Экз. № 1

ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

доктора технических наук, доцента Козачка Александра Васильевича на диссертационную работу Каннера Андрея Михайловича на тему «Модель и алгоритмы обеспечения безопасности управления доступом в операционных системах семейства Linux», представленной на соискание ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Актуальность темы исследования

В настоящее время операционные системы (ОС) GNU/Linux являются наиболее распространенными в среде свободного программного обеспечения. При этом с учетом процессов импортозамещения вопросы защиты конфиденциальной информации и персональных данных, хранящихся в ОС GNU/Linux, приобретают все большую актуальность. Изначально ОС Linux проектировалась без учета необходимости выполнения высоких требований по защите обрабатываемой информации, поэтому механизмы разграничения доступа не являются неотъемлемой частью ядра ОС. Для обеспечения безопасности управления доступом в среде GNU/Linux необходимо обеспечить активацию и непрерывную работу функций защиты, что подразумевает невозможность загрузки ОС с отключенными механизмами защиты информации и невозможность изменения конфигурации этих механизмов на всем протяжении ее функционирования – от загрузки и до завершения работы. Для этого требуется решить актуальную научную задачу по разработке алгоритмов обеспечения безопасности управления доступом в GNU/Linux, что в свою очередь требует учета особенностей реализации механизмов управления доступом при формировании модели безопасности управления доступом.

Диссертационная работа Каннера А.М. имеет целью разработку научно-обоснованных алгоритмов обеспечения безопасности управления доступом, исключающих возможность обхода действующих правил доступа в ОС GNU/Linux.

Научная новизна полученных результатов

К новым научным результатам, полученным единолично автором при выполнении диссертационной работы, следует отнести:

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

алгоритм обеспечения доверенной загрузки загрузчика и ОС GNU/Linux, в котором, в отличие от известных алгоритмов, используются процедуры ограничения и контроля загрузчиков, что, в свою очередь, обеспечивает невозможность нарушения целостности компонент системы и позволяет устранить возможность блокировки процесса активации средства разграничения доступа;

алгоритм встраивания функций защиты от НСД на начальном этапе загрузки ОС GNU/Linux, в котором, в отличие от известных алгоритмов, используются процедуры обеспечения активации функций безопасности и блокировка их отключения, что исключает нарушение функционирования средства разграничения доступа.

Обоснованность и достоверность научных положений, сформулированных в диссертации

Обоснованность и достоверность научных результатов проведенных исследований подтверждается их апробацией на конференциях, публикациях в рецензируемых изданиях, корректностью использования теорий моделирования и автоматов, математической логики и теоретических основ компьютерной безопасности, а также положительными результатами использования разработанного средства разграничения доступа в реальных проектах и

совпадением ожидаемых результатов от использования предложенных алгоритмов обеспечения безопасности с полученными при экспериментальных исследованиях.

Основные научные результаты диссертации опубликованы в 24 печатных работах, из них 17 – в рецензируемых научных изданиях, определенных ВАК РФ и Аттестационным советом УрФУ, получено 1 свидетельство о государственной регистрации программы для ЭВМ.

Теоретическая значимость результатов диссертации

Теоретическая значимость научных результатов исследования заключается в обосновании необходимых и достаточных условий достижения безопасного состояния на начальной фазе работы ОС и условий последующего непрерывного выполнения заданных правил доступа, а также в разработке соответствующих им алгоритмов обеспечения безопасности управления доступом.

Практическая значимость результатов диссертации

Практическая значимость результатов работы заключается в том, что на базе полученных научных результатов обоснованы требования и разработано удовлетворяющее им средство разграничения доступа для ОС GNU/Linux, реализующее предложенные алгоритмы обеспечения безопасности.

Оценивая актуальность и практическую значимость работы Каннера А.М., достаточно отметить, что полученные результаты внедрены в ЗАО «ОКБ САПР», ФАУ «ГНИИИ ПТЗИ ФСТЭК России» и НИЯУ МИФИ.

Оценка содержания диссертации и ее оформления

Диссертационная работа содержит 166 страниц основного текста, 19 рисунков и 7 таблиц, состоит из введения, четырех глав основного материала, заключения, списка сокращений и условных обозначений, списка литературы, списка иллюстративного материала и четырех приложений.

Во введении обосновывается актуальность темы диссертационного исследования, формулируются его цель и задачи, определяются научная новизна, теоретическая значимость и практическая ценность полученных результатов. Дается краткая характеристика положений, выносимых на защиту.

В первой главе проводится анализ существующих средств разграничения доступа для GNU/Linux и применяемых в них способов защиты информации, предъявляемых к ним требований, согласно нормативных документов Российской Федерации, а также результатов известных исследований по совершенствованию способов управления доступом и формальных моделей безопасности в современных ОС.

Вторая глава посвящена формированию модели безопасности ОС GNU/Linux, в которой исключается возможность обхода действующих правил разграничения доступа системы, и обоснованию необходимости использования разрабатываемых алгоритмов, обеспечивающих активацию и выполнение внедряемых функций безопасности.

Третья глава диссертации посвящена рекомендациям по практическому использованию предложенных алгоритмов обеспечения безопасности и модели безопасности в реализующем их средстве разграничения доступа ОС GNU/Linux.

В четвертой главе приводятся результаты экспериментальной апробации разработанных алгоритмов обеспечения безопасности и средства разграничения доступа в ОС GNU/Linux. Подтверждается корректность взаимодействия и сочетания встроенных в ОС средств защиты информации с разработанным средством разграничения доступа и приводятся результаты исследования его влияния на GNU/Linux.

В заключении достаточно кратко и обоснованно сформулированы основные выводы по диссертации, позволяющие четко представить существо проделанной работы.

Текст диссертации изложен логично, написан ясно для понимания, характеризуется внутренним единством, написан математически грамотно. Тема и содержание диссертации отвечают паспорту специальности 2.3.6. Методы

и системы защиты информации, информационная безопасность. Автореферат с достаточной полнотой отражает содержание диссертации.

Замечания и вопросы по работе

В то же время диссертационная работа не лишена некоторых недостатков. К числу наиболее существенных недостатков следует отнести следующие:

1. Предложенные автором рекомендации по практическому использованию разработанных алгоритмов обеспечения безопасности управления доступом сформулированы в отношении ОС GNU/Linux, тогда как теоретические результаты работы из главы 2 являются в достаточной степени универсальными и применимы для широкого спектра программных и аппаратных платформ, в том числе отличных от ОС GNU/Linux.

2. В главе 4 при описании инвариантов безопасности в модели ИПСС недостаточно обоснована их полнота. Возможно, следовало бы в приложениях привести также помимо листинга модели и результаты ее верификации.

3. В ходе экспериментальных исследований разработанной соискателем подсистемы управления доступом положительный эффект от использования предложенных алгоритмов и формальной модели безопасности показан на качественном уровне. Для оценки степени достижения цели исследования следовало бы определить некоторую количественную оценку повышения защищенности данных от несанкционированного доступа при использовании результатов диссертационного исследования.

4. В приложении Б приведены листинги исходных кодов, однако их объем, представляется недостаточным для полного понимания реализации разработанной подсистемы управления доступом.

5. В главе 4 на основе результатов экспериментальных исследований делается вывод об отсутствии существенного влияния внедренных функций защиты на производительность системы. В приведенных диаграммах часть данных с большим значением соответствует лучшему результату, другая часть – худшему, что делает менее наглядным полученные результаты. Возможно,

следовало бы сгруппировать диаграммы в зависимости от подхода к интерпретации результатов.

Отмеченные недостатки свидетельствуют о достаточной сложности тематики, рассмотренной в диссертации, и не снижают значение теоретических результатов, полученных автором, а также их практическую ценность для обеспечения безопасности управления доступом в ОС.

Заключение по работе

Исходя из представленных автореферата и диссертации, можно сделать вывод, что по качеству и объему проведенного исследования диссертационная работа Каннера А.М. представляет собой законченную научно-квалификационную работу, имеет теоретическую и практическую значимость для технической отрасли знаний в области обеспечения безопасности управления доступом операционных систем. Диссертация полностью соответствует пункту 9 Положения о присуждении ученых степеней в УрФУ. Автор диссертации Каннер Андрей Михайлович заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Официальный оппонент:
доктор технических наук, доцент
сотрудник Академии ФСО России

Козачок Александр Васильевич

«25» июля 2023 г.

Федеральное государственное казённое военное образовательное учреждение высшего образования «Академия Федеральной службы охраны Российской Федерации» (Академия ФСО России)
Тел.: +7(4862) 54-99-16
E-mail: a.kozachok@academ.msk.rsnet.ru
Адрес: Россия, 302015, г. Орёл, ул. Приборостроительная, д. 35

Подпись сотрудника Академии ФСО России, доктора технических наук, доцента Козачка Александра Васильевича ЗАВЕРЯЮ.

Руководитель кадрового аппарата Академии ФСО России

А.Б. Семибратов