ОТЗЫВ

на автореферат диссертации Каннера Андрея Михайловича на тему «Модель и алгоритмы обеспечения безопасности управления доступом в операционных системах семейства Linux», представленной на соискание учёной степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность

Вопросы обеспечения безопасности систем и решений, построенных на базе операционных систем (ОС) GNU/Linux, на сегодняшний день стоят наиболее остро в связи с уходом западных производителей ОС с российского рынка. При этом использования встроенных механизмов безопасности недостаточно для защиты конфиденциальных и чувствительных данных от несанкционированного доступа (НСД), поскольку, в силу специфики проектирования ОС GNU/Linux, средства разграничения доступа не являются неотъемлемой частью ядра Linux. Это делает их потенциально уязвимым объектом для нарушителя и существенно повышает риски информационной безопасности для всей системы. В таких условиях актуальным направлением является создание моделей обеспечения безопасности управления доступом для ОС семейства Linux и разработка программных решений на их основе. В связи с этим, тема диссертации Каннера А.М. является актуальной, поскольку в ней автор предлагает решение вышеописанных проблем за счет формирования научно-обоснованной модели и основанных на ней алгоритмов для обеспечения безопасности управления доступом в ОС GNU/Linux.

Каннером А.М. получены следующие научные результаты:

1. Предложена научно-обоснованная модель безопасности для ОС GNU/Linux и средства разграничения доступа, обеспечивающая реализацию заданной политики управления доступом в отношении различных пользователей и системных субъектов.

2. Разработан алгоритм доверенной загрузки загрузчика и ОС GNU/Linux, обеспечивающий невозможность нарушения целостности компонент системы и позволяющий устранить возможность блокировки процесса активации средства разграничения доступа.

3. Разработан алгоритм встраивания функций защиты от НСД на раннем этапе загрузки ОС GNU/Linux, использующий процедуры по обеспечению активации функций безопасности и блокировки их отключения, что исключает возможность нарушения функционирования средства разграничения доступа во время работы системы.

На основании полученных научных результатов разработано средство разграничения доступа для GNU/Linux, реализующее предложенные алгоритмы обеспечения безопасности на практике и соответствующее сформированной в диссертации модели безопасности.

Необходимо отдельно отметить, что разработанное автором средство разграничения доступа входит в состав разрабатываемого компанией ЗАО «ОКБ САПР» и поставляемого в другие организации программно-аппаратного комплекса СЗИ от НСД «Аккорд-Х». Результаты диссертационной работы также применяются в ФАУ «ГНИИИ 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, и используются в учебном процессе кафедры «Криптология и кибербезопасность» НИЯУ МИФИ в рамках дисциплины «Программно-аппаратные средства защиты информации».

Автореферат написан грамотным языком, имеет логичную и четкую структуру, достаточно подробно и наглядно отражает суть исследования и полученные автором результаты.

Однако имеются следующие замечания:

1. Рисунки, приведенные в автореферате, и их шрифт имеют маленький размер, что затрудняет восприятие представленной на них информации.

2. Следовало бы обосновать выбор темпоральной логики действий Лэмпорта для верификации модели.

3. В автореферате достаточно большое количество аббревиатур, расшифровываемых при первом употреблении. Наличие списка используемых сокращений упростило бы восприятие теста автореферата.

Указанные замечания не снижают научной и практической ценности результатов диссертационной работы и значимости положений, выносимых на защиту.

Считаю, что представленные в автореферате результаты диссертационного исследования полностью раскрывают положения, выносимые на защиту. Диссертационная работа является законченной научно-квалификационной работой и соответствует п. 9 Положения о присуждении ученых степеней в УрФУ, а ее автор, Каннер Андрей Михайлович, заслуживает присуждения степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Лаврова Дарья Сергеевна
доктор технических наук, доцент,
профессор Института кибербезопасности и защиты информации,
Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский политехнический университет Петра Великого»
E-mail: lavrova@ibks.spbstu.ru
Тел.: +7 (812) 552-76-32
Адрес: 195251, г. Санкт-Петербург, ул. Политехническая, д. 29, ауд. 172

10.08.2023
(подпись) (дата)

Подпись д.т.н., профессора Лавровой Д.С. заверяю:

_____ _____
(подпись) (дата)

Подпись Лавровой Д.С.
УДОСТОВЕРЯЮ
ведущий специалист
по кадрам
«10» 08 2023 г.