшний день версий ОС Windows указываются в том числе: Windows XP, Server 2003, Vista, Server 2008, 7, Server 2008 R2, … (официальная поддержка которых прекращена).

Выводы

Диссертационная работа **соответствует научной специальности** 2.3.6 «Методы и системы защиты информации, информационная безопасность» (технические науки) по пунктам 2 «Методы, аппаратно-программные средства и организационные меры защиты систем (объектов) формирования и предоставления пользователям информационных ресурсов различного вида», 15 «Принципы и решения (технические, математические, организационные

и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности», 18 «Модели и методы управления информационной безопасностью, непрерывным функционированием и восстановлением систем, противодействия отказам в обслуживании» паспорта научной специальности.

Диссертационная работа Каннер Андрея Михайловича содержит решение актуальной научной задачи, является самостоятельной завершенной научной квалификационной работой, выполненной на актуальную тему. Изложена достаточно грамотным научно-техническим языком, в полной мере отвечает требованиям по актуальности, научной новизне, практической значимости, а также полностью соответствует п. 9 Положения о присуждении ученых степеней в УрФУ. Автор работы, Каннер Андрей Михайлович, заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.6 — Методы и системы защиты информации, информационная безопасность.

Официальный оппонент:
кандидат технических наук, доцент,
военнослужащий в/ч 69617
Тел.: +7-343-375-94-24
e-mail: a.s.kollerov@urfu.ru
Адрес: г. Екатеринбург, Сибирский тракт, 11 км.

Коллеров Андрей Сергеевич

01.09.2023

Подпись Коллерова Андрея Сергеевича заверяю:

Пасько Евгений Алексеевич