Федеральное государственное автономное образовательное учреждение
высшего образования «Уральский федеральный университет имени первого
Президента России Б.Н. Ельцина»

На правах рукописи

Каннер Андрей Михайлович

Модель и алгоритмы обеспечения безопасности управления доступом в операционных системах семейства Linux

2.3.6. Методы и системы защиты информации,
информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Екатеринбург – 2023

Работа выполнена на кафедре №42 «Криптология и кибербезопасность» ФГАОУ ВО «Национальный исследовательский ядерный университет «МИФИ».

Научный руководитель: кандидат технических наук, доцент, **ЕПИШКИНА Анна Васильевна**

Официальные оппоненты:

КОЗАЧОК Александр Васильевич, доктор технических наук, доцент, ФГКВОУ ВО «Академия Федеральной службы охраны Российской Федерации», г. Орёл, сотрудник Академии ФСО России;

РОСС Геннадий Викторович, доктор экономических наук, доктор технических наук, профессор, ООО «Компонент Безопасности», г. Москва, советник генерального директора;

КОЛЛЕРОВ Андрей Сергеевич, кандидат технических наук, доцент, Войсковая часть 69617, г. Екатеринбург, военнослужащий

Защита диссертации состоится «19» сентября 2023 г. в 14:00 часов на заседании диссертационного совета УрФУ 2.3.12.13 по адресу: 620002, г. Екатеринбург, ул. Мира, 19, ауд. И-420 (зал Ученого Совета).

С диссертацией можно ознакомиться в библиотеке и на сайте ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»: https://dissovet2.urfu.ru/mod/data/view.php?d=12&rid=4967

Автореферат разослан «____» _____ 2023 года.

Ученый секретарь диссертационного совета — Сафиуллин Николай Тахирович

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Операционная система (ОС) GNU/Linux является наиболее известным представителем свободного программного обеспечения (ПО). После принятия государственных программ GNU/Linux широко применяется в учебных, государственных и иных учреждениях Российской Федерации – ПФР, ФНС и других. В связи с этим все больше конфиденциальной информации и персональных данных хранится и обрабатывается в среде GNU/Linux, и, значит, возрастает необходимость в обеспечении безопасности таких систем.

Операционные системы общего назначения, которой является GNU/Linux, изначально проектировались без учета необходимости обеспечения защиты данных. Из-за этого средства разграничения доступа не являются неотъемлемой частью ядра Linux – в случае их отключения система будет продолжать функционировать. В соответствии с этим любое средство разграничения доступа GNU/Linux имеет уязвимые периоды: когда ОС уже начала работать, но функции защиты информации еще не активизированы; когда функции защиты активизированы, но были случайно или преднамеренно отключены. Важным преимуществом GNU/Linux перед другими распространенными ОС с этой точки зрения является открытость исходных кодов встроенных средств защиты, что упрощает возможность анализа и исправления их недостатков.

Существуют известные уязвимости компонент ОС, которые позволяют внутреннему нарушителю[1] исключить активацию средств разграничения доступа GNU/Linux и других систем на начальном этапе загрузки средства вычислительной техники (СВТ) еще до запуска их ядра[2]. Также известны уязвимости, позволяющие несанкционированно воздействовать на средство разграничения доступа ОС GNU/Linux с целью изменения порядка его работы или отключения функций защиты информации[3]. Приведенные уязвимости позволяют осуществлять несанкционированный доступ (НСД) к защищаемым данным ОС. При этом главной причиной возникновения этих уязвимостей является то, что встроенные средства разграничения доступа GNU/Linux и ассоциированные с ними объек-

[1] 3й тип (внутренний нарушитель) в соответствии с руководящими документами ФСТЭК.
[2] уязвимости CVE-2009-4128 и CVE-2015-8370.
[3] уязвимости CVE-2018-1063, CVE-2021-23240 и CVE-2021-4034.

ты (списки разрешенных субъектов и их права доступа) не рассматриваются как полноценные объекты системы, которые необходимо защищать как и данные.

В связи с этим для обеспечения безопасности управления доступом в среде GNU/Linux необходимо обеспечивать активацию и непрерывность работы функций защиты, что подразумевает невозможность загрузки ОС без средств защиты информации и невозможность изменения конфигурации этих средств на всем протяжении ее функционирования – от загрузки и до завершения работы.

Кроме того, в ОС GNU/Linux одновременно функционирует сразу несколько встроенных средств разграничения доступа, но внедряемые с помощью них правила не всегда соответствуют формальным моделям безопасности (Харрисона-Руззо-Ульмана, Белла-ЛаПадула и другим), из-за чего нельзя теоретически гарантировать защищенность данных от НСД или выполнение заданной политики управления доступом. Более того, в известных и широко используемых формальных моделях безопасности средство разграничения доступа и связанные с ним объекты не участвуют в моделируемом субъектно-объектном взаимодействии системы. В большинстве моделей безопасности на уровне аксиом подразумевается присутствие средства разграничения доступа и обязательное его участие в любых типах взаимодействия субъектов и объектов доступа, а вопрос безопасности самого этого средства защиты не рассматривается.

Таким образом, в настоящее время существует потребность в использовании GNU/Linux и в защите информации в среде этих ОС, но применения для этого встроенных средств недостаточно для защиты данных от несанкционированного доступа. Более того, устранение перечисленных недостатков для всех существующих встроенных средств разграничения доступа в GNU/Linux – практически нереализуемая задача. В соответствии с этим требуется формирование модели и алгоритмов для обеспечения безопасности управления доступом в среде GNU/Linux, а также их практическая реализация, и тема диссертационной работы является актуальной.

Степень разработанности темы исследования. В разное время ощутимый вклад в развитие теории и практики основ компьютерной безопасности сложных информационных систем (ИС), в том числе в части формальных моделей безопасности, защиты технических, программных и информационных ресурсов внесли такие отечественные и зарубежные ученые, как В. А. Гераси-

менко, В. П. Лось, В. А. Конявский, М. Харрисон (M. Harrison), В. Руззо (W. Ruzzo), Дж. Ульман (J. Ullman), Д. Белл (D. Bell), Л. ЛаПадула (L. LaPadula), Р. Сандху (R. Sandhu), Д. Феррайоло (D. Ferraiolo), Р. Кун (R. Kuhn), Д. Деннинг (D. Denning), Дж. МакЛин (J. McLean), П. Н. Девянин, Д. П. Зегжда и А. Ю. Щербаков. Вопросам возможности применения полученных научных результатов для совершенствования систем управления доступом в существующих реальных компьютерных системах (КС), в том числе в ОС на основе ядра Linux, посвящены труды П. Н. Девянина, Д. П. Зегжды, А. Ю. Щербакова и В. А. Конявского, в которых описаны результаты практического использования моделей безопасности компьютерных систем.

Средства разграничения доступа в ОС должны соответствовать одной или нескольким согласованным формальным моделям безопасности КС, предложенным в работах вышеперечисленных авторов, только в этом случае при применении таких средств можно обеспечить защищенность данных от НСД. Однако даже при использовании известных формальных моделей безопасности не удается устранить все недостатки существующих средств разграничения доступа ОС, в частности в GNU/Linux. Средство разграничения доступа должно активироваться на начальном этапе работы ОС, исключая любую возможность повлиять на процесс своей загрузки и дальнейшего функционирования, для последующего предотвращения НСД к информации. При этом должна также существовать четкая процедура для санкционированного изменения правил управления доступом, препятствующая их модификации недоверенными субъектами доступа – процедура безопасного администрирования. Поэтому формальные модели безопасности должны учитывать вопросы построения и администрирования средств разграничения доступа. Работы А. Ю. Щербакова и В. А. Конявского частично учитывают эту необходимость, однако, использования созданных на основе результатов этих исследований средств доверенной загрузки не всегда достаточно. В исследованиях остальных авторов средство разграничения доступа не является сущностью системы, которую также необходимо защищать. Они направлены на выполнение другой важной задачи – обеспечение безопасности данных за счет принятой политики управления доступом при условии, что все доступы проходят через абстрактное средство разграничения доступа.

С другой стороны, результаты работ указанных авторов являются научно обоснованными и вместе с разработанными моделями безопасности позволяют обеспечить теоретические гарантии защищенности систем, в которых они применяются. В связи с этим целесообразно провести исследование существующих средств разграничения доступа с учетом выделенных аспектов и с использованием результатов известных работ разработать и обосновать корректность новых подходов к защите информации, устраняющих выявленные недостатки таких средств в ОС GNU/Linux. Отсюда вытекает научная задача диссертации, которая заключается в формировании модели и алгоритмов обеспечения безопасности управления доступом, позволяющих в условиях потребности использования ОС GNU/Linux соблюдать установленный порядок предоставления доступа к хранящимся и обрабатываемым данным.

Целью диссертационной работы является разработка научно-обоснованных алгоритмов обеспечения безопасности управления доступом, исключающих возможность обхода действующих правил доступа в ОС GNU/Linux.

Задачи работы. Для достижения поставленной цели в работе решались следующие задачи:

1. Анализ существующих средств разграничения доступа к данным в ОС GNU/Linux и используемых в них способов защиты информации.

2. Разработка научно-обоснованных алгоритмов обеспечения безопасности управления доступом, основанных на использовании модели изолированной программной среды субъектов, исключающей возможность обхода действующих правил управления доступом.

3. Разработка средства разграничения доступа для ОС GNU/Linux, реализующего предложенные алгоритмы и модель безопасности.

4. Апробация и анализ результатов применения разработанных алгоритмов и средства разграничения доступа в ОС GNU/Linux.

Положения, выносимые на защиту. В диссертационной работе получены и выносятся на защиту следующие положения и научные результаты:

1. Стандартные средства разграничения доступа ОС GNU/Linux имеют уязвимые фазы работы на этапе загрузки системы и в процессе ее функционирования, что обеспечивает возможность обхода нарушителем применяемой политики управления доступом.

2. Предложенный алгоритм доверенной загрузки загрузчика и ОС GNU/Linux, устраняет возможность блокировки процесса активации средства разграничения доступа при загрузке системы на различных аппаратных платформах.

3. Предложенный алгоритм встраивания функций защиты от НСД на начальном этапе загрузки ОС GNU/Linux, обеспечивает их активацию и блокирует возможность отключения функций безопасности, а также осуществляет принудительную остановку системы, обусловленную нарушением точек встраивания средства разграничения доступа.

4. Разработанное средство разграничения доступа для ОС GNU/Linux, в котором реализованы предложенные алгоритмы безопасности управления доступом, обеспечивает выполнение заданной политики безопасности на протяжении всего периода работы ОС.

Научная новизна работы. Новизна полученных научных результатов работы заключается в следующем:

– Предложена научно-обоснованная 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 (соответствует п.15 паспорта специальности «Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности»).

– 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 (соответствует п.2 паспорта специальности «Методы, аппаратно-программные средства и организационные меры защиты систем (объектов) фор-

мирования и предоставления пользователям информационных ресурсов различного вида»).

– 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 (соответствует п.18 паспорта специальности «Модели и методы управления информационной безопасностью, непрерывным функционированием и восстановлением систем, противодействия отказам в обслуживании»).

Теоретическая значимость работы. 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 ценность работы. Практическая значимость результатов исследования 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 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 (системы управления базами данных, системы виртуализации, межсетевое взаимодействие и др.).

– 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 автором алгоритмы обеспечения безопасности, а также разработанное средство разграничения доступа имеют широкое назначение,

могут быть применены не только в отношении GNU/Linux, но и для других POSIX/SUS[4]-совместимых ОС, а также на СВТ с архитектурой x86_64, arm64, s390x (мейнфреймы IBM System Z) и других.

Методология и методы исследования. В диссертационной работе используются методы системного анализа, а также теории моделирования, математической логики, автоматов и множеств.

Достоверность научных положений и выводов обеспечена 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 и совпадением ожидаемых результатов от использования предложенных алгоритмов обеспечения безопасности с полученными при экспериментальных исследованиях.

Внедрение результатов работы. Результаты диссертационной работы используются ГНИИ ПТЗИ ФСТЭК России в рамках исследований уязвимостей системного ПО для национального банка данных угроз безопасности информации и для верификации функциональных требований к средствам защиты информации от НСД на раннем этапе загрузки ОС. Также результаты работы применяются ЗАО «ОКБ САПР» в программно-аппаратном комплексе средств защиты информации от НСД «Аккорд-X» (свидетельство о государственной регистрации № 2015612555). Результаты исследования также внедрены в учебный процесс НИЯУ МИФИ по дисциплине «Программно-аппаратные средства защиты информации» (лабораторные работы). Соответствующие документы, подтверждающие практическое использование и внедрение результатов исследования, приведены в приложении к тексту диссертационной работы.

Апробация работы. Основные положения и результаты работы представлялись и обсуждались на следующих конференциях: XVII, XVIII, XIX, XXIII, XXIV, XXV и XXVI Международные конференции «Комплексная защита информации», г. Суздаль (2012, 2018), г. Брест (РБ, 2013), г. Псков (2014), г. Витебск (РБ, 2019), МО (2020), Минск (РБ, 2021); XIII Международная конференция «Информационная безопасность», г. Таганрог (2013); Международ-

[4] **p**ortable **o**perating **s**ystem **i**nterface for Uni**x** (POSIX), **S**ingle **U**nix **S**pecification (SUS) – набор стандартов, описывающих интерфейсы между ОС и прикладным программным обеспечением.

ная конференция «Обеспечение безопасности инфокоммуникационных и цифровых технологий», г. Воронеж (2015 и 2016); VII Международная конференция «Engineering & Telecommunication», г. Долгопрудный (2020); Международная конференция «Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology», г. Екатеринбург (2021 и 2022).

Публикации. Основные результаты по теме диссертации изложены в 24 печатных работах общим объемом 9.52 п.л., в которых автору принадлежит 8.30 п.л. Из них 17 печатных работ изданы в рецензируемых научных изданиях, определенных Высшей аттестационной комиссией при Министерстве науки и высшего образования Российской Федерации и Аттестационным советом УрФУ, в том числе 4 – в журналах, индексируемых международной системой научного цитирования Scopus. Имеется 1 свидетельство о государственной регистрации программы для ЭВМ.

Личный вклад. Содержание диссертации и основные положения, выносимые на защиту, отражают персональный вклад автора в работу. Все основные представленные в диссертации результаты получены автором самостоятельно. В работах, опубликованных в соавторстве, лично автору принадлежат: схема взаимодействия субъектов и объектов в GNU/Linux, способы встраивания средства разграничения доступа в ОС и их практическая реализация; анализ средств разграничения доступа к информации в GNU/Linux и путей их совершенствования, программно-технические решения по созданию средств разграничения доступа; реализация очистки динамически выделяемой памяти в ОС GNU/Linux, оценка ее влияния на производительность системы; результаты тестирования и верификации средств защиты информации.

Структура и объем работы. Диссертационная работа состоит из введения, 4 глав, заключения и 4 приложений. Объем основного текста диссертации составляет 166 страниц(ы) с 19 рисунками и 7 таблицами. Приложение также содержит документы, подтверждающие практическое использование и внедрение результатов диссертационного исследования. Количество наименований в списке литературы — 110.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обосновывается актуальность темы диссертационного исследования, формулируются его цель и задачи, определяются научная новизна, теоретическая и практическая значимость полученных результатов. Рассматриваются положения, выносимые на защиту.

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

В главе обосновано, что существующие средства разграничения доступа в GNU/Linux, а также известные исследования по их совершенствованию не учитывают возможность нарушения действующих правил управления доступом или исключения активации средств защиты от НСД на этапе загрузки ОС. Тем самым существует потенциальная возможность обхода действующей в системе политики безопасности.

Также в главе обоснована актуальность темы диссертационного исследования, сформулирована постановка научной задачи и намечены возможные пути ее решения на основе разработки модели безопасности, а также алгоритмов обеспечения безопасности управления доступом в GNU/Linux.

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

В рамках предлагаемой модели безопасности ОС со средством разграничения доступа введено понятие системы, состоящей из множеств субъектов S и объектов O, представляющей собой детерминированный автомат (V, v_0, Q, f), для которого:

– $V = S_{active} \times O_{func} \times O_{data} \times O_{na}$ – множество состояний системы, где:

$S_{active} \subseteq S$ – множество всех активных субъектов.

$O_{func} \subseteq S_{active} \times O$ – множество объектов, ассоциированных с субъектами функционально (процессы).

$O_{data} \subseteq S_{active} \times O$ – множество объектов, ассоциированных с субъектами как данные.

$O_{na} \subseteq O$ – множество объектов, неассоциированных с субъектами.

– $v_0 \in V$ – начальное состояние системы.

– $Q = S \times O \times E$ – множество входов (запросов, инициируемых субъектами доступа с помощью ассоциированных объектов к сущностям $E = S \cup O$).

– $f : Q \times V \to V$ – функция переходов системы по запросам.

Каждое состояние $v_t \in V$ в момент работы системы $t \in \mathbb{N}_0$ описывается сущностями:

– $S^t_{active} \subseteq S_{active}$, при этом $S^0_{active} = \{s_0, s'_0\}$, где:

s_0 – системный субъект (ядро ОС);

s'_0 – субъект средства разграничения доступа.

– $O^t_{func} \subseteq O_{func}$, при этом $O^0_{func} = \{(s_0, o_0), (s'_0, o'_0)\}$;

– $O^t_{data} \subseteq O_{data}$, при этом $O^0_{data} = \varnothing$;

– $O^t_{na} \subseteq O_{na}$, при этом $O^0_{na} \subseteq O$.

X – множество функций x: $\mathbb{N}_0 \to Q$, задающее все последовательности запросов к системе.

Y – множество функций y: $\mathbb{N}_0 \to V$, задающее все последовательности состояний системы.

Реализацией системы (V, v_0, Q, f) называется пара $(x,y) \in X \times Y$, такая, что: $\forall t \in \mathbb{N}_0$, $f(x(t), y(t)) = y(t+1)$. Все реализации системы (V, v_0, Q, f) описывают любые возможные начальные состояния v_0 в части начального состава множества объектов, последовательности запросов из Q и последовательности состояний из V.

$T = Q \times V \times V$ – множество переходов реализаций, $\forall (q, v_t, v_{t+1}) \in T$: $f(q,v_t) = v_{t+1}$.

В рамках известного подхода безопасности переходов КС для исключения возможности нарушения действующей политики управления доступом вводится определение абсолютной корректности субъектов.

В реализации $(x,y) \in X \times Y$ системы (V, v_0, Q, f) при переходе $(q, v_t, v_{t+1}) \in T$ субъект $s \in S^t_{active}$ абсолютно корректен относительно субъекта $s' \in S^{t+1}_{active}$, $s \neq s'$ в моменты времени работы системы $t \in \mathbb{N}_0$ и $t+1$, если для запроса $q \in Q$ выполняется одно из условий:

– $\forall o, o' \in O$: $q \neq (s,o',o)$ – то есть запрос выполняется без участия s.

– Если для $o, o' \in O$: $q = (s,o',o)$ и $(s,o') \in O^t_{func}$, тогда в постусловии запроса q:

– Либо $o_t = o_{t+1}$ – то есть состояние объекта o не изменилось.

– Либо $o_t \neq o_{t+1}$ и для реализации (x,y): $\nexists\, l > t+1$ и $v_l = y(l)$: $(s',o) \in O^l_{func} \cup O^l_{data}$.

Субъекты $s \neq s'$: $s \in S^t_{active}$ и $s' \in S^{t+1}_{active}$ называются абсолютно корректными в моменты времени $t \in \mathbb{N}_0$ и $t+1$, если s абсолютно корректен относительно s' и s' абсолютно корректен относительно s.

Свойство абсолютной корректности субъектов запрещает выполнять информационный поток (запрос к системе), изменяющий состояние объекта доступа, который в дальнейшем будет являться функционально ассоциированным объектом или объектом-данными другого субъекта доступа. *Смысл свойства абсолютной корректности* применительно к ОС GNU/Linux заключается в том, что объекты-процессы должны выполняться в индивидуальных адресных пространствах и не должно существовать возможности изменения «чужих» ассоциированных объектов-данных. Свойством абсолютной корректности субъектов доступа могут также обладать:

– Переход системы $(q, v_t, v_{t+1}) \in T$, если $\forall s \in S^t_{active}$ и $s' \in S^{t+1}_{active}$, $s \neq s'$ абсолютно корректны в моменты времени $t \in \mathbb{N}_0$ и $t+1$.

– Реализация системы $(x,y) \in X \times Y$, если $\forall t \in \mathbb{N}_0$: $(x(t),y(t),y(t+1))$ обладает свойством абсолютной корректности субъектов доступа.

– Система (V, v_0, Q, f), если $\forall (x,y) \in X \times Y$ обладает свойством абсолютной корректности субъектов доступа. Такая система называется изолированной программной средой субъектов (ИПСС).

Для обоснования невозможности изменения действующих в системе правил доступа доказано следующее утверждение.

Утверждение (*Базовая теорема ИПСС*). *В системе (V, v_0, Q, f) невозможно нарушение действующей политики управления доступом тогда и только тогда, когда она является ИПСС.*

Для обоснования необходимых и достаточных условий достижения безопасного состояния системы, которые в дальнейшем обеспечивали бы невоз-

можность нарушения действующей политики управления доступом, введено следующее определение и доказано следствие из утверждения.

В реализации $(x,y) \in X \times Y$ системы (V, v_0, Q, f) субъект $s \in S^t_{active}$ абсолютно корректен в обратном смысле относительно субъекта $s' \in S^t_{active}$, $s \neq s'$ в момент времени работы системы $t \in \mathbb{N}_0$, если выполняется:

– $\forall o, o' \in O$: $(s',o) \in O^t_{func} \cup O^t_{data}$ в реализации (x,y): $\nexists\, l < t-1$ и состояний $v_l = y(l)$, $v_{l+1} = y(l+1)$, для которых в постусловиях запроса $x(l) = (s,o',o)$: $o_l \neq o_{l+1}$.

Субъекты $s \neq s'$: $s, s' \in S^t_{active}$ называются абсолютно корректными в обратном смысле в момент времени работы системы $t \in \mathbb{N}_0$, если s абсолютно корректен в обратном смысле относительно s' и s' абсолютно корректен в обратном смысле относительно s.

Свойство абсолютной корректности субъектов в обратном смысле запрещает возникновение у субъекта функционально ассоциированных объектов или объектов-данных, которые ранее были изменены другим субъектом доступа. Аналогично предыдущим определениям свойством абсолютной корректности в обратном смысле могут обладать переходы системы.

Следствие (*о достижении безопасного начального состояния*)**.** В системе (V, v_0', Q, f), в которой, в отличие от определения системы (V, v_0, Q, f), начальное состояние имеет вид $v_0' = (\{s_0\}, \{(s_0, o_0)\}, O^0_{data}, O^0_{na}) \in V$ невозможно нарушение действующей политики управления доступом тогда и только тогда, когда $\forall (x,y) \in X \times Y$: $\exists t \in \mathbb{N}$ и выполняются условия:

1. $\forall\, l < t-1$: выполняется $S^l_{active} = \{s_0\}$.
2. $x(t-2) = (s_0, o, s_0')$, в постусловиях которого $s_0' \in S^{t-1}_{active}$, $(s_0',o) \in O^{t-1}_{func}$, и переход $(x(t-2),y(t-2),y(t-1))$ обладает свойством абсолютной корректности субъектов в обратном смысле.
3. $x(t-1) = (s_0', o, o_0')$, в постусловиях которого $(s_0',o_0') \in O^t_{data}$ и переход $(x(t-1),y(t-1),y(t))$ обладает свойством абсолютной корректности субъектов в обратном смысле.
4. $\forall\, l > t$: $(x(l),y(l),y(l+1))$ обладает свойством абсолютной корректности субъектов в обратном смысле.

В случае нарушения условий 1–3 дальнейшая работа КС должна прерываться, то есть последующие запросы не выполняются. В случае нарушения

условия 4 соответствующий запрос $x(l)$ должен блокироваться за счет правил доступа из $o'_0 \in O$: $(s'_0, o'_0) \in O_{data}$ либо работа системы должна прерываться.

В условии 2 выполняется запрос ОС типа $create\_shadow(s_0,o,s'_0)$ – загрузка средства разграничения доступа. В условии 3 выполняется запрос ОС типа $read(s'_0,o,o'_0)$ – чтение/загрузка правил управления доступом.

Требования абсолютной корректности в прямом и обратном смысле не позволяют выполнять в системе следующие административные действия в произвольный момент $t \in \mathbb{N}_0$: для $s \in S^t_{active}$, $o \in O$: $(s,o) \in O^t_{func}$ реализовать запрос типа $write(s,o,o'_0)$. В соответствии с этим в системе должен присутствовать субъект s_{admin} с исключительными правами доступа, способный краткосрочно переводить КС в специальное состояние для администрирования, в котором в момент $l \in \mathbb{N}_0$: $S^l_{active} = \{s_{admin}\}$.

Таким образом, в рамках предложенной модели безопасности обосновано, что при выполнении сформулированных выше условий в системе при любых ее реализациях во все последующие моменты времени гарантируется выполнение заданной политики безопасности. Важным также является, то, что ИПСС является инвариантной относительно действующей в КС политики управления доступом, если ее правила не нарушают положений для ИПСС. Все используемые при формировании данной модели положения в достаточной степени общие, в соответствии с чем, сама модель безопасности имеет широкое назначение и может быть использована как для ОС GNU/Linux, так и для множества других систем. На выполнение условий достижения безопасного начального состояния из следствия направлены предлагаемые алгоритмы обеспечения безопасности управления доступом ОС.

Алгоритм обеспечения доверенной загрузки загрузчика и ОС GNU/Linux при пошаговом контроле целостности позволяет ограничить возможности системных загрузчиков для невозможности несанкционированного изменения сценариев загрузки в динамике, а также контролировать целостность связанных с ними объектов или обеспечивать технологическую невозможность нарушения целостности критически важных компонент системы. Блок-схема данного алгоритма приведена на Рисунке 1. Алгоритм доверенной загрузки загрузчика и ОС GNU/Linux необходим для выполнения условий 1 и частично 2-3 из следствия о достижении безопасного начального состояния КС. В отличие от аналогов,

данный алгоритм позволяет обеспечить не только доверенную загрузку загрузчика GNU/Linux, но и дальнейшую доверенную загрузку самой ОС, а также применим на аппаратных платформах, на которых использование стандартных аппаратных модулей доверенной загрузки невозможно.

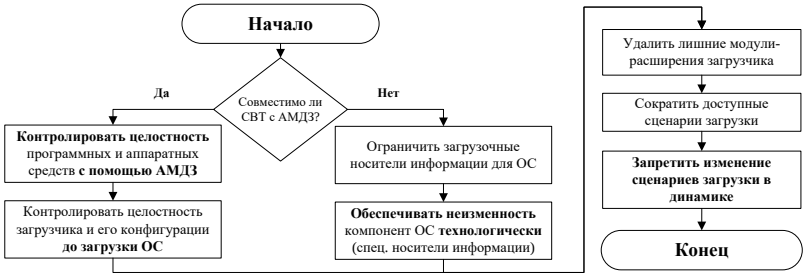

Рисунок 1 – Блок-схема алгоритма доверенной загрузки загрузчика и ОС GNU/Linux

Предложенный алгоритм встраивания функций защиты от НСД заключается во внедрении функций безопасности, начиная с начального этапа загрузки ОС GNU/Linux до возникновения субъектов или защищаемых объектов с обеспечением блокирования дальнейшей загрузки и работы при невозможности активации средства разграничения доступа или нарушении его точек встраивания, а также в контроле любых типов доступа субъектов к объектам и передаче управления стандартным обработчикам системных вызовов для санкционированных попыток доступа. Блок-схема данного алгоритма приведена на Рисунке 2.

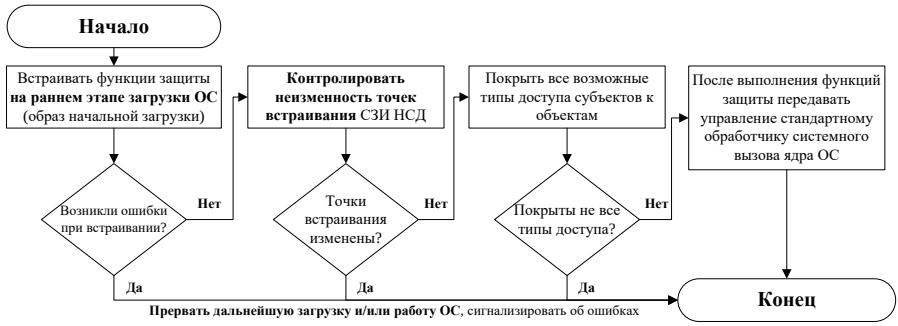

Рисунок 2 – Блок-схема алгоритма встраивания функций защиты от НСД на раннем этапе загрузки ОС

Алгоритм встраивания средства разграничения доступа на раннем этапе загрузки ОС GNU/Linux необходим для обеспечения активизации, целостности и

невозможности отключения функций безопасности средства разграничения доступа с момента его загрузки, а также для обеспечения невозможности работы системы без выполнения операций субъектом s'_0. Таким образом данный алгоритм позволяет выполнить условия 2-4 из следствия о достижении безопасного начального состояния КС.

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

На основе полученных в диссертации результатов сформированы требования, которым должно удовлетворять средство разграничения доступа для ОС GNU/Linux с целью исключения возможности обхода действующих правил доступа. Предложенные требования и сравнение возможности их выполнения существующими средствами разграничения доступа в GNU/Linux приведены в Таблице 1, в соответствии с которой все требования не могут быть выполнены даже при сочетании нескольких таких средств защиты.

Таблица 1 – Сравнение возможностей и характеристик средств защиты GNU/Linux в соответствии с предложенными требованиями к средствам разграничения доступа ОС

Возможности (характеристики) СЗИ НСД	**DAC/ACL CAPS**	**SELinux**	**Tomoyo AppArmor**	**TPM IMA/EVM**	**Secret Net LSP**
1. Корректность встраивания, статическая неизменность ядра ОС		+	+	+	~
2. Гарантия активизации и непрерывности работы	~	–	–	+	~
3. Возможность сочетания с другими средствами защиты	+	~	~	+	+
4. Контроль порождения субъектов	+	+	–		+
5. Гарантия вызова функций защиты для любого типа доступа	+	+	~		+
6. Ограничение всех субъектов системы (пр. наименьших привилегий)	–	+	~		–
7. Независимость от компонент / конфигурации ОС	–	–	+	+	–
8. Возможность безопасного централизованного администрирования	–	~	+		~
9. Выполнение «самозащиты»	–	–	–	+	–
10. Соответствие требованиям по защите информации РФ	–	–	–	–	+

– возможность не реализована / хар-ка отсутствует

~ – возможно при определенных условиях

\+ – возможность реализована / хар-ка присутствует

– не предусмотрено для выполнения

На Рисунке 3 представлено разработанное средство разграничения доступа «Аккорд-X», удовлетворяющее всем сформированным требованиям и соответ-

ствующее предложенной в диссертации модели безопасности. При этом, вследствие реализации в системе свойств абсолютной корректности в прямом или обратном смысле, нарушение правил доступа этого средства защиты информации может вести только к реализации угроз безопасности для данных определенного субъекта доступа, но не к компрометации всей системы в целом.

Рисунок 3 – Состав разработанного комплекса средств защиты информации

В четвертой главе приводятся результаты экспериментальной апробации разработанных алгоритмов обеспечения безопасности и средства разграничения доступа в ОС GNU/Linux. Также в главе 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 ходе экспериментальных исследований подтверждены невозможность отключения или несанкционированного изменения правил разграничения доступа, невозможность возникновения несанкционированных субъектов и неучтенных объектов доступа, достижимость и невозможность «размыкания» ИПСС и другие свойства разработанного средства разграничения доступа.

Для системы, в которой реализованы предложенные алгоритмы обеспечения безопасности и модель ИПСС, проведена верификация на соответствие инвариантам безопасности с использованием темпоральной логики действий Лэмпорта. При этом возможные запросы к системе описываются в виде предикатов с пред- и постусловиями, а свойства безопасности системы модели ИПСС представляются в виде инвариантов и темпоральных свойств. Верификация системы заключается в проверке выполнения инвариантов во всех возможных состоя-

ниях системы, а также в проверке выполнения условий темпоральных свойств в зависимости от времени выполнения и событий в моделируемой системе. В процессе верификации в автоматическом режиме доказана следующая теорема о выполнении свойств безопасности во всех возможных состояниях и реализациях моделируемой системы:

```
THEOREM Spec =>
  \* инвариант контроля типов переменных моделируемой системы
  /\ [] TypeInv
  \* инвариант контроля консистентности множеств сущностей
  /\ [] ConsistencyInv
  \* инвариант контроля незарегистрированных субъектов
  /\ [] BlockedInv
  \* инвариант контроля активизации первого системного субъекта
  /\ [] OSKernelExists
  \* инвариант контроля активизации средства разграничения доступа
  /\ [] SormInits
  \* инвариант проверки свойства корректности субъектов
  /\ [] Correctness
  \* инвариант проверки абсолютной корректности в обратном смысле
  /\ [] AbsCorrectnessOpp
  \* темпоральное свойство для возможности работы пользователей
  /\ OSUsabilityLiveness
  \* темпоральное свойство проверки абсолютной корректности субъектов
  /\ AbsCorrectness
```

Также при экспериментальных исследованиях разработанного средства разграничения доступа проведены нагрузочные тесты с различным сочетанием активных функций защиты, которые выявили накладные расходы в микротестах производительности, не оказывающие значительного влияния на общую работоспособность системы. Сравнительные временные диаграммы некоторых тестов в стационарной фазе работы системы приведены на Рисунке 4.

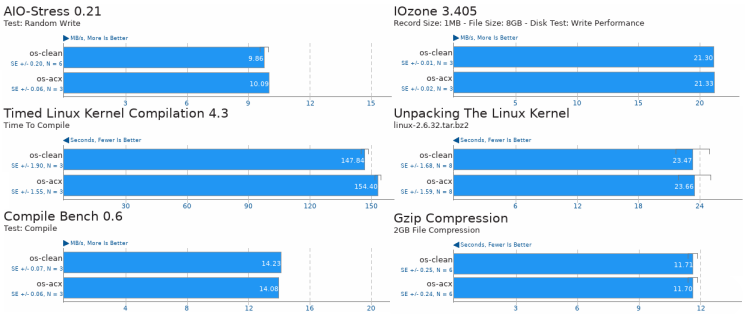

Рисунок 4 – Диаграммы сравнения результатов нагрузочных тестов в ОС GNU/Linux до и после внедрения средства разграничения доступа

Основные положения и результаты работы представлены и обсуждены на 13 международных конференциях, имеются 3 акта об их внедрении.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

1. Проведенный анализ существующих средств разграничения доступа для ОС GNU/Linux и реализованных в них механизмов защиты информации от НСД выявил актуальную задачу формировании модели и алгоритмов обеспечения безопасности управления доступом.

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

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

4. 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.

5. 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.

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

7. 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.

СПИСОК РАБОТ, ОПУБЛИКОВАННЫХ ПО ТЕМЕ ДИССЕРТАЦИИ

Статьи в рецензируемых научных изданиях, определенных ВАК РФ и Аттестационным советом УрФУ:

1. *Kanner, A. M.* Verifying Security Properties of the Source Code of Access Control Tools Using Frama-C / A. M. Kanner, T. M. Kanner // *2022 Ural-Siberian Conference on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT 2022)*. — 2022. — Pp. 255–258. (0.39 п.л. / 0.20 п.л.) (Scopus).
2. *Kanner, A. M.* Special Features of TLA + Temporal Logic of Actions for Verifying Access Control Policies / A. M. Kanner, T. M. Kanner // *2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT 2021)*. — 2021. — Pp. 411–414. (0.53 п.л. / 0.27 п.л.) (Scopus).
3. *Каннер, А. М.* Применение TLA+ нотации для описания модели изолированной программной среды субъектов доступа и ее дальнейшей верификации / А. М. Каннер // *Вопросы защиты информации*. — 2021. — № 3. — С. 8–11. (0.34 п.л.).
4. *Kanner, A. M.* Verification of a Model of the Isolated Program Environment of Subjects Using the Lamport's Temporal Logic of Actions / A. M. Kanner, T. M. Kanner // *2020 International Conference on Engineering and Telecommunication (En&T 2020)*. — 2020. — Pp. 1–5. (0.53 п.л. / 0.29 п.л.) (Scopus).
5. *Каннер, А. М.* Моделирование и верификация подсистемы управления доступом средства защиты информации Аккорд-X / А. М. Каннер, Т. М. Каннер // *Вопросы защиты информации*. — 2020. — № 3. — С. 6–10. (0.34 п.л. / 0.18 п.л.).
6. *Каннер, А. М.* Разграничение доступа в Linux при использовании средства виртуализации kvm / А. М. Каннер // *Вопросы защиты информации*. — 2019. — № 3. — С. 3–7. (0.52 п.л.).
7. *Каннер, А. М.* Различия подходов к пошаговому контролю целостности: TPM и IMA/EVM или ПАК СЗИ НСД / А. М. Каннер // *Вопросы защиты информации*. — 2018. — № 2. — С. 9–13. (0.50 п.л.).

8. *Каннер, А. М.* Требования гарантии выполнения функций защиты встраиваемых средств разграничения доступа к данным в операционных системах / А. М. Каннер // *Вопросы защиты информации*. — 2018. — № 1. — С. 7–12. (0.55 п.л.).
9. *Каннер, А. М.* Исследование применимости подсистемы разграничения доступа в операционных системах Linux / А. М. Каннер // *Информация и безопасность*. — 2017. — Т. 20, № 4. — С. 604–609. (0.30 п.л.).
10. *Каннер, А. М.* Эффективность внедряемых функций защиты от несанкционированного доступа в операционных системах Linux / А. М. Каннер // *Вопросы защиты информации*. — 2017. — № 2. — С. 3–8. (0.41 п.л.).
11. *Kanner, A. M.* Correctness of Data Security Tools for Protection against Unauthorized Access and their Interaction in GNU/Linux / A. M. Kanner // *Global Journal of Pure and Applied Mathematics*. — 2016. — Vol. 12, no. 3. — Pp. 2479–2501. (1.26 п.л.) (Scopus).
12. *Каннер, А. М.* Отличительные особенности программно-аппаратных средств защиты информации от несанкционированного доступа для операционных систем GNU/Linux и Windows / А. М. Каннер // *Информация и безопасность*. — 2015. — Т. 18, № 3. — С. 412–415. (0.29 п.л.).
13. *Каннер, А. М.* Linux: о жизненном цикле процессов и разграничении доступа / А. М. Каннер // *Вопросы защиты информации*. — 2014. — № 4. — С. 37–40. (0.28 п.л.).
14. *Каннер, А. М.* zLinux: разграничение доступа в мейнфреймах / А. М. Каннер // *Безопасность информационных технологий*. — 2014. — № 4. — С. 27–32. (0.41 п.л.).
15. *Каннер, А. М.* Linux: о доверенной загрузке загрузчика ОС / А. М. Каннер // *Безопасность информационных технологий*. — 2013. — № 2. — С. 41–46. (0.39 п.л.).
16. *Каннер, А. М.* Особенности доступа к системным функциям ядра ОС GNU/Linux / А. М. Каннер, В. П. Лось // *Вопросы защиты информации*. — 2012. — № 3. — С. 39–44. (0.44 п.л. / 0.36 п.л.).
17. *Каннер, А. М.* Управление доступом в ОС GNU/Linux / А. М. Каннер, Л. М. Ухлинов // *Вопросы защиты информации*. — 2012. — № 3. — С. 35–38. (0.38 п.л. / 0.30 п.л.).

Свидетельство о регистрации программы:

18. Свидетельство о государственной регистрации программы для ЭВМ. Заявка 2014663519. Российская Федерация. Аккорд-X / Автор Каннер А. М., правообладатель ЗАО «ОКБ САПР». — № 2015612555; заявл. 24.12.2014; опубл. 19.02.2015.

Другие публикации:

19. *Каннер, А. М.* Linux: к вопросу о построении системы защиты на основе абсолютных путей к объектам доступа / А. М. Каннер // *Комплексная защита информации. Материалы XVIII Международной конференции 21-24 мая 2013 года, Брест (РБ)*. — 2013. — № 6. — С. 126–128. (0.27 п.л.).
20. *Каннер, А. М.* Linux: объекты контроля целостности / А. М. Каннер // *Комплексная защита информации. Материалы XVIII Международной конференции 21-24 мая 2013 года, Брест (РБ)*. — 2013. — № 6. — С. 123–126. (0.34 п.л.).
21. *Каннер, А. М.* Особенности реализации механизма очистки освобождаемых областей оперативной памяти в GNU/Linux / А. М. Каннер, В. С. Прокопов // *Комплексная защита информации. Материалы XVIII Международной конференции 21-24 мая 2013 года, Брест (РБ)*. — 2013. — № 6. — С. 120–123. (0.42 п.л. / 0.21 п.л.).
22. *Каннер, А. М.* Идентификация и аутентификация пользователей при работе подсистемы разграничения доступа в ОС Linux / А. М. Каннер // *Безопасность информационных технологий*. — 2012. — № 1кзи. — С. 104–105. (0.15 п.л.).
23. *Каннер, А. М.* Контроль печати в ОС Linux / А. М. Каннер // *Безопасность информационных технологий*. — 2012. — № 1кзи. — С. 106–108. (0.26 п.л.).
24. *Каннер, А. М.* Особенности перехвата системных вызовов при построении подсистемы разграничения доступа в ОС Linux / А. М. Каннер // *Безопасность информационных технологий*. — 2012. — № 1кзи. — С. 109–111. (0.22 п.л.).