ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

доктора экономических наук, доктора технических наук, профессора Росса Геннадия Викторовича 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

Операционные системы (ОС) GNU/Linux применяются во многих критически важных информационных системах, в соответствии с чем, актуальным является защита хранящейся и обрабатываемой в них информации, особенно в части препятствия возникновению несанкционированного доступа (НСД). Традиционно для защиты от НСД применяются средства разграничения доступа, которые реализуют одну или несколько политик управления доступом в ОС. В диссертации Каннера А.М. рассматриваются существующие способы и средства разграничения доступа ОС GNU/Linux и показано, что при их применении существует возможность либо отключить функции защиты от НСД на раннем этапе загрузки ОС, либо повлиять на данные функции с дальнейшей возможностью обхода действующих правил управления доступом в системе.

В работе Каннера А.М. рассматривается принципиальная выполнимость внедряемых в систему функций защиты от НСД, в том числе при наличии возможного внутреннего нарушителя, в то время как известные работы в области защиты информации от НСД направлены на улучшение формальных моделей безопасности и совершенствование непосредственно самих способов управления доступом субъектов к объектам. В своей работе автор делает больший акцент не на самом процессе ограничения доступа субъектов, а на обеспечении невозможности совершать доступы в обход действующих правил подсистемы управления доступом.

Таким образом, тема диссертационной работы, является актуальной.

Научная новизна полученных результатов

В диссертационной работе получены следующие новые научно-обоснованные результаты:

1. Предложена научно-обоснованная модель безопасности для ОС GNU/Linux и средства разграничения доступа, обеспечивающая реализацию заданной политики управления доступом различных пользователей и системных субъектов и одновременный контроль непрерывного выполнения функций защиты для всех действующих в системе правил доступа.
2. Предложен 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.
3. Предложен 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

Все выводы и рекомендации работы, как и сформулированные по результатам диссертационного исследования научные положения, достаточно полно обоснованы и подтверждены представленными исследованиями.

Необходимо отметить высокую квалификацию соискателя, которая проявилась в удачном сочетании аппарата системного анализа, теорий моделирования, математической логики, автоматов и множеств. Такой подход предоставил возможность получить новые результаты, связанные с формальной моделью безопасности, гарантирующей невозможность изменения действующих правил управления доступом в системе. Кроме того, соискателем получены положительные результаты применения разработанного средства разграничения доступа в реальных

проектах, что свидетельствует о совпадении ожидаемых результатов от использования предложенных алгоритмов обеспечения безопасности с полученными при экспериментальных исследованиях. Результаты неоднократно докладывались и обсуждались на профильных международных конференциях. Поэтому достоверность результатов сомнений не вызывает.

Основные результаты работы полно и адекватно представлены в 24-х статьях, в том числе 17 из которых – в рецензируемых журналах из списка ВАК РФ.

Практическая значимость результатов диссертации

Практическая значимость результатов диссертации 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. Самостоятельное практическое значение имеют также следующие результаты работы: разработанная модель безопасности может быть использована не только в рамках ОС Linux, но также и для других ОС и систем, в которых реализуется субъектно-объектное взаимодействие; система с внедренным средством разграничения доступа, соответствующая предложенной модели безопасности и реализующая необходимые алгоритмы обеспечения безопасности управления доступом, смоделирована с использованием темпоральной логики действий и верифицирована на соответствие инвариантам безопасности; предложенные алгоритмы обеспечения безопасности и разработанное средство разграничения доступа имеют широкое назначение, могут быть применены не только в отношении GNU/Linux, но и для других ОС, а также на средствах вычислительной техники с архитектурой, отличной от x86_64.

Оценка содержания диссертации и ее оформления

Диссертация состоит из введения, четырех глав основного материала, заключения, списка сокращений и условных обозначений, списка использованных источников, списка иллюстративного материала и четырех приложений.

Во введении диссертант обосновал актуальность темы исследования, сформулировал его цель и задачи, определил научную новизну, теоретическую и

практическую значимость полученных результатов, сформулировал выносимые на защиту научные положения, представил сведения о внедрении и апробации результатов.

В первой главе приведен анализ существующих средств разграничения доступа в ОС GNU/Linux и применяемых в них способов защиты информации, а также анализ предъявляемых требований нормативных документов РФ по защите информации. Диссертантом обосновано, что существующие средства и способы разграничения доступа в ОС GNU/Linux, а также известные исследования по их совершенствованию не учитывают возможность нарушения действующих правил управления доступом или исключения активизации средств защиты от НСД на этапе загрузки ОС. Тем самым существует потенциальная возможность обхода действующей в системе политики безопасности.

Во второй главе автором предложена модель безопасности ОС GNU/Linux, в которой исключается возможность обхода действующих правил разграничения доступа системы. Данная модель позволила разработать необходимые алгоритмы, обеспечивающие активацию и непрерывность выполнения внедряемых функций безопасности – алгоритм обеспечения доверенной загрузки загрузчика и ОС, алгоритм встраивания функций защиты от НСД на раннем этапе загрузки ОС.

В третьей главе формулируются рекомендации по практическому использованию предложенных алгоритмов обеспечения безопасности управления доступом и модели безопасности в реализующем их средстве защиты для ОС GNU/Linux.

В четвертой главе описываются результаты экспериментальной апробации разработанных алгоритмов обеспечения безопасности и средства разграничения доступа в ОС GNU/Linux. Также 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 на основе проведенных исследований сформулированы основные выводы и результаты диссертации. В качестве наиболее важных,

обладающих научной новизной и практической значимостью, следует отметить следующие:

1. Предложенная модель безопасности ОС со средством разграничения доступа позволяет гарантировать в системе выполнение заданной политики безопасности для всех субъектов, объектов и типов доступа.

2. Сформулированные необходимые и достаточные условия достижения безопасного состояния системы в рамках предложенной модели безопасности обеспечивают невозможность нарушения действующей политики управления доступом.

3. Предложенный алгоритм обеспечения доверенной загрузки загрузчика и ОС GNU/Linux при пошаговом контроле целостности, необходимый для достижения начального состояния системы в рамках разработанной модели безопасности, позволяет устранить возможность исключения активации средства разграничения доступа до или на раннем этапе загрузки системы на различных аппаратных платформах.

4. Предложенный алгоритм встраивания функций защиты от НСД на начальном этапе загрузки ОС GNU/Linux позволяет обеспечить в рамках разработанной модели активацию и невозможность отключения функций безопасности, а также принудительную блокировку системы в случае несанкционированного отключения средства разграничения доступа.

5. На базе полученных научных результатов разработано средство разграничения доступа для ОС GNU/Linux, соответствующее предложенной модели безопасности и реализующее алгоритмы обеспечения безопасности.

6. Проведенные экспериментальные исследования подтвердили невозможность отключения или несанкционированного изменения правил доступа и соответствие разработанного средства разграничения доступа предложенной модели безопасности, а также отсутствие существенного негативного влияния внедряемых функций безопасности на характеристики системы.

Автореферат достаточно полно и адекватно отражает суть работы.

Замечания и вопросы по работе

Тем не менее, к тексту диссертации имеется ряд непринципиальных замечаний:

1) В главе 2 недостаточно хорошо демонстрируется насколько точно различные типы запросов в моделируемой системе покрывают все множество возможных операций в различных операционных системах, для которых можно использовать предлагаемую модель безопасности.
2) В главе 2 недостаточно понятно описаны существующие ограничения на применение предложенной модели безопасности на практике. Следовало бы их дополнительно описать после условий следствия о достижения безопасного начального состояния моделируемой системы.
3) В главе 3 описываются компоненты, входящие в состав разработанного комплекса средств защиты информации от НСД «Аккорд-X», при этом отсутствует его визуальное представление. Это не дает полного понимания архитектуры предложенного решения и личного вклада автора.

Перечисленные недостатки не влияют на достоверность работы и не снижают как ценность предоставленных в работе научных результатов, так и положительную оценку диссертации в целом.

Заключение по работе

Диссертация Каннера А.М. представляет собой законченную научно-квалификационную работу, выполненную на высоком научном уровне и удовлетворяющую критериям актуальности, целостности, научной новизны и практической значимости. Сформулированные по результатам исследования научные положения, выводы и рекомендации обоснованы теоретически, основаны на известных положениях теорий моделирования, математической логики, автоматов и множеств, подтверждены проведенными экспериментами. Результаты полно изложены в тексте работы, апробированы на профильных научных конференциях и опубликованы в ведущих научных изданиях по теме диссертации.

Диссертационная работа полностью соответствует п. 9 Положения о присуждении ученых степеней в УрФУ, а ее автор – 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 экономических технических наук, доктор технических наук, профессор,
советник генерального директора,
ООО «Компонент Безопасности»
Тел.: +7 (495) 994-72-60
E-mail: zakaz@kb.com.ru
Адрес: 129085, г. Москва, бульвар Звездный, д.21, стр. 1, эт.4, пом.I, ком.11Д

_____ Росс Геннадий Викторович

«01» 08 2023 г.

Подпись д.э.н., д.т.н. Росса Г.В. заверяю:

Зам. главного инженера _____ М.В. Красовский

«01» августа 2023 г.