

Министерство образования и науки Российской Федерации  
Московский физико-технический институт (государственный  
университет)

Физтех-школа радиотехники и компьютерных технологий  
Кафедра системного программирования ИСП РАН  
Лаборатория (laboratory name)

Выпускная квалификационная работа бакалавра

Система автоматизированного тестирования файловой  
системы JFFS2

**Автор:**

Студент Б01-009 группы  
Дементьев Даниил Викторович

**Научный руководитель:**

Мутилин Вадим Сергеевич

**Научный консультант:**

Хорошилов Алексей Владимирович



Москва 2024

**Аннотация**

Автоматизированная система тестирования файловой системы  
JFFS2

*Дементьев Даниил Викторович*

**Abstract**

Automative JFFS2 filesystem testing suite.

## Содержание

<b>1</b>	<b>Введение</b>	<b>4</b>
1.1	Файловая система . . . . .	4
1.2	Устройства долговременного хранения информации . . . . .	4
1.3	Взаимодействие ФС с флэш-памятью . . . . .	5
1.4	Устройств на основе технологии памяти MTD . . . . .	6
1.5	Файловая система JFFS2 . . . . .	6
1.6	Тестирования файловых систем . . . . .	6
<b>2</b>	<b>Постановка задачи</b>	<b>8</b>
<b>3</b>	<b>Обзор существующих решений</b>	<b>9</b>
3.1	Xfstests . . . . .	9
3.2	Fsfuzz . . . . .	9
3.3	Syzkaller . . . . .	9
3.4	Тесты из пакета инструментов MTD . . . . .	10
<b>4</b>	<b>Исследование и построение решения задачи</b>	<b>11</b>
4.1	Тестовое покрытие . . . . .	11
4.2	Расширение тестового покрытия ФС . . . . .	11
4.3	Функционал JFFS2 . . . . .	11
4.4	Окружение файловой системы . . . . .	13
4.5	Создание системы автоматизированного тестирования . . . . .	14
<b>5</b>	<b>Описание практической части</b>	<b>15</b>
5.1	Использованные инструменты . . . . .	15
5.2	Тестирование с использованием готовых решений . . . . .	17
5.3	Результаты первого эксперимента . . . . .	17
5.4	Расширение тестового покрытия . . . . .	18
5.5	Расширенное тестовое покрытие . . . . .	18
5.6	Фаззинг-тестирование . . . . .	19
5.7	Тестирование с использованием симуляции сбоя . . . . .	20
5.8	Анализ непокрытого кода . . . . .	20
<b>6</b>	<b>Заключение</b>	<b>21</b>

## 1 Введение

В данной главе вводятся основные понятия, необходимые для постановки задачи.

### 1.1 Файловая система

Одна из основных функций операционной системы (ОС) - управление устройствами долговременного хранения информации и предоставление пользовательским приложениям интерфейса для взаимодействия с ними с целью хранения и организации доступа к данным. Элемент операционной системы, отвечающий за эти функции - **файловая система** (ФС).

Для интеграции ряда файловых систем в единую структуру с пользовательской точки зрения в ядре ОС Linux используется концепция виртуальной файловой системы, позволяющая обращаться к различным файловым системам используя единый интерфейс системных вызовов. Для оптимизации своей работы ФС использует множество внутренних структур данных. Для хранения метаданных пользовательских файлов и каталогов ФС использует структуру данных называемую **индексным дескриптором**. Также для хранения информации о свободном пространстве на устройстве файловые системы используют особые структуры данных, например битовую карту данных или список свободных блоков устройства. Для оптимизации процесса монтирования вся информация о файловой системе необходимая ОС в процессе монтирования хранится в структуре называемой **суперблоком**.

### 1.2 Устройства долговременного хранения информации

Большинство файловых систем ядра Linux были разработаны для взаимодействия с накопителями на жестком магнитном диске, особенности строения которых формировали алгоритмы хранения данных, используемые файловыми системами. Подобные устройства хранения состоят из вращающегося диска с магнитными дорожками и считывающей головки, способной перемещаться между дорожками. Из-за подобного строения доступ к произвольному блоку данных на жестком диске имел задержку позиционирования считывающей головки над нужной дорожкой и задержку вращения диска, обусловленную скоростью вращения магнитного диска. Для оптимизации задержки вращения в файловых системах использовались различные алгоритмы размещения данных на диске, например раз-

мещение файлов из одного каталога и их индексных дескрипторов поблизости.

С развитием технологий на рынке устройств долговременного хранения информации начали появляться аналоги жестким дискам в виде **устройств флэш-памяти**. Устройства флэш-памяти состоят из транзисторов, за счет чего скорость доступа к произвольному блоку имеет тот же порядок, что и скорость последовательного доступа к данным. Ячейки флэш-памяти организованы в так называемые **стираемые блоки**, которые обычно имеют размер 128 килобайт. Интерфейс взаимодействия с устройствами флэш-памяти отличается от интерфейса жесткого диска и составляет три основные команды: чтение данных из блока, стирание всего блока, то есть установка всех его бит в единицу и программирование памяти, то есть замена части единичных бит на нули для записи нужных данных, что может быть осуществлено после стирания блока.

Главная проблема флэш-памяти - износ. В процессе стирания и перезаписи блока на транзисторах накапливается избыточный заряд, из-за чего становится невозможно определить значение на транзисторе и блок становится непригодным к использованию. Время жизни блоков флэш-памяти измеряется в циклах стирания и имеет значение порядка 100000 циклов. Для предотвращения излишнего использования определенных блоков и продления срока службы всей микросхемы, используется технология **выравнивания износа** блоков, что означает равномерное использование всех блоков.

### 1.3 Взаимодействие ФС с флэш-памятью

Для эффективного использования флэш-памяти в качестве запоминающего устройства необходимо разрешить несколько основных проблем: выравнивание износа, обеспечение надежности в случае отключения питания, сборка мусора и необходимость программной обработки дефектных блоков. Эти проблемы решаются **уровнем флэш-преобразования (FTL)**.

Уровень флэш-преобразования может быть размещен в контроллере устройства памяти, в драйвере устройства или в файловой системе, как это реализовано в JFFS2 и других ФС, взаимодействующих с неуправляемой флэш-памятью, например UBIFS и YAFFS2.

## 1.4 Устройств на основе технологии памяти MTD

Для доступа к неуправляемой, то есть не имеющей контроллера выполняющего функции FTL, флэш-памяти в ядре Linux используется система устройств на основе **технологии памяти** (MTD - Memory Technology Device), предоставляющая базовые интерфейсы для взаимодействия с устройствами, а также обработки и идентификации дефектных блоков. Подсистема MTD состоит из трех уровней: основной набор функций, драйверы микросхем флэш-памяти и драйверы пользовательского уровня, предоставляющие пользователю интерфейс символьного и блочного устройства для взаимодействия с флэш-памятью.

## 1.5 Файловая система JFFS2

Файловая система JFFS2 (Journaling Flash Filesystem 2) была разработана для использования неуправляемых микросхем флэш-памяти в качестве запоминающего устройства и поддерживает устройства как NOR, так и NAND типа. JFFS2 является исторически первой файловой системой Linux для флэш-накопителей, но используется до сих пор. Она имеет журнальную структуру и использует подсистему устройств технологий памяти MTD для доступа к флэш-памяти.

Для того, чтобы избежать чтения всего журнала для вычисления структуры каталогов на этапе монтирования, JFFS2 использует сводные узлы (summary node). Сводный узел записывается в конец открытого стираемого блока и содержит в себе всю информацию, необходимую на этапе монтирования. Такой подход позволяет уменьшить время монтирования ценой небольшого перерасхода объема используемой памяти. Этот режим включается при установке определенного конфигурационного параметра ядра.

С целью различить является ли стираемый блок, в котором все биты установлены в 1 стертым, или он хранит полезную информацию, состоящую из всех единичных бит, JFFS2 использует маркеры очистки (clean marker), записываемые в начале блока. Если маркер очистки присутствует в блоке, значит блок очищен.

## 1.6 Тестирования файловых систем

Обеспечение надежности и отказоустойчивости модулей ядра, и файловой системы в частности - важная и непростая задача. Наличие ошибок в исходном коде ФС может привести к нарушениям в основных функциях

файловой системы, получению пользователем несанкционированного доступа к привелигированному режиму ядра, а также полному краху или блокировке системы. Подобные последствия ошибок на серверах и суперкомпьютерах могут привести к потерям значимых данных или несанкционированному доступу к ним.

Большинство веб-серверов и суперкомпьютеров используют операционные системы на основе ядра Linux, имеющего открытый исходный код. В ядре Linux имеется множество файловых систем, разработанных для различных типов устройств хранения информации и использующие различные алгоритмы расположения данных на устройстве.

Решением для проверки корректности функционирования операционных систем и их модулей является создание систем автоматизированного тестирования.

Важнейшей метрикой, характеризующей качество подобных систем тестирования является тестовое покрытие кода. Полнота тестового покрытия кода является предметом для множества исследований, в том числе в области тестирования файловых систем. Данная работа посвящена созданию системы автоматизированного тестирования файловой системы JFFS2 и исследованию достигаемого тестового покрытия исходного кода этой файловой системы.

## 2 Постановка задачи

Целью данной работы является разработка системы автоматизированного тестирования файловой системы JFFS2.

Для достижения данной цели были поставлены следующие задачи:

- Изучить особенности внутреннего устройства файловой системы JFFS2.
- Исследовать существующие решения тестирования файловых систем и модулей ядра Linux.
- Расширить тестовое покрытие кода, достигаемое существующими решениями.
- Разработать тесты, соответствующие особенностям JFFS2.

Актуальность данной работы обусловлена тем, что инструменты тестирования ядра Linux в лаборатории Linux Verification Center часто обнаруживают в исходном коде JFFS2 ошибки, требующие исправлений. Для проверки корректности внесенных исправлений требуется система тестирования, специализированная под особенности этой ФС и покрывающая своими тестами основной функционал.

JFFS2 в данный момент не имеет тестовых наборов, специализированных под ее архитектурные особенности ввиду небольшой популярности. Однако эта ФС до сих пор используется на множестве устройств.



### 3 Обзор существующих решений

Для большинства файловых систем ядра Linux сообществом были разработаны тестовые наборы, фреймворки стресс-тестирования и инструменты фаззинг-тестирования. В данной главе будут описаны наиболее популярные и подходящие к тестированию JFFS2 решения.

#### 3.1 Xfstests

**Xfstests** - набор регрессионных тестов, изначально разработанный под файловую систему xfs, но в данный момент поддерживает множество других файловых систем ядра Linux, среди которых btrfs, reiserfs, f2fs и другие. Этот набор представляет собой множество bash-скриптов, разделенных по каталогам на группы. Среди тестов имеются как нацеленные на тестирование общих для всех ФС функций, так и предназначенные для определенных систем. На данный момент xfstests является наиболее популярным и широко используемым решением для тестирования файловых систем.

#### 3.2 Fsfuzz

**Fsfuzz** - это инструмент фаззинг-тестирования ФС, представляющий собой bash-скрипт, суть работы которого заключается в генерации множества случайных образов выбранной файловой системы и дальнейшего монтирования этих образов. Подобный метод перебора не покрывает все основные функции файловой системы, однако может привести к редким сценариям обработчика ошибок, что полезно, так как подобные редкие сценарии сложно покрыть обычными тестовыми наборами.

#### 3.3 Syzkaller

**Syzkaller** - наиболее популярный инструмент динамического анализа кода ядра ОС. Суть его работы заключается в конструировании случайных программ на основе системных вызовов, запуске их на тестируемой системе и получении обратной связи в виде покрытия кода ядра. Случайные программы конструируются с использованием различных системных вызовов в различном порядке и со случайно подобранными аргументами с целью расширения покрытия кода. При достижении ошибок syzkaller генерирует программы репродьюсеры на языке Си, повторяющие сценарий достижения ошибки.

В файле конфигурации `syzkaller` можно определить список разрешенных к использованию системных вызовов, таким образом ограничить его покрытие, но нацелить на определенные сценарии с выбранными системными вызовами. При должной конфигурации `syzkaller` может быть использован для тестирования определенного модуля ядра, в том числе и ФС.

### 3.4 Тесты из пакета инструментов MTD

Пакет **`mtd-utils`** содержит множество инструментов для работы с устройствами флэш-памяти, в том числе и инструмент создания образа файловой системы JFFS2. Разработчиками этого пакета инструментов были добавлены тесты для файловых систем флэш-памяти в виде четырех `bash`-скриптов.

Эти тесты должны хорошо покрывать функции, отвечающие особенностям файловой системы JFFS2, однако такого небольшого числа скриптов недостаточно для покрытия всех основных функций ФС.

## 4 Исследование и построение решения задачи

В данной главе будут подробно рассмотрены идеи, разработанные в ходе исследования и построения решения задачи. Реализации данных идей подробно описывается в следующей главе.

### 4.1 Тестовое покрытие

**Тестовое покрытие** является основной метрикой, характеризующей качество системы тестирования любой программы. Однако функционал модулей ядра операционной системы, и ФС в частности, во многом зависит от конфигурации окружения в котором она работает. То есть для получения полной информации о покрытии достигаемом при помощи тестового набора необходимо провести несколько экспериментов в различном окружении.

### 4.2 Расширение тестового покрытия ФС

Для расширения тестового покрытия исходного кода ФС, достигаемого при помощи тестового набора необходимо провести анализ основных функций тестируемой ФС и параметров конфигурации ее окружения, от которых зависит ее функционал.

### 4.3 Функционал JFFS2

Основные функции файловой системы JFFS2 можно разделить на несколько групп по их предназначению:

1. **Основные операции с файлами** К этой группе относятся функции, отвечающие за основной функционал операций с файлами и каталогами и внутренними структурами ФС. Этот базовый функционал является общим для всех ФС. К таким операциям относятся например чтение и запись данных в файл, создание и удаление файла или каталога и соответствующих им индексных дескрипторов, установка расширенных атрибутов файлов. Функции этой группы могут быть покрыты тестовыми наборами других ФС, так как являются частью общего для всей файловых систем функционала.
2. **Функции контроля доступа** К этой группе относятся функции, отвечающие за контроль доступа к пользовательским данным и операции

- с внутренними структурами, отвечающими за это, например списком контроля доступа.
3. **Функции взаимодействия с устройствами хранения** К этой группе относятся функции, определяющие тип устройства хранения с которым работает ФС и работающие с его блоками, например обеспечивающие выравнивание износа стираемых блоков.
  4. **Сборщик мусора** К этой группе относятся функции, обеспечивающие работу алгоритма сборщика мусора JFFS2. Этот алгоритм является специфичным для этой ФС и его функции могут не покрываться при стандартных сценариях.
  5. **Алгоритмы сжатия данных** В JFFS2 есть 4 различных алгоритма сжатия данных, состоящих из множества внутренних функций. Помимо функционала самих алгоритмов, в коде присутствуют функции, отвечающие за стратегию выбора алгоритма сжатия. Например выбор может производиться по приоритету, размеру сжатых данных или вынуждая ФС в любом случае использовать один алгоритм.
  6. **Обработчик ошибок** К этой группе относятся функции обрабатывающие ошибки и редко достигаемые в обычных сценариях работы ФС. Эти ошибки могут быть связаны с некорректным выделением памяти, несоответствием важных параметров образа и устройства, используемого для его подключения или невалидностью данных, по причине наличия ошибок во внутренней логике самой файловой системы. Функции этой группы лучше всего покрываются при помощи фаззинг-тестирования либо методом **внедрения неисправностей** (fault injection).
  7. **Обработка входных параметров команд** К этой группе относятся функции, обрабатывающие суперблок ФС и входные параметры при выполнении команды монтирования. Эти функции являются частью основного функционала любой ФС, однако могут быть выделены в отдельную группу, так как лучше покрываются не обычными тестовыми сценариями, а фаззинг-тестированием ввиду большой вариативности возможных входных параметров и образа ФС.
  8. **Функции работы с внутренними структурами** К этой группе относятся функции работающие со внутренними структурами, особенными для исследуемой ФС. Для JFFS2 такими структурами являются

например сводные узлы и маркеры очистки блоков. Ввиду своего назначения, эти функции могут не покрываться обычными тестовыми наборами и требовать написания специализированных тестов.

#### 4.4 Окружение файловой системы

Функционал файловой системы зависит от множества факторов ее окружения. В данном разделе будут выделены параметры, от которых зависит функционал JFFS2.

Во-первых, для различных типов запоминающих устройств файловая система может использовать разные функции для работы с данными. Файловая система jffs2 по разному работает с устройствами технологии памяти типа NOR и NAND, а также имеет особый интерфейс взаимодействия с образцами с несортированными блоками (UBI) и устройствами флэш-памяти dataflash, подключаемыми по шине SPI.

Во-вторых, при тестировании заранее созданного образа ФС, тестируемый образ может быть создан с различными опциями. Для файловой системы JFFS2 опции команды mkfs, создающей образ ФС, могут быть использованы для задания размера выходного образа, размера стираемого блока, размера страницы, используемого алгоритма сжатия данных, используемой стратегии автоматического выбора алгоритма сжатия, используемого порядка бит в выходном образе и подключения либо отключения функционала расширенных атрибутов файлов Linux.

В-третьих, при тестировании команды монтирования, используемой для подключения файловой системы к единому дереву каталогов, могут быть указаны различные опции. При помощи опций общих для всех файловых систем можно устанавливать режим доступа к данным, содержащимся на подключаемом устройстве, например доступ только для чтения, либо для чтения и записи. С использованием опций специфичных для JFFS2 можно например выбрать используемый алгоритм сжатия данных.

В-четвертых, функционал собранного ядра операционной системы во многом определяется составленным на этапе сборки файлом конфигурации. Опции, определяемые в этом файле могут отвечать за подключение определенных модулей ядра и указание параметров для этих модулей. Для модуля устройств на основе технологии памяти в конфигурационном файле могут быть указаны опции, отвечающие за подключение различных эмуляторов и определение их параметров, поддержку драйве-

ров нужных для взаимодействия с различными чипами и контроллерами устройств памяти. Для файловой системы JFFS2 при помощи опций конфигурационного файла подключается поддержка расширенных атрибутов Linux, поддержка буфера записи, использование структуры сводных узлов и маркеров очистки и поддержка различных алгоритмов сжатия. Также при помощи конфигурационных опций может быть выбрана стратегия автоматического выбора алгоритма сжатия. Например, строка "CONFIG\_JFFS2\_CMODE\_PRIORITY=y" в файле конфигурации ядра указывает файловой системе выбирать алгоритм сжатия на основе их приоритета, а строка "CONFIG\_JFFS2\_CMODE\_SIZE=y" указывает на выбор алгоритма сжатия на основе размера сжатых данных.

#### **4.5 Создание системы автоматизированного тестирования**

В соответствии с целью и поставленными в работе задачами, для создания системы автоматизированного тестирования файловой системы JFFS2 необходимо протестировать исследуемую ФС при помощи имеющихся решений, в процессе доработать или адаптировать необходимые инструменты, расширить покрытие достигаемое при использовании имеющихся решений, произведя запуск в различных конфигурациях окружения, протестировать функции обработки ошибок при помощи инструментов фаззинг-тестирования, и создать тесты, покрывающие редкие сценарии с использованием технологии внедрения ошибок.

## 5 Описание практической части

### 5.1 Используемые инструменты

В данном разделе будет приведен список инструментов используемых в ходе практической части работы.

В ходе всей работы по тестированию JFFS2 используется код ядра Linux версии 5.10 из репозитория лаборатории Linux Verification Center. Процесс тестирования происходит на виртуальной машине Qemu, эмулирующей машину архитектуры x86-64 под гостевой системой Ubuntu Linux.

Для тестирования сценариев работы с различными типами устройств флэш-памяти без использования реальных микросхем памяти, необходимо использовать эмуляторы флэш-устройств. На данный момент в модуле устройств на основе технологии памяти (MTD) ядра Linux реализованы 3 эмулятора: `mtddram`, эмулирующий NOR-память в оперативной памяти системы, `block2mtd`, эмулирующий устройство NOR-памяти поверх блочного устройства и `nandsim`, эмулирующий устройство NAND-памяти в оперативной памяти. Поддержка эмуляторов подключается в файле конфигурации ядра, например строка `"CONFIG_MTD_MTDRAM=y"` позволяет использовать эмулятор `mtddram`, а параметры `"CONFIG_MTDRAM_TOTAL_SIZE"` и `"CONFIG_MTDRAM_ERASE_SIZE"` устанавливают размер эмулируемого устройства и размер его стираемого блока.

За основу при создании системы автоматизированного тестирования было решено взять тестовый набор `xfstests`, так как он содержит в себе множество скриптов, тестирующих базовые функции общие для всех ФС, а также является наиболее популярным решением для тестирования файловых систем ядра Linux и имеет удобный функционал для добавления новых тестов. Для добавления в набор `xfstests` своих тестовых сценариев необходимо описать сценарий в виде `bash`-скрипта, запустить скрипт `new` для добавления нового теста в набор и создать файл, определяющий выходные данные, которые должны генерироваться в ходе корректной работы теста. При тестировании `xfstests` использует 2 блочных устройства, называемые `TEST` и `SCRATCH` с тестируемой ФС на них и два каталога, используемые для монтирования. Для предоставления тестовому набору интерфейса блочного устройства в модуле MTD есть драйвер `mtddblock`. Для использования этого драйвера необходимо установить соответствующую ему опцию конфигурации ядра, что делается при помощи строки `"CONFIG_MTD_BLOCK=y"`.

Для сбора информации о покрытии исходного кода модулей ядра используется утилита `gcov`. Для визуализации собранной информации в виде `html` отчета используется расширение утилиты `gcov` - `lscov`. Для сбора информации о покрытии в ядре Linux достаточно добавить строку `"CONFIG_GCOV"` файл конфигурации ядра при его сборке, а так же строку `"GCOV_PROFILE=y"` в файл `fs/jffs2/Makefile` для активации профилирования директории, содержащей исходные файлы тестируемой ФС. Для сбора корректного покрытия в ходе работы тестов перед запуском необходимо сбросить информацию о покрытии. Сброс покрытия можно осуществить командой `"echo 0 > /sys/kernel/debug/gcov"`. После окончания работы тестов, информация о покрытии хранится в директории `/sys/kernel/debug/gcov`. На основе собранного покрытия утилита `lscov` генерирует информационный файл, который преобразуется в `html`-отчет утилитой `genhtml`.

Для создания тестируемого образа файловой системы используется команда `mkfs` с опцией определяющей тип файловой системы. Команда для создания образа JFFS2 (`mkfs.jffs2`) является частью пакета инструментов для работы с флэш-памятью `mtdd-utils`. По неизвестной причине, из четырех алгоритмов сжатия, поддерживаемых JFFS2, команда создания образа файловой системы поддерживала только 3: `lzo`, `zlib` и `rttime`. С целью достичь более полного тестирования исходного кода, в процессе работы исходный код инструмента `mkfs.jffs2` был доработан, и таким образом была добавлена возможность создания образа JFFS2 с использованием алгоритма сжатия `rubin`.

Как было описано в прошлой главе, JFFS2 имеет специальные функции для работы с устройствами `dataflash`, подключенными по протоколу SPI и устройствами разделенными на томы с несортированными блоками (UBI устройства). К сожалению в открытом доступе нет эмулятора устройства `dataflash`, для тестирования сценария монтирования устройства такого типа, однако в модуле MTD есть эмулятор устройств с несортированными блоками - `gluebi`. Для подключения этого эмулятора в конфигурационном файле ядра используется строка `"CONFIG_MTD_UBI_GLUEBI=y"`. Подсистема UBI, являющаяся частью модуля MTD выполняет функции уровня флэш-преобразования, обеспечивая выравнивание износа блоков устройства, а также управляет томами, являющимися более высокоуровневой абстракцией над устройствами технологии памяти. В процессе практической работы, эмулятор `gluebi` вызывал панику ядра путем разыменования нулевого указателя. Для корректного использования эмулятора по-



требовалось исправление его исходного кода.

Для покрытия функций обработок ошибок фаззинг-тестированием, в работе будут использованы инструменты `syzkaller` и `fsfuzz`. Несмотря на то, что в документации инструмент фаззинг-тестирования файловых систем `fsfuzz` заявляется о совместимости с файловой системой JFFS2, прямолинейный запуск инструмента для исследуемой ФС не принес результата, так как `bash`-скрипт `fsfuzz` использует при монтировании виртуальные блочные устройства, что является неподходящим для JFFS2. После внесения правок в исходный код инструмента с целью использования MTD устройств при указании в качестве опции тип файловой системы JFFS2, инструмент удалось применить к тестированию исследуемой ФС.

## 5.2 Тестирование с использованием готовых решений

Для тестирования файловой системы с использованием готовых решений необходима предварительная сборка ядра с определенной конфигурацией, наличие тестируемого образа файловой системы и блочных устройств для монтирования. Далее в этом разделе будет описана базовая конфигурация, необходимая для тестирования JFFS2 при помощи готовых решений.

Во первых, необходимо в конфигурации ядра добавить поддержку тестируемой ФС и необходимой для ее работы подсистемы устройств технологии памяти, которая отсутствует в базовой конфигурации ядра. Это может быть осуществлено добавлением следующих строк в файл конфигурации ядра Linux: `"CONFIG_MTD=y` поддержка подсистемы MTD, `"CONFIG_JFFS2_` поддержка JFFS2. Во-вторых, после конфигурации и сборки ядра необходимо создать образ тестируемой ФС. Для этого используется команда `mkfs.jffs2`, являющаяся частью пакета инструментов `mtd-utils`, который требует предварительной установки, например при помощи менеджера пакетов `apt-get`. В третьих, для монтирования тестируемой ФС необходимы блочные устройства, которые в случае JFFS2 создаются драйвером `mtdblock` поверх MTD устройств эмулируемых одним из эмуляторов, например `block2mtd`, который тоже необходимо подключить в конфигурации ядра.

## 5.3 Результаты первого эксперимента

Прямолинейный запуск набора `xfstests` в описаной выше минимальной необходимой конфигурациидал результат в виде тестового покрытия ис-

ходного кода в 64%, а прямолинейный запуск тестов из пакета mtd-utils дал результат в виде покрытия 53% исходного кода. Следующим важным шагом является расширение тестового покрытия, на основе анализа функционала JFFS2 и параметров окружения, который был приведен в прошлой главе, а также анализа достигнутого в первом эксперименте покрытия.

#### 5.4 Расширение тестового покрытия

Первым шагом на пути к расширению тестового покрытия является добавление в конфигурации ядра всего функционала тестируемой ФС. Опции конфигурации JFFS2 и функционал на который они влияют описаны в файле `fs/jffs2/Kconfig`.

Анализ достигнутого при первом эксперименте покрытия показал, что не покрыты функции, используемые для работы с устройствами NAND-памяти и UBI томами, так как используемые эмулятор `block2mtd` эмулирован флэш-память NOR-типа. Для расширения тестового покрытия необходимо использовать эмулятор UBI томов `gluebi` и NAND-памяти `pandsim`.

Также не были покрыты функции алгоритмов сжатия данных. Для их покрытия необходимо подключить их поддержку в конфигурации ядра, создать несколько тестируемых образов с разными параметрами `mkfs`, например команда `mkfs.jffs2 compression-mode=size` создает образ ФС, алгоритм сжатия на котором будет определяться размерам сжатых данных. Для использования каждого конкретного алгоритма сжатия можно установить режим выбора алгоритма на выбор по приоритету и устанавливать приоритет тестируемого алгоритма выше остальных параметрами команды `mkfs`. Например команда `mkfs.jffs2 compression-priority=100:zlib` устанавливает максимальный приоритет алгоритму `zlib`.

#### 5.5 Расширенное тестовое покрытие

Тестовые наборы были перезапущены несколько раз с различными конфигурациями. Покрытия полученные в этих экспериментах, объединенные с результатом первого эксперимента дали результат в виде тестового покрытия в 75.8%.

По сравнению с первым экспериментом тестовое покрытие увеличилось на 11.8% или на 1275 строк кода.

## 5.6 Фаззинг-тестирование

Наиболее популярный инструмент фаззинг-тестирования ядра Linux и его модулей - syzkaller. Однако он плохо подходит для задачи тестирования файловой системы, так как суть его работы заключается в генерации случайных программ состоящих из различных системных вызовов. Для достижения типичного сценария работы ФС syzkaller должен сгенерировать программу, состоящую как минимум из монтирования валидного образа файловой системы и дальнейших взаимодействий с ним при помощи, например системных вызовов `open`, `write` и `close`. Для случайной генерации подходящего сценария потребуется множество перебранных неудачных вариантов последовательностей системных вызовов или монтирования невалидных образов.

Для того, чтобы сузить тестируемые syzkaller области, был применен файл конфигурации, приведенный в ПРИЛОЖЕНИИ. Параметры конфигурации syzkaller указывают ему список разрешенных к использованию системных вызовов и запрещают другие, чтобы он быстрее приходил к нужному сценарию. Инструменты описания грамматики системных вызовов, разработанные в syzkaller позволяют определить свою "мутацию" системного вызова заключающуюся например в определенных передаваемых параметрах. Таким образом в файле `sys/linux/filesystem.txt` определен системный вызов монтирования образа файловой системы JFFS2: `"syz_mount_image$jffs2"`. При включении этого вызова в конфигурации и отключении других вариантов монтирования, монтирование всего будет производиться с параметром типа файловой системы `jffs2`.

При столкновении с ошибкой в виде блокировки, неопределенного поведения, либо просто сообщения об ошибке или предупреждения syzkaller генерирует программу репродьюсер на языке Си, при запуске которой будет воспроизведен сценарий достигающий этой ошибки. Для генерации репродьюсеров при достижении строк не имеющих ошибок, но сценарий достижения которых необходимо воспроизвести, как с ранее непокрытыми тестовыми наборами в нашем случае, нужно добавить в код ядра предупреждение об ошибке например макросом `"WARN_ON(1)"`.

При помощи syzkaller удалось достичь покрытия 11 ранее непокрытых строк, отвечающих редким сценариям при обработке суперблока в процессе монтировании ФС.

Таким образом для расширения покрытия кода ФС, syzkaller был за-

пущен в конфигурации, разрешающей ему производить только системные вызовы для работы с ФС. Достигаемое им тестовое покрытие было проанализировано и в недостижимые ранее строки были помещены предупреждения об ошибках. При повторном запуске `syzkaller` при достижении этих строк он генерировал программы репродьюсеры, которые необходимо добавить в разрабатываемую систему автоматизированного тестирования.

При тестировании JFFS2 при помощи доработанного инструмента фаззинга файловых систем `fsfuzz` было также достигнуто покрытие 13 ранее непокрытых строк, составляющих две ранее непокрытые функции обновления опций монтирования при реконфигурации суперблока ФС.

Таким образом, фаззинг-тестирование помогло покрыть 24 ранее непокрытых строки кода, достижимые только в редких сценариях.

## **5.7 Тестирование с использованием симуляции сбоев**

TODO

## **5.8 Анализ непокрытого кода**

TODO

## 6 Заключение

В результате проделанной работы была разработана система автоматизированного тестирования файловой системы JFFS2 на основе существующих решений для тестирования файловых систем. В процессе разработки системы тестирования был доработан инструмент создания образа JFFS2, путем добавления в него поддержки алгоритма сжатия `rubin`, был адаптирован для тестирования JFFS2 с использованием драйвера `mttblock` инструмент фаззинг-тестирования файловых систем `fsfuzz`. Был проиведен анализ достигаемого разработанной системой покрытия и были классифицированы непокрытые строки исходного кода тестируемой ФС.

## Список литературы