**ОТЗЫВ**

официального оппонента на диссертационную работу
**Андрианова Павла Сергеевича** на тему
«Анализ корректности синхронизации компонентов ядра операционных систем», представленную на соискание ученой степени кандидата физико-математических наук по специальности 05.13.11 Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей.

Диссертация П.С. Андрианова посвящена **важной и актуальной** теме – верификации программ и программных систем. Важность данного направления обусловлена, прежде всего, необходимостью обеспечения надежности и эффективности компьютерных программ и систем. Особое место среди таких проблем занимают задачи, связанные с проверкой корректности синхронизации компонентов ядра операционных систем (ОС).

В работе решается задача поиска ошибок, связанных с некорректной синхронизацией компонентов ядра ОС, таких, как состояния гонки по данным (англ. data race). Состояние гонки может приводить к недетерминированному поведению программы, что становится особенно критично для ядра ОС.

Проявление ошибок, связанных с некорректной синхронизацией, возможно только в многопоточном исполнении, что серьезно затрудняет их поиск и исправление. Для компонентов ядра ОС задача осложняется большим объемом исходного кода и его спецификой. В связи с этим диссертанту приходится решать задачу анализа корректности синхронизации с учетом требования эффективности. Для решения этой задачи используется подход с раздельным рассмотрением потоков (англ. thread-modular analysis).

Диссертационная работа состоит из введения, четырех глав, заключения, списка литературы и двух приложений.

**Во введении** автор обосновывает актуальность исследования, формулирует цель диссертации, характеризует ее научную новизну и практическую ценность.

**Первая глава** диссертации представляет собой обзор работ в области верификации многопоточного программного обеспечения. Автор рассматривает три основные группы методов анализа программ: динамические методы, методы статического анализа и методы статической верификации.

Во **второй главе** описывается метод верификации многопоточной программы с раздельным рассмотрением потоков. В этой главе описывается формальная модель программы, затем описывается адаптивный статический анализ (англ. Configurable Program Analysis, CPA) с абстрактными переходами. Отметим, что абстрактные переходы являются расширением классического варианта теории для возможности выражения подхода с раздельным рассмотрением потоков. После этого формулируется основная теорема о корректности (англ. soundness) подхода. Далее приводятся описания различных способов анализа и доказывается, что они удовлетворяют условиям теоремы.

**Третья глава** посвящена описанию реализации метода поиска состояний гонки. В ней приведено устройство инфраструктуры CPAchecker и даны детали реализации каждого из применяемых CPA-анализаторов. Также в этой главе описаны технические оптимизации, позволяющие повысить эффективность анализа.

В **четвертой главе** приведены результаты экспериментальной оценки разработанного инструмента. Инструмент может использовать различные CPA-анализаторы, каждый из которых имеет свои режимы работы. Кроме того, различные варианты работы инструмента могут быть эффективнее для

того или иного целевого кода, поэтому сравнение проводилось на нескольких наборах задач: небольших рукописных тестах, драйверах ОС Linux и ядрах ОС реального времени. Далее был проведен анализ причин ложных срабатываний и анализ причин пропуска ошибок на основе существующих исправлений.

В **заключении** перечислены основные результаты диссертации.

В **приложении А** приведены доказательства теоремы и утверждений главы 2.

В **приложении Б** приведено описание изменений, содержащих исправления ошибок, связанных с состоянием гонки.

Список литературы содержит 100 ссылок.

Отметим основные **новые** научные результаты, полученные в диссертации:

1. Разработан метод поиска состояний гонки на основе раздельного анализа потоков, использующий средства абстракции состояний и переходов для управления точностью и ресурсоемкостью верификации.
2. Разработан алгоритм построения окружения потока, который позволяет гибко настраивать уровень абстракции над взаимодействием потоков, и доказана его корректность.
3. Разработан новый алгоритм, который является обобщением существующего алгоритма статической верификации программ при помощи метода CPA, расширяющий типовой набор CPA-анализаторов средствами верификации многопоточных программ с раздельным анализом потоков, и доказана его корректность.

Таким образом, в диссертационной работе П.С. Андрианова разработан новый метод верификации многопоточного программного обеспечения. Выполненное исследование является важным вкладом в развитие теории и практики верификации программных систем.

По тексту работы имеются следующие **замечания**.

1. В постановке задачи фигурирует нестрогая формулировка «приемлемый уровень ложных предупреждений», в главе 4 отсутствует обоснование достижения такого уровня.
2. Неудачна формулировка результатов диссертационной работы - выпала практическая составляющая, имеющаяся в работе.
3. В реализации ThreadModularCPA (раздел 3.3) применена небезопасная оптимизация.
4. Автор использует сленг разработчиков (патчи - правки, коммиты - изменения), что негативно сказывается на восприятии текста научной работы.
5. Приложение 2 не несет полезной информационной нагрузки, поскольку приведенные детальные описания изменений предполагают хорошее знакомство читателя с исходными кодами, о которых идет речь. Вполне достаточно краткого описания, сделанного в разделе 4.7.
6. В работе смешиваются понятия «дуга» и «ребро» графа потока управления. Термин «ребро» встречается на с. 40 и 117. Правильнее говорить о дугах, поскольку рассматривается ориентированный граф.
7. Под определение состояния гонки (с. 46, определение 1) не подпадают высокоуровневые гонки. Остается неясной возможность выявления этого класса ошибок.

Сделанные замечания не влияют на общую положительную оценку работы.

Таким образом диссертация Андрианова П.С. «Анализ корректности синхронизации компонентов ядра операционных систем» представляет собой законченную научно-исследовательскую работу. Положения и выводы, сформулированные в диссертации, обоснованы и достоверны. Теоретические результаты сопровождаются математическими доказательствами. Результаты диссертационной работы являются новыми, представляют значительный

научный интерес, подтверждаются экспериментальными данными. Опубликованные работы и автореферат достаточно полно и правильно отражают основное содержание диссертации.

Представленная диссертационная работа соответствует требованиям, предъявляемым Положением о порядке присуждения ученых степеней к кандидатским диссертациям, соответствует профилю специальности 05.13.11 «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей», а ее автор заслуживает присуждения ему ученой степени кандидата физико-математических наук по указанной специальности.

Доктор физико-математических наук, заведующий
сектором Федерального государственного
учреждения «Федеральный научный центр Научно-
исследовательский институт системных
исследований Российской академии наук»

Галатенко Владимир Антонович

«15» апреля 2021 г.