Ордена Трудового Красного Знамени федеральное государственное бюджетное
образовательное учреждение высшего образования
«Московский технический университет связи и информатики»

На правах рукописи

Рыбаков Сергей Юрьевич

ОБНАРУЖЕНИЕ И КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ АТАК МЕТОДАМИ МУЛЬТИФРАКТАЛЬНОГО АНАЛИЗА И МАШИННОГО ОБУЧЕНИЯ

Специальность 2.3.6.
Методы и системы защиты информации, информационная безопасность

ДИССЕРТАЦИЯ
на соискание ученой степени
кандидата технических наук

Научный руководитель:
доктор технических наук,
профессор Шелухин Олег Иванович

Москва - 2025

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования. В настоящее время в связи с повсеместным ускоренным развитием и внедрением разнообразных информационных систем, возрастает и число возможных уязвимостей и, соответственно, компьютерных атак (КА) на них. Важным этапом в противодействии различным угрозам информационной безопасности является не только своевременное обнаружение КА, но и их правильная классификация.

Обеспечение информационной безопасности как противодействие компьютерным атакам — это важная задача, которая должна решаться в современных компьютерных сетях (КС). Проблема обнаружения КА обусловлена как вариативностью выбора эффективного математического аппарата и реализацией соответствующего алгоритма, так и неопределенностью (по виду, времени и сигнатуре) воздействия атаки. Большинство известных методов обнаружения КА достаточно сложны в программной реализации и имеют недостатки, связанные с недостоверным определением момента (флага) начала атаки.

Существенный прогресс в области обнаружения КА связан с применением методов интеллектуального анализа данных, а в частности, методов машинного обучения. Однако эти методы сталкиваются с проблемами обработки большого числа малозначимых признаков, высокой вероятностью ложных срабатываний и, что наиболее важно, неспособностью выявлять сложные атаки, изменяющие свойства сетевого трафика. В этой связи особую актуальность приобретает поиск новых, устойчивых и информативных атрибутов (признаков), отражающих глубинные структурные изменения в трафике при атаке. В качестве таких признаков часто рассматриваются фрактальные характеристики сетевого трафика. Ранее установлено, что любая атака или аномальная активность в сети приводит к изменению текущего значения фрактальной размерности, что позволяет использовать этот факт как индикатор начала атаки/аномалии.

Особенностью сетевого трафика является достаточно устойчивое самоподобие, что позволяет вскрывать изменения его временной структуры, выявлять изменения процессов, невидимые при обычном мониторинге в режиме реального времени, сигнализировать о возможном начале КА.

Поскольку свойство самоподобия наблюдается в относительно широком временном интервале (от нескольких миллисекунд до минут), наличие в трафике аномальной активности, возможно связанной с атакой, изменяет фрактальную природу при разном временном разрешении, что указывает на то, что КА, по-видимому, имеет мультифрактальную структуру. В связи с этим исследование и разработка методов обнаружения и классификации КА с использованием мультифрактального анализа является актуальной научной задачей, решение которой направлено на повышение уровня защищенности КС.

Таким образом, перспектива улучшения качества работы сетевой защиты информации видится в комплексном использовании мультифрактального и интеллектуального анализа данных и разработки соответствующего научно-методического аппарата.

Степень разработанности темы

Методам фрактального анализа в различных областях техники посвящено достаточно много исследований авторов Божокина С.В., Паршина Д.А., Басараба М.А., Лавровой Д.С., Шелухина О.И., Mandelbrot B.B., Willinger W., Taqqu M.S., Abry P., Veitch D. и др.

В свою очередь вопросам обнаружения атак методами машинного обучения в компьютерных сетях посвящено достаточно большое количество работ: Петренко С.А., Бирюкова Д.Н., Лавровой Д.С., Павленко Е.Ю., Саенко И.Б., Котенко И.В., Израилова К.Е., Шелухина О.И., Харроу Ф., А. Окутана, Barabasi A.L, Al-Garadi M.A., Ferrag M.A. и др.

Однако вопросам совместного использования методов машинного обучения и фрактального анализа с целью повышения достоверности обнаружения и (или) классификации КА ранее не уделено должного внимания. В результате, несмотря на существенный задел по двум направлениям, созданный отечественными и

зарубежными учеными, интегральная задача обнаружения КА в КС и их классификации с использованием МО и фрактального анализа не могла считаться разрешенной и потребовала проведения новых исследований. При этом анализ опубликованных работ подтверждает актуальность исследований в области интеллектуального обнаружения компьютерных атак, используя выявление их фрактальной свойств.

Объект исследования – сетевой трафик компьютерных сетей.

Предмет исследования – методы, модели и алгоритмы фрактального анализа и машинного обучения для обнаружения и классификации КА в компьютерных сетях.

Целью работы является повышение качества классификации компьютерных атак в компьютерных сетях с помощью комбинации мультифрактального анализа и машинного обучения.

Достижение поставленной цели предусматривает решение **частных задач**:

1. Анализ объекта с позиции предмета исследований.
2. Разработка улучшенной модели оценки фрактальных свойств компьютерных атак в онлайн-режиме методами вейвлет-анализа.
3. Разработка метода повышения эффективности алгоритмов обнаружения/классификации атак в компьютерных сетях методами машинного обучения при условии дополнительной информации о фрактальных свойствах атак и сетевого трафика.
4. Разработка модели алгоритмической и численной оценки мультифрактальных свойств сетевого трафика и компьютерных атак.
5. Разработка метода композиции машинного обучения и мультифрактального анализа сетевого трафика для улучшения многоклассовой классификации компьютерных атак.

Научная новизна полученных результатов:

1. Модель оценки фрактальной размерности, отличающаяся от известных дополнительной фильтрацией детализирующих коэффициентов вейвлет-

разложения, что повышает точность на 15…40% в зависимости от используемого типа материнского вейвлета.

2. Метод обнаружения и классификации КА, который повышает достоверность и точность обнаружения КА в среднем на 10% за счет введения дополнительной информации о статистических характеристиках фрактальной размерности (ФР) сетевого трафика и КА.

3. Новая модель оценки характеристик мультифрактального спектра фрактальной размерности (МСФР) трафика и КА с помощью последовательности текущих оценок ФР в окне фиксированной длины, варьируемой в зависимости от интервала разрешения (времени дискретизации), что позволяет формализовать новые полезные признаки классификации.

4. Новый метод композиции машинного обучения и мультифрактального анализа сетевого трафика, который позволяет повысить точность многоклассовой классификации КА за счет добавления новых атрибутов, в среднем на 7-10%.

Теоретическая значимость работы заключается в развитии теории мультифрактального анализа с учетом априорной информации о моно и мультифрактальных характеристик КА и сетевого трафика, а также разработке улучшенных алгоритмов обнаружения и классификации компьютерных атак на основе методов машинного обучения и дискретного вейвлет-анализа.

Практическая значимость работы. Реализация разработанных алгоритмов при мониторинге и обеспечения информационной безопасности КС широкого профиля, в том числе киберфизических систем, в промышленном Интернете вещей, а также в других сложных информационных системах с иерархической структурой.

Методология и методы исследования: системный анализ, методы фрактального и вейвлет-анализа, теория вероятности, математическая статистика, методы математического численного имитационного моделирования, методы машинного обучения и интеллектуального анализа данных.

Положения, выносимые на защиту:

1. Модель оценки фрактальной размерности компьютерных атак в реальном времени, использующая дополнительную фильтрацию коэффициентов вейвлет разложения с помощью трешолдинга.

2. Метод обнаружения и классификации КА, учитывающий дополнительную априорную информацию о статистических характеристиках фрактальной размерности сетевого трафика и КА.

3. Модель оценки характеристик мультифрактального спектра фрактальной размерности трафика и КА в окне фиксированной длины, варьируемой в зависимости от интервала разрешения (времени дискретизации).

4. Метод композиции машинного обучения и мультифрактального анализа, основанный на введении дополнительных атрибутов МСФР при многоклассовой классификации сетевого трафика и КА.

Все выносимые на защиту результаты являются новыми.

Достоверность и обоснованность результатов, представленных в диссертации, подтверждается анализом предшествующих научных работ в данной области, корректным использованием математического аппарата, полученными адекватными экспериментальными данными, достаточно широкой апробацией результатов исследования в научных публикациях и докладах на конференциях.

Внедрение и реализация результатов исследования.

Результаты работы внедрены в проектную деятельность ФГУП «НИИ «Квант», в учебный процесс МТУСИ при проведении лекционных занятий по дисциплинам «Искусственный интеллект и машинное обучение в кибербезопасности» и «Обнаружение вторжений в компьютерные сети»

Апробация результатов

Основные результаты диссертационной работы обсуждались и получили одобрение на конференциях: XXV международная научная конференция «Wave Electronics and Its Application in Information and Telecommunication Systems (WECONF-2022)» (Санкт-Петербург, 2022); XVII Международная отраслевая научно-техническая конференция «Технологии информационного общества»

(Москва, 2023); 33-я научно-техническая конференция «Методы и технические средства обеспечения информационной безопасности» (Санкт-Петербург, 2024); X Всероссийская научно-техническая конференция «Фундаментальные и прикладные аспекты компьютерных технологий и информационной безопасности» (Таганрог, 2024); Международная научная конференция «Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO)» (Выборг, 2024).

Публикации

Результаты диссертационной работы отражены в 16 работах, в том числе:

9 - в научных изданиях перечня ВАК; 2 - в научных рецензируемых изданиях по базе Scopus; 4 – в материалах конференций и других изданиях. Получено свидетельство о Государственной регистрации программы для ЭВМ.

Соответствие паспорту специальности. Научные результаты соответствуют следующим пунктам паспорта научной специальности 2.3.6. - Методы и системы защиты информации, информационная безопасность:

п.6. Методы, модели и средства мониторинга, предупреждения, обнаружения и противодействия нарушениям и компьютерным атакам в компьютерных сетях.

п.15. Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.

Личный вклад автора. Все основные научные результаты, касающиеся разработки методов, моделей, алгоритмов и их реализации, получены автором лично. Вклад соавторов ограничивался постановкой задач на исследование и обсуждением полученных результатов.

Глава 1 Анализ методов обнаружения компьютерных атак в компьютерных сетях. Постановка цели и задач исследования

1.1 Тенденции создания методов обнаружения компьютерных атак в компьютерных сетях

Задача обнаружения компьютерных атак (КА) в компьютерных сетях (КС) стабильно остается одной из ключевых в области информационной безопасности. Причина очевидна - подавляющее большинство атак проявляется в виде отклонений характеристик сетевого трафика от нормального профиля, при том, что спектр самих атак чрезвычайно разнообразен по технике и уровню сложности. При ограниченном наборе альтернативных, сопоставимых по эффективности подходов именно детектирование аномалий выступает базовой парадигмой защиты, что и объясняет наличие значительного числа обзоров по современному состоянию области, включая попытки унификации классификаций атак, методов и средств их обнаружения [1–6].

Статистические подходы сохраняют практическую значимость и во многих сценариях демонстрируют приемлемые результаты [7]. Однако по мере усложнения и распределенности современных инфраструктур на первый план выходят методы/алгоритмы машинного обучения (МО), которые чаще обеспечивают более высокую результативность при детектировании аномалий в сетевом трафике [8, 9]. Алгоритмы МО позволяют автоматически извлекать слабовыраженные многомерные закономерности из больших массивов сетевых данных, тем самым повышая скорость реагирования на КА и снижая трудоемкость аналитических процедур в кибербезопасности [10].

Показателен опыт использования алгоритмов опорных векторов (Support Vector Machine, SVM): по данным работы [11], SVM остаются одним из наиболее часто используемых инструментов детектирования КА и достигают точности (accuracy) порядка 80–99,6% в зависимости от условий эксперимента; сопоставимые результаты получены и для мобильных сетей [12–14]. Идея

целенаправленного поиска сетевых аномалий, ассоциированных с конкретными классами атак, последовательно развита в [15]. Применимость методов МО подтверждена и для инфраструктур Интернета вещей (IoT) [16], где из-за ограничений по вычислительным ресурсам предъявляются жесткие требования к «легкости» моделей по памяти и времени исполнения задач.

Важным направлением повышения эффективности выступают гибридные и ансамблевые схемы. Работы [17, 18] демонстрируют, что рациональные комбинации SVM, деревьев решений, наивного байесовского классификатора, многослойных персептронов и др. позволяют ускорять обучение и анализ трафика в режиме реального времени; вместе с тем точность может варьироваться в зависимости от конфигурации ансамбля и свойств данных.

Также активно развиваются методы глубокого обучения. Комбинированные нейросетевые архитектуры показывают высокую результативность как в обнаружении аномалий, так и в идентификации инцидентов компьютерной безопасности [19, 20]. Часто в состав таких систем включают автоэнкодеры, понижающие размерность и формирующие информативные представления признаков перед классификацией. Не теряют актуальности и самоорганизующиеся карты (карты Кохонена), которые после обучения группируют близкие по описанию векторы, что упрощает выделение выбросов в сетевом трафике [21–23].

Заметную роль играют рекуррентные нейронные сети, учитывающие временную структуру наблюдений [24, 25]. На практике чаще всего применяются LSTM-модели (Long Short-Term Memory) благодаря сочетанию устойчивости результатов и умеренной сложности реализации. В [26] предложено объединять LSTM и SVM для повышения производительности при анализе последовательностей переменной длины. Работа [27] демонстрирует эффективность LSTM-автоэнкодера для выявления аномалий в непериодических временных рядах. В [28] представлен LSTM-детектор, не требующий предварительного обучения, а [29] показывает масштабируемость LSTM к крупным многомерным наборам данных.

1.2 Особенности сетевого трафика и КА сетей IoT

Технологии IoT (интернета вещей) появились сравнительно недавно и за последнее десятилетие получили широкое распространение. Интернет вещей представляет собой систему взаимосвязанных компьютерных сетей и физических объектов, оборудованных множеством встроенных сенсоров, которые собирают информацию о окружающей среде. С этой целью используется специальное программное обеспечение, которое обрабатывает данные и передает информацию с датчиков по сети для последующего анализа, удаленного контроля и управления объектами IoT без участия пользователя. Также программное обеспечение обеспечивает функции хранения данных и обеспечивает доступ к ним [30,31]. Обычно в рамках IoT присутствуют отдельные сети, каждая из которых разработана для решения конкретных задач.

Специалисты в области IoT прогнозируют ежегодное увеличение на 20% количества «умных» устройств в период с 2020–2025 [32]. В связи с быстрым ростом количества устройств и технологии в целом появляются риски, связанные с обеспечением информационной безопасности. Устройства интернета вещей подключены к Интернету и связаны между собой и нередко становятся целью злоумышленников, желающих получить доступ к ресурсам «умных» устройств.

Поскольку устройства IoT обладают ограниченным объемом памяти и малой вычислительной мощностью в них обычно не устанавливаются средства обеспечения безопасности от сетевых атак.

Однако, производители услуг и оборудования, связанных с интернетом вещей (IoT), чаще всего не придерживаются принципа сквозной информационной безопасности, в основном из-за экономических факторов и причин. Это означает, что информационной безопасности в сфере IoT обычно не уделяется должного внимания, несмотря на то что все больше пользователей и организаций приобретают "умные" устройства, такие как роутеры или камеры видеонаблюдения. К сожалению, мало кто задумывается о защите этих устройств и установке актуальных обновлений.

Существует опасность, связанная с распространением целевых кибератак на устройства IoT, и количество таких атак продолжает расти [33]. Поэтому, информационная безопасность должна учитывать и закладываться еще на стадии проектирования устройства или услуги и поддерживаться на протяжении всего его жизненного цикла.

Злоумышленники в свою очередь используют зараженные сети "умных" устройств для осуществления DDoS-атак или в качестве прокси-серверов для других вредоносных действий.

Согласно предоставленным данным [34], атаки на устройства интернета вещей (IoT) обычно не требуют сложной реализации, однако они достаточно незаметны для обычных пользователей. Одним из самых распространенных видов вредоносных программ, позволяющих ботнетам захватывать и управлять IoT-устройствами путем использования устаревших уязвимостей, является Mirai. Например, одна из версий вредоносной сети Mirai проникла в более чем 5 миллионов устройств, включая IoT-устройства, в 164 странах мира. Это семейство вредоносного программного обеспечения использовалось в 39% всех атак. К числу других наиболее распространенных атак в сетях IoT относятся атаки типа SSDP Flood, OS Scan.

1.3 Анализ методов машинного обучения (МО) используемых для обнаружения компьютерных атак

1.3.1 Особенности методов машинного обучения и вычислительного интеллекта

Машинное обучение — это класс методов, в которых программная система улучшает качество решения заданной задачи за счет опыта, извлекаемого из данных. Формально цель методов/алгоритмов МО — построить функцию отображения входов в выходы с хорошей обобщающей способностью: модель должна не просто «запомнить» обучающие примеры, а корректно работать на

новых, ранее не виденных данных. В практических терминах это достигается через подбор параметров модели по критерию качества (например, минимизации функции потерь) на обучающей выборке.

Различают несколько парадигм обучения: с учителем (когда доступны пары «признаки—метка»), без учителя (поиск структур и зависимостей без целевых меток), полу-контролируемое обучение (комбинация маркированных и немаркированных данных) и обучение с подкреплением (оптимизация стратегии действий по сигналу вознаграждения). Современные подходы включают как классические алгоритмы (SVM, деревья решений, ансамбли), так и глубокие нейронные сети, способные автоматически извлекать представления признаков. В прикладном конвейере это дополняется этапами подготовки данных, отбора или построения признаков, настройки гиперпараметров и валидации (например, перекрестной).

Ключевое отличие от традиционных статистических методик не в противопоставлении, а в фокусе: статистика стремится к объяснению и интерпретации механизмов порождения данных и проверке гипотез, тогда как МО приоритетно оптимизирует предсказательную точность. На практике эти подходы взаимодополняемы: статистическое мышление нужно для корректной постановки задачи, оценки неопределенности и предотвращения методологических ошибок, а инструменты МО — для масштабируемого извлечения сложных закономерностей в высокоразмерных данных. Важной чертой МО является адаптивность: модели могут обновляться по мере поступления новых данных (онлайн-обучение), переносить знания между смежными задачами (transfer learning) и перестраиваться при изменении распределения данных (обработка «дрейфа концепции»).

Одновременно у МО есть ограничения.

- Во-первых, высокие вычислительные затраты на обучение (особенно у глубоких моделей), требующие значительных ресурсов памяти и специализированного железа.

- Во-вторых, чувствительность к качеству и репрезентативности данных: шум, смещения выборки и несоответствие доменов приводят к деградации качества и усложняют адаптацию под конкретную предметную область.
- В-третьих, риски переобучения и необходимость тщательной регуляризации, корректной валидации и подбора гиперпараметров.
- В-четвертых, ограниченная интерпретируемость сложных моделей, вопросы устойчивости (в том числе к целенаправленным вмешательствам), воспроизводимости и соблюдения ограничений по задержкам/ресурсам при внедрении.

Подход машинного обучения, как правило, включает следующие этапы:

- Определение атрибутов класса (признаков) и классов в обучающих данных.
- Выбор подмножества атрибутов, необходимых для классификации, с целью уменьшения размерности.
- Обучение модели на обучающих данных.
- Использование обученной модели для классификации неизвестных данных в режиме тестирования.

В постановке задачи обнаружения КА с контролируемым обучением на этапе тренировки для каждого класса компьютерных атак модель настраивается по соответствующим размеченным примерам из обучающей выборки. На этапе применения (тестирования) новые наблюдения подаются на вход обученному классификатору, и каждому экземпляру присваивается метка одного из известных классов атак. Если образец не соответствует ни одному из этих классов по принятому решающему правилу, он трактуется как нормальный трафик.

В процессе обнаружения аномалий проводится подготовка, валидация и тестирование моделей машинного обучения. На этапе подготовки определяется профиль нормального трафика, а на этапе тестирования обученная модель применяется к новым данным для классификации их как нормальных или аномальных.

Однако, для достижения высокой точности на тестовых данных и выбора оптимальной модели, требуется третий этап - валидация. По завершении обучения, когда имеется несколько моделей, например, искусственные нейронные сети (ИНС), применяется набор данных для валидации. Модель, показывающая наилучшие результаты на валидационных данных, выбирается для использования. Важно отметить, что выбранная модель не должна быть модифицирована в зависимости от точности на тестовых данных, чтобы избежать искажения результатов при использовании различных наборов данных. Такой подход позволяет достичь более надежных результатов в задаче обнаружения аномалий с использованием методов машинного обучения.

Машинное обучение имеет три основных типа подходов, каждый из которых отличается своей методологией:

1. Обучение без учителя (unsupervised learning): здесь основной задачей является нахождение шаблонов, структур или знаний в непомеченных данных. Этот подход позволяет обнаруживать скрытые закономерности и группировать данные на основе их схожести без явно указанных меток.

2. Обучение с учителем (supervised learning): — это подход, при котором каждому объекту в данных заранее сопоставлена целевая метка, полученная при сборе данных или в результате экспертной разметки. Цель состоит в построении отображения из признакового пространства в пространство меток. После обучения на размеченной выборке такая модель применяется к данным для их классификации (или предсказания целевого значения).

3. Сочетание обучения без учителя и с учителем (semi-supervised learning): в полуобучаемом подходе часть данных помечена, а другая часть остается непомеченной. Добавление помеченных данных значительно помогает в решении задачи. Этот тип подхода позволяет использовать как непосредственную информацию из помеченных данных, так и изучать общие закономерности в непомеченных данных.

В задачах обнаружения аномалий методы, основанные на классификации, применяются для обучения модели на размеченных данных, отнесенных к

различным классам (этап обучения). Затем эта модель может использоваться для классификации новых экземпляров данных и определения их принадлежности к нормальному или аномальному классу (этап экзамена). Это предполагает, что классификатор, обученный в заданном пространстве признаков, сможет разделить нормальные и аномальные объекты, что является ключевым аспектом в задаче обнаружения аномалий.

Среди различных методов обнаружения аномалий, основанных на классификации, можно выделить следующие подходы, которые используются [35, 36]:

1. Метод байесовских сетей. Это графическая модель, которая отображает вероятностные зависимости между переменными и позволяет делать вероятностные выводы. Байесовская сеть состоит из графической структуры, определяющей зависимости между случайными переменными, и набора вероятностных распределений, определяющих силу этих зависимостей. При использовании метода байесовских сетей для обнаружения аномалий оценивается вероятность наблюдения нормального или аномального классов. Примером простого подхода является наивный байесовский подход (Naive Bayes Approach) [37].

2. Метод опорных векторов (Support Vector Machine). Этот метод применяется для обнаружения аномалий в системах, где нормальное поведение представлено только одним классом. Он строит границу региона, в котором находятся экземпляры нормальных данных. Затем каждый исследуемый экземпляр проверяется на принадлежность этому региону. Если экземпляр находится за пределами региона, он считается аномальным. Описание работы метода опорных векторов можно найти, например, в [38].

3. Продукционные правила. В этом методе обнаружения аномалий выделяются два случая. В первом случае обучающее множество содержит примеры только одного класса, и основной интерес заключается в определении принадлежности рассматриваемых объектов к этому классу. Здесь требуется установить "границу", по которой временной ряд будет относиться к классу из

обучающего множества (не являться аномалией) или не относиться (являться аномалией). Во втором случае необходимо дополнительно определить принадлежность объекта к конкретному классу.

Каждый из этих методов представляет собой инструмент для обнаружения аномалий и имеет свои особенности и применения.

Обнаружение аномалий на основе классификации предлагает множество преимуществ благодаря разнообразию методов и алгоритмов, разработанных в области машинного обучения. Особенно полезно это при наличии обучающих данных, содержащих примеры из разных классов.

В отличие от методов, опирающихся на заранее размеченные данные, методы кластеризации выявляют аномалии, используя структуру кластеров в выборке или информацию о ближайших соседях. Логика работы базируется на следующих допущениях:

1. «Нормальные» объекты образуют компактные области высокой плотности, тогда как аномальные лежат вне этих областей.

2. Типичные объекты располагаются ближе к центру своего кластера; аномалии имеют существенно большие радиальные расстояния.

3. Обычные объекты принадлежат крупным, плотным кластерам, тогда как аномальные тяготеют к небольшим и разреженным группам (или остаются изолированными).

К этому же классу относят методы на ближайших соседях: объект считается аномальным, если его расстояния до k-ближайших соседей велики или локальная плотность заметно ниже, чем у окружения.

Преимущества подхода - возможность обучения без учителя, относительная гибкость к типам данных и эффективное разделение «норма/аномалия» при небольшом числе кластеров. Вместе с тем имеются существенные ограничения - высокая чувствительность к выбранному алгоритму кластеризации и его гиперпараметрам (число кластеров, метрика, пороги плотности), а также тот факт, что цель кластеризации — группировать похожие объекты, а не специально искать

выбросы. В результате аномалии нередко появляются лишь как побочный продукт процедуры кластеризации, что может снижать надежность детектирования.

1.3.2 Постановка задачи бинарной классификации

В условиях, когда для наблюдений доступна разметка (например, по результатам верификации инцидентов или экспертной оценки), задача выявления отклонений естественным образом сводится к бинарной классификации: различению «нормы» и «атаки». Такой подход обеспечивает воспроизводимость решений, возможность строгого выбора порога с учетом стоимости ошибок и применение стандартных метрических оценок качества.

Задача бинарной классификации может быть сформулирована в следующем виде. Пусть дано множество X, в котором хранится описание объектов *o*. Y – конечное множество классов. Классификатором F является отображение X в множество Y, т.е. $\boldsymbol{F}: \boldsymbol{X} \to \boldsymbol{Y}$. Признак (атрибут) f объекта o – это отображение $\boldsymbol{f}: \boldsymbol{o} \to \boldsymbol{D_f}$, где $\boldsymbol{D_f}$–множество допустимых значений признака f. Если задан набор признаков $\boldsymbol{f_1}, \dots, \boldsymbol{f_m}$ для некоторого объекта o, то вектор признаков x объекта $\boldsymbol{o} \in \boldsymbol{X}$ может быть определен как $\boldsymbol{x} = \boldsymbol{f_1}(\boldsymbol{o}), \dots, \boldsymbol{f_m}(\boldsymbol{o})$. Классификатор F должен быть способен классифицировать произвольный объект $\boldsymbol{o} \in \boldsymbol{X}$. Для обучения классификатора F используется обучающая выборка, заданная множеством $\boldsymbol{D} = \{(x_1, y_1), \dots, (x_v, y_v)\}, y_r \in \boldsymbol{Y} = \{0; 1\}, r = \overline{1, v}$.

Оптимальным считается классификатор, который дает наименьшую вероятность ошибки ***P(x)*** при всех допустимых значениях $\boldsymbol{x}$. Тогда критерием оптимальности будет $\boldsymbol{P}(\boldsymbol{x}) \to \min\limits_{x \in \boldsymbol{X}}$. Ошибки классификатора разделяются на «ошибки 1-го рода» (False Positive — ложно положительные события) и «ошибки 2-го рода» (False Negative — ложно отрицательные события).

1.3.3 Алгоритмы и метрики классификации

В соответствии с [39] для решения задачи классификации был рассмотрен репрезентативный набор моделей, охватывающий метрические, линейные, вероятностные, ядровые и древовидные подходы. Для всех методов, за исключением дерева решений, применялась предварительная нормализация признаков.

- ***k-ближайших соседей (k-Nearest Neighbors, kNN).*** Обучение и оценка проводились на нормализованном признаковом пространстве.
- ***Множественная логистическая регрессия*** (Logictic Regression, ***LR***). Для решения оптимизационной задачи использовался стохастический градиентный алгоритм SAGA; данные предварительно нормализованы.
- ***Мультиномиальный Наивный Баиес*** (*Multinomial Naive Bayes*, ***NB***). Модель обучалась на нормализованном наборе признаков.
- ***Метод опорных векторов*** (Support Vector Machines, SVM, **VM**). Применялось радиально-базисное ядро $(k(x, x') = e^{(-\gamma \|x-x\prime\|^2)}$ с параметром $\gamma = 2$. Использовались нормализованные данные.
- ***Дерево решений (****Decision Tree Classifier,* ***DTC***). В качестве критерия разделения выбран индекс нечистоты Джини; нормализация признаков не требовалась. По результатам эмпирического подбора гиперпараметров наилучшее качество достигалось при числе учитываемых признаков 28 и глубине дерева 23.
- ***Случайный лес (****Random Forest* - ***RF)***. Из-за того, что основой алгоритма является дерево решений, *нормализация не требуется.* Наилучший результат для рассматриваемого набора данных был получен при разбиении потока данных на 100 подвыборок.
- ***Ada Boost (AB)***. Из-за того, что основой алгоритма является дерево решений, *нормализация не требуется.* Наилучший результат для рассматриваемого набора данных был получен при разбиении потока данных на 1000 подвыборок.

Для оценки эффективности построенных моделей обычно используются следующие метрики: точность (*precision*), полнота (*recall*), F-мера (*F-score*),

$$accuracy = \frac{TP + TN}{TP + TN + FP + FN}, \tag{1.1}$$

$$precision = \frac{TP}{TP + FP}, \tag{1.2}$$

$$recall = \frac{TP}{TP + FN}, \tag{1.3}$$

$$F_{score} = \frac{2TP}{\left(2TP + FN + FP\right)}, \tag{1.4}$$

$$AUC = \int_{\infty}^{-\infty} TPR(T)FPR'(T)dt = \left\langle TPR \right\rangle. \tag{1.5}$$

где TP (англ. True Positive) – истинно положительный исход классификации; TN (англ. True Negative) – Истинно отрицательный исход классификации, FP (англ. False Positive) – Ложно положительный исход классификации, FN (англ. False Negative) – Ложно отрицательный исход классификации.

1.4 Анализ методов обнаружения КА основанных на фрактальном анализе и оценке фрактальной размерности (ФР)

1.4.1 Анализ публикаций

Многочисленные исследования статистики сетевого трафика, сетевых аномалий и компьютерных атак (КА) фиксируют наличие у соответствующих временных рядов свойств самоподобия и (или) фрактальности, а также вариативность метрик, которые эти свойства количественно описывают [40–42]. Для оценки степени самоподобия обычно привлекают две взаимосвязанные характеристики: хаусдорфову фрактальную размерность D графа процесса и

показатель Херста H, отражающий выраженность долгосрочных зависимостей. Они связаны соотношением $D=2-H$.

В телекоммуникационных приложениях на практике чаще используют именно показатель Херста H (он отличается от D на фиксированную величину), о чем свидетельствуют работы [41–43]. В дальнейшем, будем интерпретировать оценки H как оценки фрактальной размерности нормального трафика и трафика при КА.

Методы фрактального анализа применяются для выявления атак и сетевых аномалий, включая сценарии мониторинга в реальном времени, когда контролируется текущее значение фрактальной размерности (или эквивалентные показатели) сетевого трафика [43]. Формализация различий между «нормальными» и аномальными реализациями может осуществляться через сопоставление: фрактальных размерностей, корреляционных размерностей, а также через характеристики мультифрактальности, в частности интервалов, описывающих «ширину» спектра Лежандра для каждой реализации.

Показано, что информационные размерности сравниваемых реализаций отличаются на небольшую константу и слабо зависят от числа уровней разложения (например, при многомасштабном анализе). Из этого следует, что длительные атаки и эпизоды аномальной активности модифицируют самоподобную структуру трафика, а указанное изменение может служить надежным индикатором для детектирования атак.

Учитывая, что для оценки ФР трафика требуется как правило значительные интервалы времени и большие объемы данных обнаружение КА с помощью фрактального анализа осуществлялось как правило независимо от других методов, позволяющих определить аномалии во временном ряду в режиме реального времени. Все это послужило поводом для поиска новых методов обнаружения и прогнозирования, к числу которых можно отнести комбинацию машинного обучения и фрактального анализа.

Появились работы, в которых вопросы обнаружения и классификации КА стали интегрироваться с методами машинного обучения [43-46].

В работе [44] на примере базы данных KDD Cup1999 [46,47] показано положительное влияние оценки самоподобных свойств сетевого трафика характеризуемого средним значением показателя Херста на качество бинарной классификации.

Установлено, что расширение признакового (атрибутного) пространства за счет включения атрибутов, описывающего фрактальную размерность атак, улучшает точность бинарной классификации для всех алгоритмов, рассмотренных в данном исследовании.

В работах [44,45] на примере набора данных UNSW-NB15 приведены результаты исследования влияния широкого спектра статистических характеристик ФР на качество бинарной классификации. Показано, что параметры ФР могут рассматриваться как дополнительные информационные признаки (атрибуты) КА.

В качестве дополнительных признаков предложно использовать широкий спектр статистических характеристик ФР обрабатываемых последовательностей. Эффективность предлагаемого метода оценивается путем оценки качества бинарной классификации сетевых атак и нормального трафика с помощью алгоритмов машинного обучения показано, что использование в качестве дополнительных информационных признаков статистических характеристик ФР позволяет повысить эффективность бинарной классификации в среднем на 10%

В работах [47,48] анализируется алгоритм обнаружения КА на компьютерные сети, базирующийся на оценке самоподобия аномалий в сетевом трафике с использованием статистических методов. Алгоритм состоит из трех этапов, в рамках которых выполняются анализ свойства самоподобия для эталонного трафика, анализ фрактальных свойств реального трафика и дополнительной обработки временных рядов статистическими методами на заключительном этапе. Программная реализации предложенного подхода подтвердила высокую эффективность предложенного алгоритма обнаружения КА в реальном времени.

В [49] предложено использовать для обнаружения аномальных выбросов в системах передачи данных метод машинного обучения, основанный на применении гибридной искусственной нейронной сети, состоящей из автокодировщика

(autoencoder) и классификатора. Экспериментальная оценка предлагаемой методики подтвердила ее достаточно высокую эффективность.

В [50] представлен метод выявления аномалий сетевого трафика, основанного на утверждении о том, что сетевой трафик является самоподобной структурой и моделируется фрактальным броуновским движением. В качестве инструментов при разработке данного метода были применены фрактальный анализ и математическая статистика. Проведен анализ существующих методов выявления сетевых аномалий на предмет их недостатков. Результатом работы является модифицированный метод выявления аномалий сетевого трафика. Данный метод относится к полуконтролируемой методике обнаружения аномалий, что позволяет процессу быть практически автономным от человеческого вмешательства. Алгоритм поиска аномалий, лежащий в основе метода, может применяться как для поиска входящих аномалий (сетевых атак), так и для поиска аномалий в исходящем трафике (DLP-системы).

В [51] на основании анализа обширных экспериментальных исследований показано, что существующие модели трафика в современных сетях связи должны отражать не только самоподобные свойства, но и мультифрактальные характеристики этих потоков трафика. Кроме того, структура этих моделей должна учитываться в алгоритме прогнозирования трафика, который выигрывает от более точного моделирования трафика.

В [52] мультифрактальные свойства трафика магистральных сетей Интернета анализируются на основе вычисления функции мультифрактального спектра над временными рядами, сформированными из различных параметров трафика: IP-адреса отправителя и получателя; порты отправителя и получателя; временная метка; размер сетевого пакета; число сетевых пакетов в потоке; тип сетевого протокола транспортного уровня; число сетевых пакетов протоколов каждого типа; • число исходящих и входящих подключений для хост и т.д.

Данный список может быть расширен. Кроме того, выделенные значения в дальнейшем подвергаются статистической обработке для получения таких параметров, как среднее/максимальное/минимальное число пакетов, размер пакета

и т. д. Все вышеописанные параметры необходимы для контроля поведения сетевого трафика, именно эти параметры формируют временные ряды, над которыми вычисляются мультифрактальные эвристики.

В работах [53, 54] предложено использовать мультифрактальный анализ для выявления в трафике магистральных сетей аномалий, свидетельствующих о сетевых неполадках или атаках. В качестве метрик безопасности применены значения характеристик мультифрактального спектра. Эффективность предложенного подхода подтверждена экспериментальными данными по обнаружению атак отказа в обслуживании.

Вместе с тем во всех указанных работах в качестве основного рассматривались традиционные асимптотические методы оценки ФР. Однако используя методы текущей оценки ФР в скользящем окне в реальном масштабе времени можно усовершенствовать рассмотренные алгоритмы.

В [55, 56] рассматривается метод обнаружения аномалий трафика на основе кратномасштабного мультифрактального анализа путем контроля за скачками фрактальной размерности в режиме реального времени. Анализируемый метод базируется на текущей оценке мультифрактальных свойств трафика с помощью скользящего окна и кратномасштабном вейвлет-анализе. Полученные численные данные позволяют сделать вывод, что использование ФР для различных составляющий мультифрактального спектра позволяют с высокой достоверностью зафиксировать наличие аномалии. Учет подобных составляющих мультифрактального спектра может быть реализован, например путем построения многоканального алгоритма, каждый канал которого ориентирован на соответствующую составляющую мультифрактального спектра.

1.4.2 Методы оценки ФР

R/S-статистика. В задачах фрактального анализа для количественной оценки самоподобия процесса широко используется показатель Херста H. Его значения интерпретируются следующим образом: H близкий к 1 указывает на

выраженные фрактальные (долговременные) зависимости, тогда как при H=0,5 признаки самоподобия отсутствуют [57]. Одним из наиболее применимых способов оценки H H является R/S-статистика (rescaled range, «нормированный размах») [58]. Для вычисления показателя Херста H необходимо определить разность между максимальным и минимальным значениями ряда (R) и стандартное отклонение (S):

$$R = \max_{1 \le u \le N} \sum_{i=1}^{u} \left(x_i - X_{\text{ср}}\right) - \min_{1 \le u \le N} \sum_{i=1}^{u} \left(x_i - X_{cp}\right)$$

$$S = \sqrt{\frac{1}{N} \sum_{i=1}^{u} \left(x_i - X_{cp}\right)^2},$$

где $X_{cp} = \frac{1}{N-1} \sum_{i=1}^{N} x_i$ – среднее арифметическое ряда наблюдений за N периодов.

Оценку показателя Херста получают из зависимости нормированного размаха R/S от длины окна N и задается формулой

$$H = \log \frac{R/S}{\log\left(aN\right)},$$

где α — заданная константа, α > 0.

Практическая применимость коэффициента Херста для диагностики сетевых состояний подтверждена в [59, 60]. В частности, показано, что до проведения атаки отказа в обслуживании на один из компонентов системы значение H составляло 0,81, что соответствует наличию выраженных самоподобных свойств во временном ряду. Во время атаки H снижалось до 0,33, что интерпретируется как утрата самоподобия и, следовательно, как индикатор аномального режима работы.

Метод кратномасштабного анализа. Вейвлет-коэффициенты, полученные в результате анализа, представляют иерархическую структуру колебаний сигнала, и наличие локальных максимумов в распределении коэффициентов свидетельствует о дроблении масштаба, что в свою очередь указывает на самоподобие исследуемого сигнала (в случае компьютерных сетей — сетевого трафика) [61]. Более того, аномальные скачки в фрактальной размерности могут служить индикатором возможного воздействия компьютерных атак, позволяя

обнаружить атаки и принять соответствующие меры по обеспечению информационной безопасности.

Из совокупности исходных условий кратномасштабного анализа следует, что перевод сигнала из пространства V_{m+1} с более высоким разрешением в пространство V_m, по существу, представляет собой нормированную децимацию сигнала - двукратное прореживание, с соответствующим уменьшением в 2 раза числа отсчетов сигнала. Это эквивалентно низкочастотной фильтрации сигналов $\bar{\bar{x}}_{m+1}(k) \in V_{m+1}$ оператором h_k с частотой среза, равной половине от наивысшей частоты сигналов $\bar{\bar{x}}_{m+1}(k)$, с автоматическим сокращением (за счет прореживания) главного частотного диапазона децимированного сигнала $\bar{\bar{x}}_m(k)$ в 2 раза. Процедура имеет вполне конкретный физический смысл разделения спектров сигналов (и самих сигналов при их восстановлении из спектров) на низкочастотную $V_{m-1}(w)$ и высокочастотную W_{m-1} части.

Для исключения потерь высокочастотной информации, которая может потребоваться при восстановлении сигнала, она должна "переводиться" и сохраняться в новые подпространства W_m, ортогональные подпространствам V_m, такие, что $V_{m+1} = V_m \oplus W_m$. Подпространства W_m называются детализирующими в том смысле, что именно они содержат ту дополнительную информацию (не пересекающуюся с пространством V_m), необходимую для повышения уровня разрешения сигнала с V_m на V_{m+1} при его восстановлении.

Таким образом выполняя многомасштабный анализ для сигнала $X(t)$, обозначающего последовательность проекций его в каждом аппроксимирующем подпространстве V_j можно записать $approx_j(t) = \left(Proj_{V_j} x\right)(t) = \sum_k a_x(j,k)\varphi_{j,k}(t)$.

Поскольку $V_j \subset V_{j-1}$, то $approx_j$ является более грубой аппроксимацией X, чем $approx_{j-1}$. По этой причине, ключевая идея ММА заключается в рассмотрении потерь информации заключенной в деталях, при переходе от одной аппроксимации к следующей, более грубой $detail_j(t) = approx_{j-1}(t) - approx_j(t)$.

ММА показывает, что детали сигнала $detail_j$ могут быть получены непосредственно из отображения $X(t)$ на подпространство, W_j, называемое вейвлет подпространством. Более того, теоретически ММА показывает, что существует функция ψ_0, называемая материнским вейвлетом, производная от φ_0, такая что ее образец $\{\psi_{j,k}(t) = 2^{-j/2}\psi_0(2^{-j}t - k), k \in Z\}$ составляет базис Рисса для W_j. Так что $detail_j(t) = \left(Proj_{W_j}x\right)(t) = \sum_k d_x(j,k)\psi_{j,k}(t)$,

Как известно, любой базис Рисса является безусловным базисом, то есть остается базисом после любой перестановки элементов. В результате ММА заключается в перезаписывании информации в $X(t)$, согласно собранным деталям с различной степенью детализации (разрешением) и аппроксимации низкого разрешения

$$x(t) = approx_J(t) + \sum_{j=1}^{j=J} detail_j(t) = \sum_k a_x(J,k)\varphi_{J,k}(t) + \sum_{j=1}^{J}\sum_k d_x(j,k)\psi_{j,k}(t) \qquad (1.6)$$

Коэффициенты аппроксимации $a_x(j,k)$ и детализации $d_x(j,k)$ определяются скалярными произведениями со скейлинговой функцией $\varphi_{J,k}(t)$ и материнским вейвлетом $\psi_{j,k}(t)$ соответственно. Таким образом, в соответствии с положениями вейвлет-анализа временной ряд $X(t)$ может быть представлен в виде

$$X(t) = X_J(t) + \sum_{j=1}^{J} D_j(t), \qquad (1.7)$$

где $X_j(t) = \sum_{k=0}^{n_0/2^J-1} a_{j,k}\varphi_{J,k}(t)$ – функция начальной аппроксимации, соответствующая масштабу J $(J < J_{max}), a_{J,k} = \langle X(t), \varphi_{J,k}\rangle$ – масштабный коэффициент аппроксимации, равный скалярному произведению исходного ряда $V(t)$ и масштабной функции «самого грубого» масштаба J, смещенной на k единиц масштаба вправо от начала координат; $D_j(t) = \sum_{k=0}^{n_0/2^J-1} d_{j,k}\psi_{J,k}(t)$ – функция детализации -го масштаба, $d_{j,k} = \langle X(t), \psi_{j,k}\rangle$ – вейвлет-коэффициент детализации масштаба j, равный скалярному произведению исходного ряда $X(t)$ и вейвлета масштаба j, смещенного на k единиц масштаба вправо от начала координат. Здесь $n_0 = 2^{J_{max}}, (n_0 \le N)$, а $J_{max} = [\log_2 N]$ – максимальное число масштабов разложения; $[\log_2 N]$ – целая часть числа $[\log_2 N]$. Значение индекса масштаба $j =$

0 соответствует случаю максимального разрешения – самой точной аппроксимации, которая равна исходному ряду $X(t)$, состоящему из n_0 отсчетов. С увеличением j $(0 < j \leq J_{max})$ происходит переход к более грубому разрешению.

Пусть $\{X(ti), \overline{i = 1, N}\}$ будет дискретным случайным процессом, определенным на интервале $i = 1 \ldots N$ и пусть разложение трафика по вейвлет коэффициентам осуществляется в скользящем окне размера N. Смещение окна анализа осуществляется с шагом $\Delta \leq N$. В результате при смещении окна анализа слева направо положение окна пробежит m положений $M = \frac{N}{\Delta}, m = \overline{1, M}$. Тогда вейвлет-коэффициенты детализации при m -ом положении окна $d_{j,k}^{m}$ могут быть найдены в конце анализируемого интервала.

Как показано в [62] для оценки фрактальной размерности при m -ом положении окна необходимо оценить среднее квадратов коэффициентов детализации $M\left|d_X^{(m)}(j,k)\right|^2$ по однократной реализации трафика конечной длины N_0. Здесь M [.] - операция нахождения второго центрального момента. Если длина выборки $X(t)$ анализируемая в окне равна N_0, тогда доступное число вейвлет-коэффициентов в октаве j равно $n_j = 2^{-j}N_0$. С учетом стационарности и слабой статистической зависимости вейвлет коэффициентов оценку совокупного среднего можно проводить по частному (временному) среднему

$$\mu_{j,m} = M\left[d_{j,k}^{2(m)}\right] \approx \frac{1}{n_j}\sum_{k=1}^{n_j}\left|d_{j,k}^{(m)}\right|^2, m = \overline{1, M} \qquad (1.8)$$

Коэффициент $\left|d_x^{(m)}(j,k)\right|^2$ измеряет величину энергии в анализируемом сигнале в окне с номером m относительно момента времени $2^j k$ и частоты $2^{-j}v_0$, где v_0 является случайной опорной частотой задаваемой функцией ψ_0.

Для нахождения текущей оценки параметра Херста $\widehat{H}_m$ при m -ом положении окна анализа необходимо выполнить линейную регрессию на шкале j в диапазоне $[j_1, j_2]$ в соответствии с уравнением

$$\log_2(\mu_{j,m}) = \log_2\left(\frac{1}{n_j}\sum_k \left|d_x^{(m)}(j,k)\right|^2\right) = \left(2\widehat{H}_m - 1\right)j + \widehat{c} == \alpha_m j + \hat{c}, \quad (1.9)$$

где $\hat{c} = const.$

Формула (3) описывает возможный способ оценки показателя Херста ДВЗ-процессов в виде линейной зависимости.

Это означает, что, если процесс $\{x_i, i = \overline{1, N_0}\}$ является долговременно зависимым процессом с показателем Херста H_m, то график зависимости $\log_2(\mu_{j,m})$ от j, называемый логарифмической диаграммой (LD), имеет линейный наклон $2\widehat{H_m} - 1$, и масштабный показатель $\hat{\alpha}_m = (2\widehat{H_m} - 1)$ может быть получен путем оценки наклона графика функции $\log_2(\mu_{j,m})$ от j при каждом m-м положении окна анализа.

1.4.3 Мультифрактальный спектр фрактальной размерности (МСФР)

Мультифракталы — это неоднородные фрактальные объекты, для полного описания которых, в отличие от обычных фракталов, недостаточно введения всего лишь одной величины — его фрактальной размерности (D или H) необходим целый спектр таких размерностей, число которых неограничено.

Большинство реальных процессов обладает мультифрактальной структурой, что означает, что они сохраняют свои характеристики на более коротких временных интервалах. Каждый такой интервал времени обладает своим фрактальным алгоритмом, отличающимся от алгоритма других интервалов времени [63-65]. С учетом этого, для оценки самоподобия рекомендуется использовать мультифрактальные модели [66]. Масштабная инвариантность указывает на то, что процессы развиваются похожим образом на различных временных интервалах, а сетевой трафик обладает свойствами самоподобия. Однако, динамика этих характеристик отличается при рассмотрении малых и больших временных интервалов. Мультифрактальные свойства проявляются через мультифрактальный спектр Лежандра и показатель Гельдера, изменение которых во времени позволяет

отслеживать изменения в мультифрактальных характеристиках процессов. В [63] утверждается, что функция f имеет локальный показатель Гельдера $\alpha \geq 0$ в точке ϑ тогда, когда существует константа $K \geq 0$ и полином p_ϑ порядка $m = \alpha$ такой, что $\forall t \in R: |f(t) - p_\vartheta(t)| \leq K|t - \vartheta|^\alpha$. В графическом представлении, мультифрактальный процесс может быть описан с помощью мультифрактального спектра. В работе [56] авторы исследуют изменения характеристик спектра сетевого трафика во время атаки DoS (Denial of Service - атака на отказ в обслуживании). Они обнаружили изменения в ширине мультифрактального спектра и правой "ветви" спектра, которая отвечает за незначительные флуктуации.

Такая ситуация заставляет заняться поиском новых количественных характеристик подобных процессов.

Определение. [41,67] Стохастический процесс *X(t)* называется мультифрактальным, если он обладает стационарными приращениями и удовлетворяет неравенству $M[|X(t)|^q] = C(q)t^{\tau(q)+1}$ для некоторого положительного $q \in Q, [0,1] \subset Q$, где $\tau(q)$ — масштабная или скейлинговая функция (функция разбиения) и моментный коэффициент C(q) не зависит от t.

Для характеристики мультифрактального множества часто используют функцию мультифрактального спектра *f(α)* характеризующую спектр сингулярностей мультифрактала для переменной *α*, которая является показателем Липшица-Гельдера и имеет смысл меры сингулярности.

В результате мультифрактальный спектр $f_L(a)$ находится преобразованием Лежандра от функции разбиения $\tau(q)$*:*

$$f_L(a) = \inf_{q \in R}\big(aq - \tau(q)\big). \quad (1.10)$$

Таким образом мультифрактальный спектр $f_L(a)$ представляет собой меру «частоты» показателя сингулярности *α(t)* к моменту времени *t* и показывает вероятность определенного значения показателя сингулярности $\tau(q) \leq inf_a\big(qa - f_L(a)\big)$.

Сам по себе расчет спектра сингулярности дает исследователю сравнительно мало информации об исследуемом временном ряде. Гораздо больше информации

можно получить при изучении динамики его спектра сингулярности с помощью скользящего окна.

Изменение спектра сингулярности может свидетельствовать об изменении характера исследуемых процессов, которое может быть невидимо как для традиционных методов, так и для фрактального анализа, основанного на расчете только показателя Херста.

Поэтому далее явления будут рассматриваться именно с точки зрения динамики мультифрактальных характеристик трафика при нормальном функционировании КС и при возникновении аномалий или сетевых атак.

1.5 Постановка цели и задач исследования

Фрактальный анализ в обнаружении атак - является математическим подходом к анализу сложных структур и данных. Он основан на концепции самоподобия, которая описывает повторяющиеся шаблоны и закономерности в данных. В контексте обнаружения атак фрактальный анализ может использоваться для анализа трафика в сети и выявления необычных или аномальных паттернов. Он позволяет выделить фрактальные признаки, такие как фрактальные размерности и спектры, которые могут быть использованы в дальнейшем анализе и обнаружении атак.

Композиция методов машинного обучения и фрактального анализа представляет собой перспективный подход для повышения эффективности обнаружения атак. В данном подходе фрактальный анализ может быть использован для извлечения дополнительной информации из данных, которая может быть недоступна для классических методов машинного обучения. Фрактальные признаки могут быть включены в процесс обучения моделей машинного обучения, что позволяет улучшить их способность к обнаружению атак и снизить вероятность ложных срабатываний.

Преимущества комбинированного подхода заключаются в следующем:

- **Повышение точности обнаружения:** Комбинирование машинного обучения и фрактального анализа позволяет объединить сильные стороны обоих подходов, что приводит к более точному и эффективному обнаружению атак.
- **Снижение ложных срабатываний:** Включение фрактальных признаков в процесс обучения моделей машинного обучения позволяет снизить вероятность ложных срабатываний, так как фрактальный анализ способен выявлять скрытые структуры в данных, которые могут указывать на атаки.
- **Адаптивность к новым типам атак:** Комбинированный подход обладает большей гибкостью и адаптивностью к новым типам атак, так как и машинное обучение, и фрактальный анализ могут быть обновлены и обучены на новых данных, что позволяет обнаруживать ранее неизвестные угрозы.

Комбинация машинного обучения и фрактального анализа представляет собой многообещающий подход для повышения эффективности обнаружения атак в компьютерных сетях. Объединение этих методов позволяет выявлять сложные и скрытые атаки, повышать точность обнаружения и снижать вероятность ложных срабатываний. Дальнейшие исследования и эксперименты в этой области могут привести к разработке более эффективных систем обнаружения атак и обеспечению безопасности сетей.

В связи с изложенным

Целью работы *является повышение качества классификации компьютерных атак в компьютерных сетях с помощью комбинации мультифрактального анализа и машинного обучения.*

Достижение поставленной цели предусматривает решение **частных задач:**

1. Анализ объекта с позиции предмета исследований.
2. Разработка улучшенной модели оценки фрактальных свойств компьютерных атак в онлайн-режиме методами вейвлет-анализа.
3. Разработка метода повышения эффективности алгоритмов обнаружения/классификации атак в компьютерных сетях методами машинного обучения при условии дополнительной информации о фрактальных свойствах атак и сетевого трафика.

4. Разработка модели алгоритмической и численной оценки мультифрактальных свойств сетевого трафика и компьютерных атак.

5. Разработка метода композиции машинного обучения и мультифрактального анализа сетевого трафика для улучшения многоклассовой классификации компьютерных атак.

ГЛАВА 2 Оценка фрактальной размерности компьютерных атак

2.1 Кратномасштабный анализ сетевого трафика

Обеспечение сетевой безопасности в условиях воздействия сетевых атак является важной проблемой современных систем связи. Проблема обнаружения КА обусловлена трудностью выбора математического аппарата или же алгоритма. Большинство из известных методов достаточно трудны в программной реализации и имеют ряд недостатков, связанных с недостоверным определением момента начала аномалии.

В работах [56,68] получены алгоритмы обнаружения сетевых атак на основе анализа скачков фрактальной размерности при резких измерениях свойств сетевого трафика. Однако полученные при этом алгоритмы не являются итеративными, что усложняет использование их в процессе обработки. Кроме того, наблюдаемые при этом флуктуации текущего показателя Херста H могут рассматриваться как дополнительный шум обработки, что также снижает эффективность таких алгоритмов.

Традиционные методы анализа временных рядов [69] основаны на процедуре сглаживания, что влечет существенную потерю информации. Сложная форма локальных особенностей также делает неэффективными методы спектрального анализа. Эффективным методом для описания таких временных рядов является вейвлет-преобразование [70]. В процессе создания систематизированной теории вейвлет-преобразования построены ортонормированные регулярные вейвлет-базисы с компактными носителями и разработаны кратномасштабные аппроксимирующие схемы сигнала, что послужило широкому распространению вейвлет-преобразования в различные сферы деятельности. В то же время качество работы конечных систем, основанных на вейвлет-преобразовании, определяется технологией его применения. Существенную роль играет выбор вейвлет-функции,

конструкции разложения временного ряда, процедура построения аппроксимирующего базиса и др.

Как известно [71-73] при конечном числе уровней разложения P, любую последовательность дискретных отсчетов анализируемого процесса $y(t_i)$ можно представить в виде упорядоченной совокупности коэффициентов разложения по системе масштабирующих функций и вейвлет-функций:

$$y(t_i) = \sum_{k=1} a_{m,k}\varphi_{m,k}(t_i) + \sum_{m=1}\sum_{k=1} d_{m,k}\psi_{m,k}(t_i), \quad m,k \in I, \tag{2.1}$$

где $\varphi_{m,k}(t_i)$ – базисная масштабирующая функция; $\psi_{m,k}(t_i)$ – материнская вейвлет-функция; $a_{m,k}, d_{m,k}$ −аппроксимирующие и детализирующие коэффициенты; m,k – параметры масштаба и сдвига в пространстве целых чисел I. Для адаптации соотношения (1) к обработке сигнала в реальном времени фиксируем длительность скользящего окна размером M.

Выполняя ДВП для выборок внутри выбранного окна, размер которого равен длительности бита в Mотсчетов, в каждый момент времени t_i, будем получать на некотором масштабном уровне jнабор коэффициентов аппроксимации $\{a_{1x},a_{2x},a_{3x}, \ ,a_{nx}\}_{t,j}$и детализации $\{d_{1x},d_{2x},d_{3x}, \ ,d_{nx}\}_{t,j}$. Причем количество коэффициентов n на уровне jв окне M будет определяться выражением $n = \frac{M}{2^j}$. Таким образом, в соответствии с положениями вейвлет-анализа [9] временной ряд $y(t)$ может быть представлен в виде

$$y(t) = y_J(t) + \sum_{j=1}^{J} D_j(t), \tag{2.2}$$

где $y_J(t) = \sum_{k=0}^{\frac{n_0}{2^J}-1} a_{J,k}\varphi_{J,k}(t)$ − функция начальной аппроксимации, соответствующая масштабуJ $(J < J_{\max})$, $a_{J,k} = \langle y(t),\varphi_{J,k}\rangle$ −масштабный коэффициент аппроксимации, равный скалярному произведению исходного ряда $y(t)$ и масштабной функции «самого грубого» масштаба J, смещенной на k единиц масштаба вправо от начала координат;

$D_j(t) = \sum_{k=0}^{\frac{n_0}{2^J}-1} d_{j,k}\psi_{J,k}(t)$ – функция детализации j-го масштаба;

$d_{J,k} = \langle y(t), \psi_{j,k} \rangle$ – вейвлет-коэффициент детализации масштаба j, равный скалярному произведению исходного ряда $y(t)$ и вейвлета масштаба j, смещенного на k единиц масштаба вправо от начала координат. Здесь $n_0 = 2^{J_{\max}}, (n_0 \le N)$, а $J_{\max} = [\log_2 N]$ – максимальное число масштабов разложения; $[\log_2 N]$ – целая часть числа.

В отличие от известных работ предлагается модифицировать алгоритм обработки путем дополнительной фильтрации текущих оценок показателя Херста, что позволяет повысить точность текущей оценки фрактальной размерности, а также достоверность обнаружения аномалии в сетевом трафике в режиме online.

2.2 Модифицированный алгоритма оценки фрактальной размерности

2.2.1 Оценка фрактальной размерности методом кратномасштабного анализа

Пусть $X(t_i)$ будет дискретным случайным процессом, определенным на интервале $i = 1,...,N$, и пусть разложение трафика по вейвлет-коэффициентам осуществляется в скользящем окне размера M. Смещение окна анализа осуществляется с единичным шагом. В результате при смещении окна анализа слева-направо оно «пробежит» m положений $m = 1,...,N-M$. Тогда вейвлет-коэффициенты детализации при m-м положении окна $d_{j,k}^m$ могут быть найдены в конце анализируемого интервала.

Как показано в [74, 75, 76] для оценки фрактальной размерности при m -ом положении окна необходимо оценить среднее квадратов коэффициентов детализации $M\left|d_X^{(m)}(j,k)\right|^2$ по однократной реализации трафика конечной длины N_0. Здесь M [.] - операция нахождения второго центрального момента. Если длина

выборки $X(t)$ анализируемая в окне равна N_0, тогда доступное число вейвлет-коэффициентов в октаве j равно $n_j = 2^{-j} N_0$. С учетом стационарности и слабой статистической зависимости вейвлет коэффициентов оценку совокупного среднего можно проводить по частному (временному) среднему

Для нахождения текущей оценки параметра Херста $\widehat{H}_m$ при m-ом положении окна анализа необходимо выполнить линейную регрессию на шкале j в диапазоне $\left[j_1, j_2\right]$ в соответствии с уравнением

$$\log_2\left(\mu_{j,m}\right) = \log_2\left(\frac{1}{n_j}\sum_k \left|d_x^{(m)}(j,k)\right|^2\right) = \left(2\widehat{H}_m - 1\right)j + \widehat{c} = \alpha_m j + \widehat{c}, \tag{2.3}$$

где $\widehat{c} = const$.

Коэффициент $\left|d_x^{(m)}(j,k)\right|^2$ измеряет величину энергии в анализируемом сигнале в окне с номером m относительно момента времени $2^j k$ и частоты $2^{-j} v_0$, где v_0 является случайной опорной частотой задаваемой функцией ψ_0.

Формула (3) описывает способ оценки показателя Херста $\widehat{H}_m$ для процессов с долговременной зависимостью в виде линейной зависимости. Это означает, что, если процесс $X\left(t_i\right)$ является долговременно зависимым процессом с показателем Херста H_m, то график зависимости $\log_2\left(\mu_{j,m}\right)$ от j, имеет линейный наклон $2\widehat{H}_m - 1$ и масштабный показатель $\hat{a}_m = (2\widehat{H}_m - 1)$ может быть получен путем оценки наклона графика функции $\log_2\left(\mu_{j,m}\right)$ от j при каждом m-м положении окна анализа.

Для нахождения взвешенной оценки масштабного показателя $\hat{a}_m$ на интервале $[j_1, j_2]$ при m-ом положении скользящего окна необходимо придерживаться следующей методики:

$$\widehat{a}_m = \sum_j w_j y_{j,m}, \tag{2.4}$$

$$\widehat{c}_m = \sum_j v_j y_{j,m}, \tag{2.5}$$

$$w_j = \frac{S_j - S_1}{\left(SS_2 - S_1^2\right)\sigma_j^2} \tag{2.6}$$

$$y_{j,m} = \log_2\left(\mu_{j,m}\right) - g(j), \tag{2.7}$$

$$g(j) = \psi\left(\frac{n_j}{2}\right)\ln 2 - \log_2\left(\frac{n_j}{2}\right) = \frac{\Gamma'\left(\frac{n_j}{2}\right)}{\left(\Gamma\left(\frac{n_j}{2}\right)\ln 2\right)} - \log_2\left(\frac{n_j}{2}\right) \sim -\frac{1}{n_j \ln 2}, \tag{2.8}$$

$$\sigma_j^2 = \frac{\xi\left(2, \frac{n_j}{2}\right)}{\ln^2 2} \sim \frac{2}{n_j \ln^2 2}, \tag{2.9}$$

$$v_j = \frac{S_2 - jS_1}{\left(SS_2 - S_1^2\right)\sigma_j^2}, \tag{2.10}$$

$$S = \sum_{j=j_1}^{j_2} 1/\sigma_j^2, S_1 = \sum_{j=j_1}^{j_2} j/\sigma_j^2, S_2 = \sum_{j=j_1}^{j_2} j^2/\sigma_j^2, \tag{2.11}$$

Где $\Gamma(x) = \int_0^\infty t^{x-1}e^{-t}dt$, Γ - гамма-функция, Γ' - является ее производной, $\xi(2,z) = \sum_0^\infty 1/(z+n)^2$ - обобщенная зета-функция Римана; $\psi(x) = \Gamma'(x)/\Gamma(x)$ — пси-функция (также называемая дигамма-функцией); n_j - количество коэффициентов-детализации на соответствующем уровне декомпозиции (j).

Таким образом, предварительно определив квантили S, S_1 и S_2 и получив взвешенную оценку $\widehat{a}$ для a:

$$\widehat{a}_m = \frac{\sum_{j=j_1}^{j_2} y_{j,m}\left(S_j - S_1\right)/\sigma_j^2}{SS_2 - S_1^2}, \tag{2.12}$$

которая является не смещенной на интервале $\left[j_1, j_2\right]$.

Соответственно, текущее значение параметра Херста $\widehat{H}_m$ в позиции m окна анализа описывается следующим соотношением:

$$\widehat{H}_m = \frac{1+\widehat{a}_m}{2},\ m=\overline{1,M}. \tag{2.13}$$

Используя формулы (2.4)…(2.12) и соотношение (2.13) для оценки параметра Херста в m-положении скользящего окна, можно преобразовать в следующее соотношение:

$$\widehat{H}_m = \frac{1}{2}\left[\frac{\sum_{j=j_1}^{j_2} S_j j\eta_{j,m} - \sum_{j=j_1}^{j_2} S_j j \sum_{j=j_1}^{j_2} S_j \eta_{j,m}}{\sum_{j=j_1}^{j_2} S_j \sum_{j=j_1}^{j_2} S_j j^2 - \left(\sum_{j=j_1}^{j_2} S_j j\right)} + 1\right], \tag{2.14}$$

где

$$\eta_{j,m} = \log_2\left(\frac{1}{n_j}\sum_k \left|d_x^{(m)}(j,k)\right|^2\right),$$

и весовой коэффициент $S_j = \left(n \ln^2 2\right)/2^{j+1}$ является обратной функцией теоретической асимптотической дисперсии.

Формула (2.13) является обобщением известных результатов на случай скользящего окна анализа и позволяет в отличие от [41] вычислять текущую оценку, а не установившееся значение параметра Херста.

Поскольку априори не известно, какое и на каких масштабах свойство масштабной инвариантности может существовать, если вообще существует, то на практике решение может быть принято при более низких отсечках октав для каждого предполагаемого режима масштабирования. Решение об этом принимается на основании результатов исследования логарифмической диаграммы при помощи доверительных интервалов. Полезная эвристика состоит в том, что линия регрессии должна ограничить каждый из доверительных интервалов в выбранном диапазоне $[j_1; j_2]$. Такой подход может быть нормализован, например, при использовании критерия согласия «хи-квадрат».

Логарифмическая диаграмма, основанная на дискретном вейвлет-преобразовании, может быть реализована при помощи быстрого пирамидального

алгоритма банка фильтров с очень низкой вычислительной сложностью порядка $O(n)$, где n – длина временного ряда. Этот алгоритм также имеет преимущества с точки зрения использования памяти при разделении данных на блоки, анализируемые и восстанавливаемые с минимумом вычислительных затрат.

Исследования статистических характеристик вейвлет коэффициентов, полученных в результате вейвлет-анализа реального трафика компьютерных сетей [41,45,75] показывают, что в достаточно общих случаях коэффициенты детализации $d_x(j,k)$ являются случайными Гаусовскими величинами. Другими словами, они получены вейвлет разложением процесса, который сам является Гаусовским.

В случае негауссовских процессов, реализация определителя сложнее. Тем не менее, в случае процессов с конечной дисперсией, значения $(1/n_j)\sum_k d_X(j,k)^2$ являются асимптотически Гауссовскими и можно показать, что корректирующие значения могут быть приведены к Гаусовскому случаю с помощью соотношений:

$$g(j) \sim -\frac{1+C_4(j)/2}{n_j log 2};$$

$$\sigma_j^2 \sim \frac{2}{\log^2 2}\frac{1+C_4(j)/2}{n_j},$$

где C_4 является нормализованным кумулянтом 4го порядка вейвлет коэффициентов на октаве j:

$$C_4(j) = \frac{Md_X(j,k)^4 - 3\left(Md_X(j,k)^2\right)^2}{\left(Md_X(j,k)^2\right)^2}.$$

Данные аналитические выражения зависят только от знания величины n_j и могут быть легко оценены на практике. Численные симуляции, описанные в [78-82] показывают, что для Гауссовских процессов эти аналитические расчеты являются хорошим приближением к реальным условиям.

2.2.2 Эффективность оценки $\hat{H}$:

Как известно, в присутствии долговременной зависимости стандартные оценки статистик второго порядка, вида $\left(1/n\sum_k x_k^2\right)$ такой например как дисперсия процесса X, имеют очень плохие статистические свойства, поскольку анализируемые данные являются сильно коррелированными [41,72,76,82,83].

В пространстве отображения вейвлет-коэффициентов для процесса с долговременной зависимостью с параметром H

$$Md_x(j,k)d_x\left(j,k^J\right)=O\left(\left|k-k^J\right|^{2H-2-2N}\right),\left|k-k^J\right|\to\infty.$$

Это отчетливо показывает, что корреляционная структура преобразованных данных, т.е. данные, представленные с помощью вейвлет коэффициентов, не является долговременно-зависимой при условии $N>H-1$, в противоположность долговременной зависимости, присутствующей в оригинальных данных.

Такое устранение корреляции в наборе анализируемых данных, полученных после вейвлет-анализа, позволяет использовать стандартные оценки дисперсии в виде $1/n_j\sum_k\left|d_x(j,k)\right|^2$. При гауссовских и квазидекоррелированных вейвлет коэффициентах, формула для дисперсии оценки H может быть получена в виде:

$$\sigma_H^2=var\hat{H}\left(j_1,j_2\right)=\frac{2}{n_{j_1}\ln^2 2}\frac{1-2^J}{1-2^{-(J+1)}\left(J^2+4\right)+2^{-2J}},$$

где $J=j_2-j_1$ является числом октав, вовлеченных в линейное сглаживание и $n_{j_1}=2^{-j_1}N_0$ является числом доступных коэффициентов в рамке j_1.

Из формулы для оценки дисперсии (2.9) в Гауссовском и асимптотическом приближении можно получить доверительный интервал

$$\hat{H}-\sigma_{\hat{H}}z_\beta\le H\le\hat{H}+\sigma_{\hat{H}}z_\beta,$$

где z_β представляет $1-\beta$ квантиль стандартного Гауссовского распределения, то есть $P\left(z\ge z_\beta\right)=\beta$. Все результаты, представленные ниже, и при числовом

моделировании, и на фактическом анализе данных, были подсчитаны при $\beta = 0.025$ (т.е. 95 % доверительный интервал), базируясь на вышеописанных гипотезах.

2.3 Оценка эффективности алгоритма оценки ФР с помощью тестовой последовательности

Оценку эффективности разработанного алгоритма оценим методом имитационного моделирования воспользовавшись эталонной псевдослучайной последовательность.

2.3.1 Моделирование тестовой последовательности со скачкообразным изменением ФР

Моделирование трассы сетевого трафика будем проводить путем моделирования ФГШ ($X_H(t)$).Процесс $X_H(t)$ является нормально распределенным - $N(0, \sigma|\delta|^H)$, с нормированной ковариационной функцией вида $r(\tau) = (|\tau + 1|^{2H}) - 2|\tau|^{2H} + |\tau - 1|^{2H})/2$.

Может быть показано, что $r(\tau) \sim H(2H-1)|\tau|^{2H-2}$ при $\tau \to \infty$, а также, что все объединенные процессы $X_H^m(t)$ имеют одинаковое распределение для всех $0 < H < 1$. Поэтому ФГШ является точно самоподобным процессом с параметров Херста H, изменяющимся в интервале $\frac{1}{2} < H < 1$.

Проведем моделирование ФГШ, используя математическую среду R-Environment. Для моделирования последовательности ФГШ воспользуемся методом $fgnSim()$, принимающим на вход такие параметры, как n – число элементов последовательности, H – значение параметра Херста в моделируемой последовательности. Среднее значение моделируемой выборки и среднеквадратическое отклонение по умолчанию задаются в 0 и 1 соответственно. Структура алгоритма представлена в Приложении Б.

Моделирование будем производить со следующими параметрами: $n = 50000, H = [0.7, 0.5, 0.8, 0.6, 0.9]$.

Получив 5 участков по 50000 значений, произведем их конкатенацию для получения результирующей последовательности. Так как отсчеты пакетов сетевого трафика в трассе должны быть неотрицательными, ко всем полученным при моделировании точкам ФГШ применим линейной преобразование (сложение с минимумом от смоделированной последовательности), что не отразится на ее корреляционной структуре (а тем самым и на приближении к ФГШ).

Трасса сетевого траффика, полученная в результате моделирования показана на рис. 2.1.

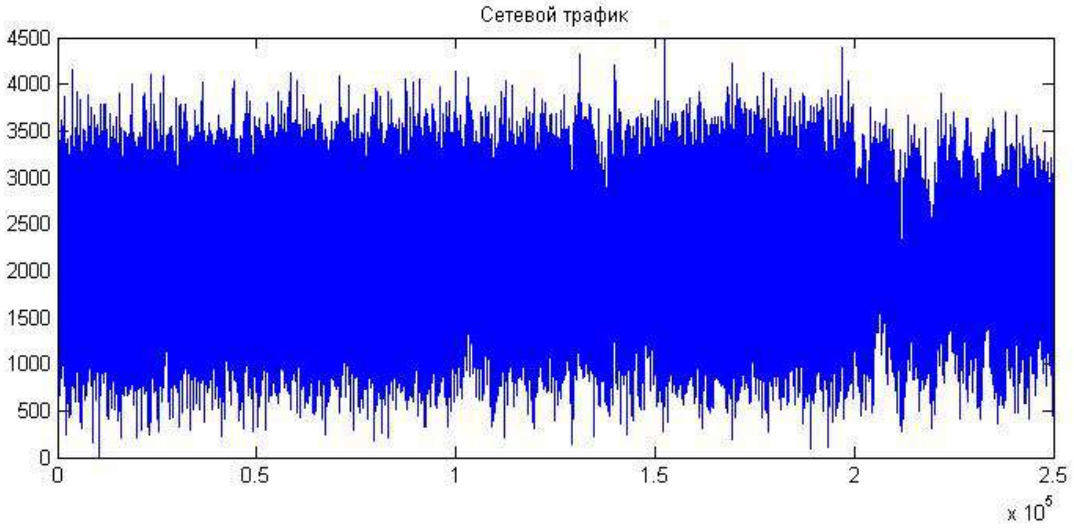


Рис.2.1 - Смоделированная трасса сетевого трафика. Процесс – ГДШ, длительность – 25000 выборок, параметр Херста: 0.7 в [0:50000], 0.5 в [50001:100000], 0.8 в [100001:150000], 0.6 в [150001:200000], 0.9 в [200001:250000]

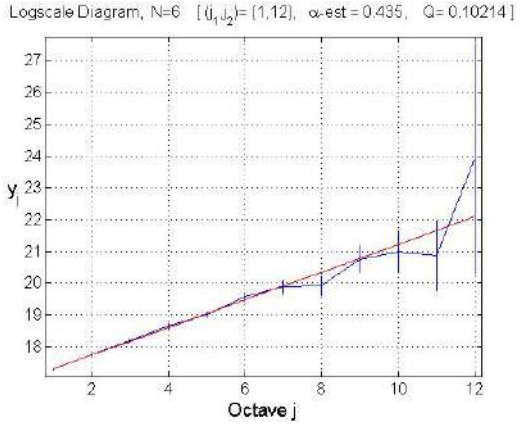
Для приведения ГДШ к виду, свойственному трассе сетевого трафика, к смоделированной последовательности было применено преобразование:
$X_{res} = Round((X_{FGN} + |Min(X_{FGN})|) \cdot 500)$.

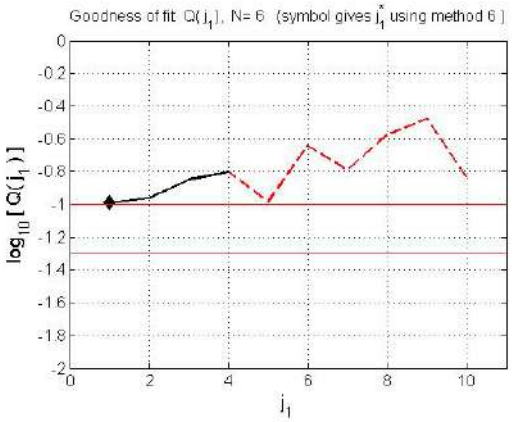
Для проверки правильности проведенного моделирования, а также для оценки промежутка масштабирования для дальнейшего анализа, применим ПО, разработанное в приложении Б.

Оценку параметра Херста будем производить для каждого промежутка (50000 элементов), входящего в смоделированную трассу. В качестве материнского вейвлета выберем $db6$. Начальным промежутком масштабирования выберем $[j_1, j_2] = [1, maxJ]$, где $maxJ = 12$ – максимальный уровень разложения вейвлетов $db6$ для последовательности с 50000 элементами.

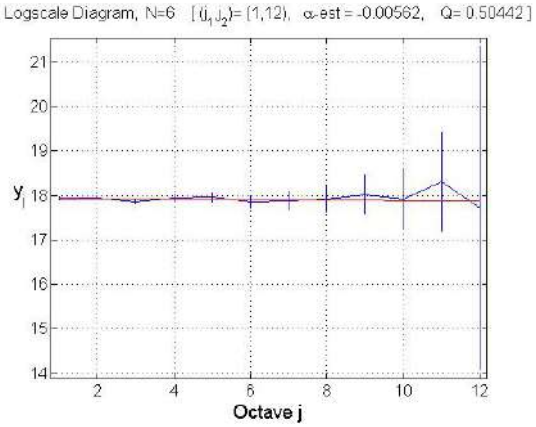
В результате оценки получаем:

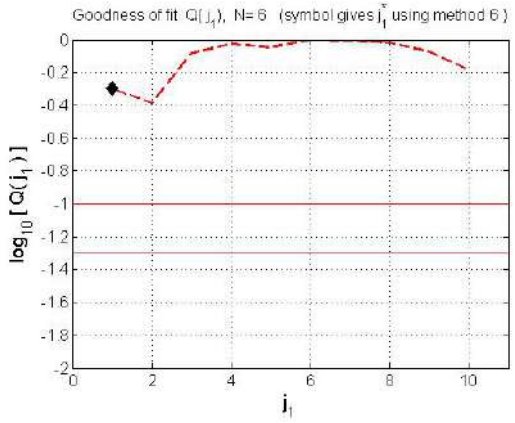
а)



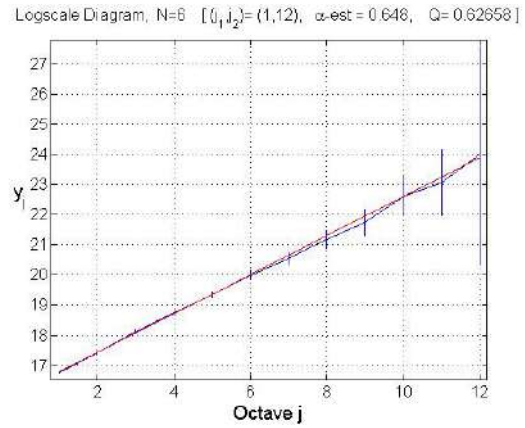


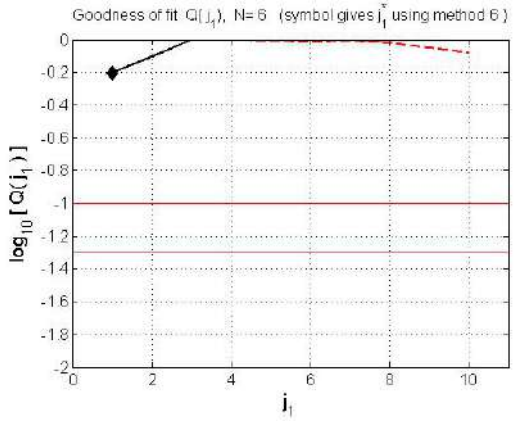
б)



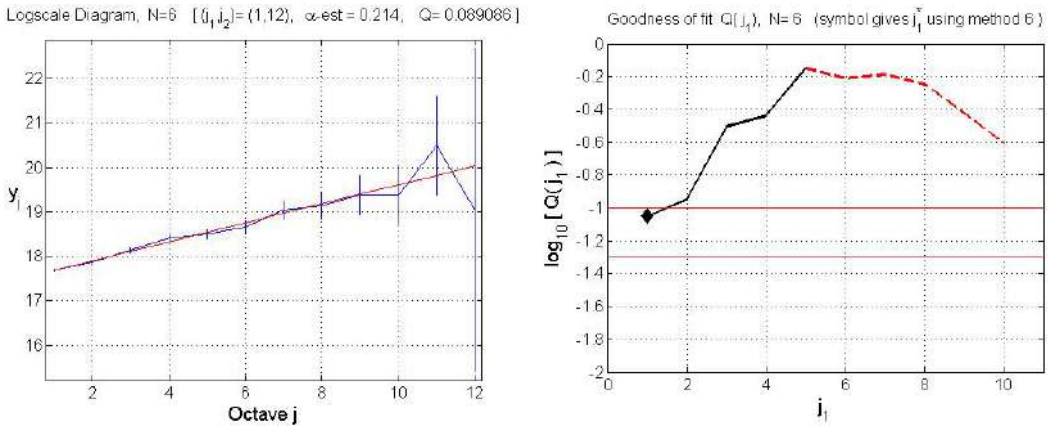


в)





г)



д)

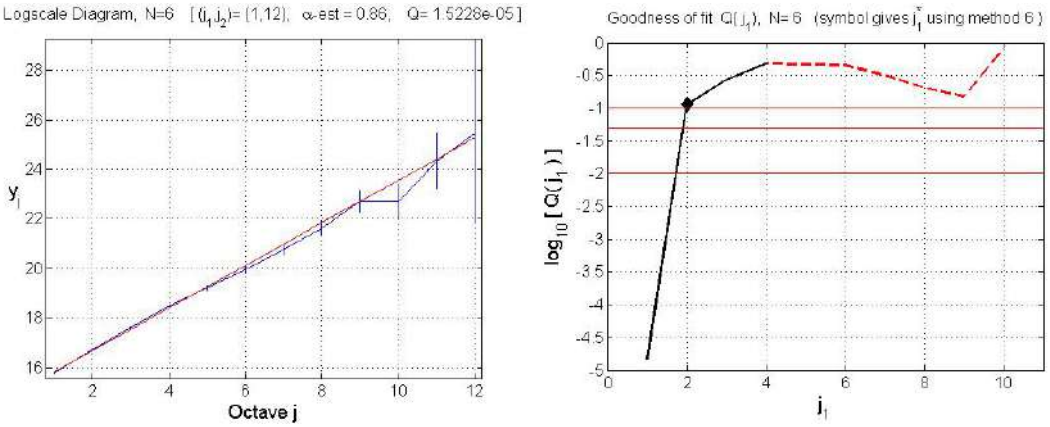


Рис. 2.2 — Результаты тестирования: а) $n = [1{:}\,50000]$, б) $n = [50001{:}\,100000]$, в) $n = [100001{:}\,150000]$, г) $n = [150001{:}\,200000]$, д) $n = [200001{:}\,250000]$

Зависимости, представленные на Рис. 2.2 свидетельствует о монофрактальности исследуемого процесса в пределах каждого из 5-ти рассматриваемых промежутков. Выбранные интервалы масштабирования начинаются с 1й октавы. Параметр Херста можно получить, используя соотношение (2.13): $H = \frac{\alpha+1}{2}$.

Результаты тестирования смоделированной трассы представлены в Табл. 2.1.

Таблица 2.1 — Результаты тестирования смоделированной трассы.

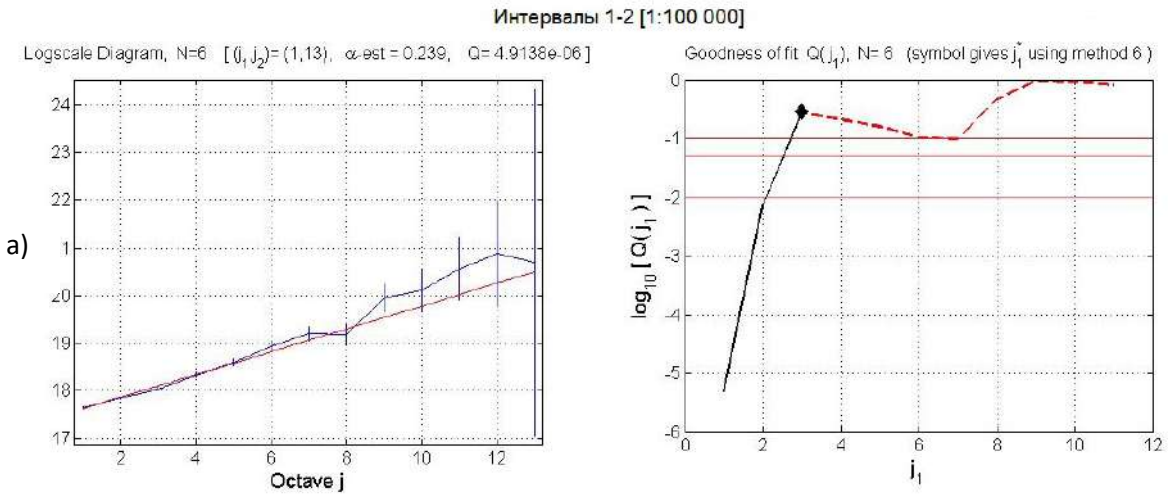
Интервал	**Выбранный промежуток масштабирования, $[j_1,j_2]$**	**α**	**Доверительный интервал, α**	**Параметр Херста, H**	**Доверительный интервал, H**
[1:50000]	[1:12]	0.43	[0.421, 0.448]	0.717	[0.711, 0.724]
[50001:100000]	[1:12]	-0.006	[-0.019, 0.007]	0.497	[0.491, 0.504]
[100001:150000]	[1:12]	0.64	[0.635, 0.661]	0.824	[0.818, 0.831]
[150001:200000]	[1:12]	0.21	[0.201, 0.227]	0.607	[0.600, 0.613]
[200001:250000]	[2:12]	0.86	[0.847, 0.873]	0.930	[0.924, 0.937]

Как можно видеть из табл.2.1, результаты тестирования подтверждают адекватность трассы, полученной путем имитационного моделирования требуемым параметрам для всех интервалов изменения параметра Херста с высокой точностью.

2.3.2 Оценка фрактальной размерности смоделированной трассы

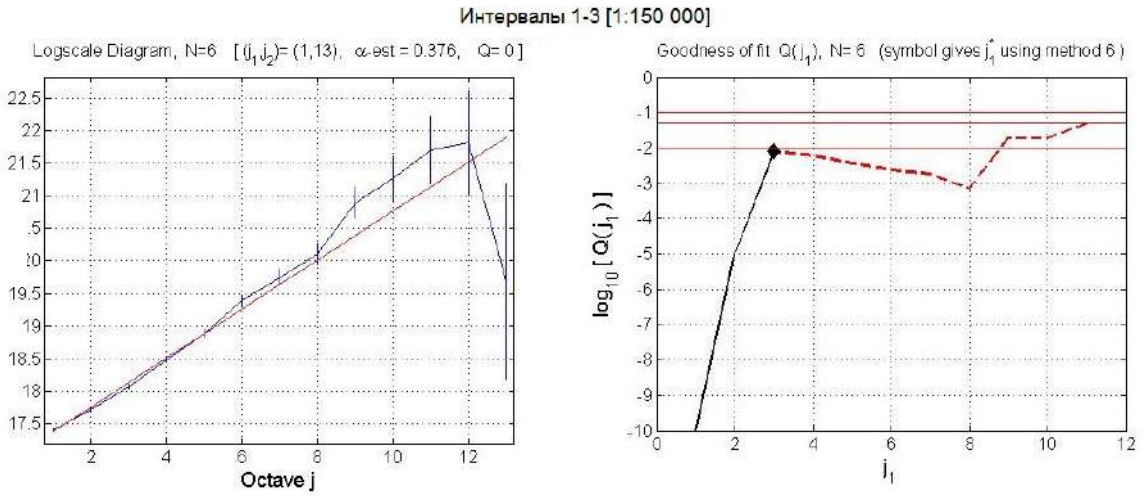
Результатом моделирования в пункте 2.2.1 было получение последовательности коэффициентов, образующих 5 временных интервалов с заданными значениями параметра H. Таким образом, на границе каждого интервала наблюдается скачкообразное изменение H.

В пункте 2.2.1 была проведена процедура тестирования фрактальной размерности каждого из смоделированных интервалов, в результате которой было подтверждено, что каждый из этих промежутков монофрактален. Для подтверждения факта изменения H для всей последовательности применим процедуру тестирования для объединений смежных смоделированных промежутков.

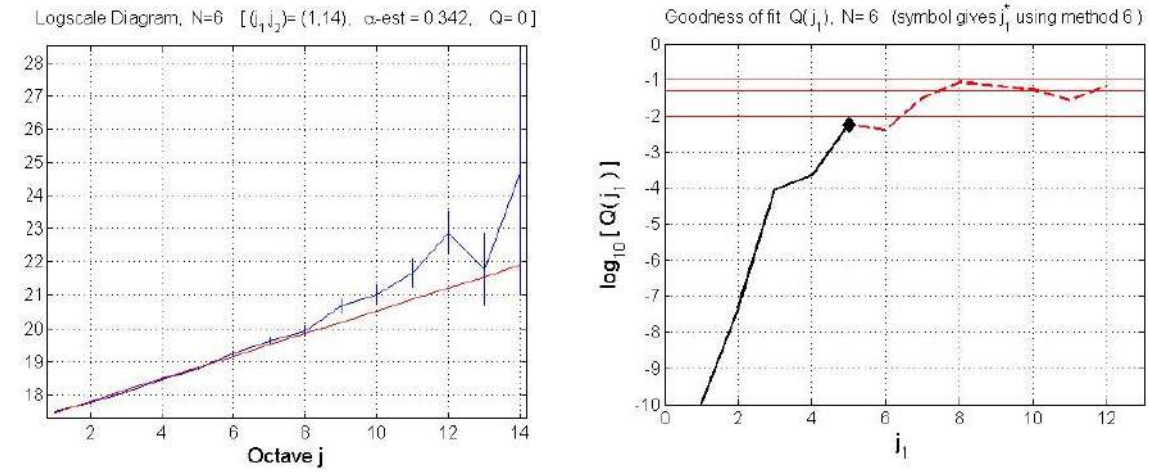


а)

б)



в)



г)

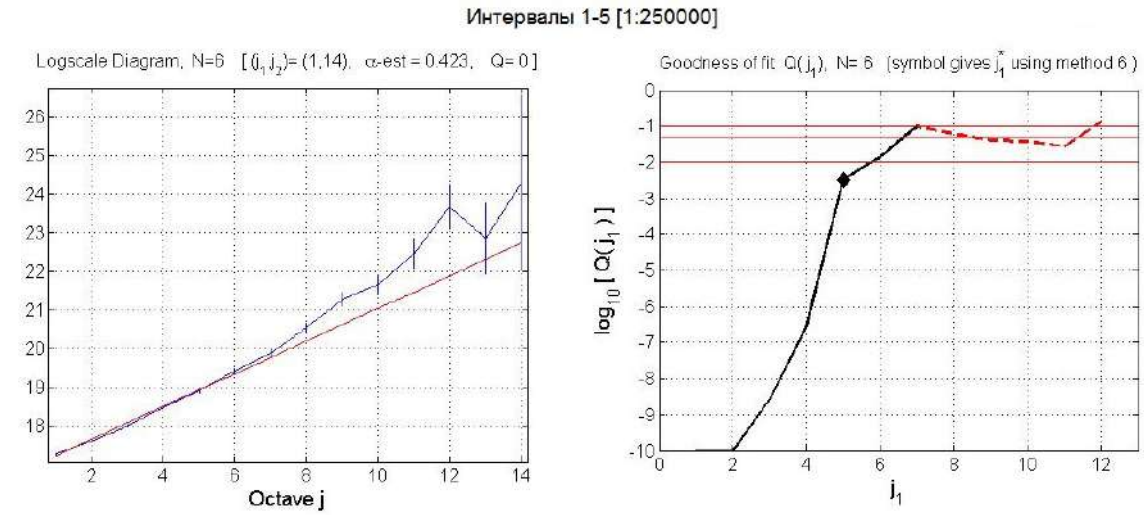


Рис. 2.3 - Результаты тестирования: а) $n = [1: 100000]$, б) $n = [1: 150000]$, в) $n = [1: 200000]$, г) $n = [1: 250000]$

Рисунок 2.3 свидетельствует о мультифрактальности для объединений смоделированных промежутков.

Таблица 2.2 - Результаты тестирования объединенных промежутков.

Интервал	**Выбранный промежуток масштабирования, $[j_1,j_2]$**	**α**	**Доверительный интервал, α**	**Параметр Херста, H**	**Доверительный интервал, H**
[1:100000]	[3:12]	0.239	[0.230, 0.248]	0.620	[0.615, 0.624]
[1:150000]	[3:12]	0.376	[0.369, 0.384]	0.688	[0.684, 0.692]
[1:200000]	[5:12]	0.342	[0.336, 0.348]	0.671	[0.668, 0.674]
[1:250000]	[5:12]	0.423	[0.417, 0.429]	0.712	[0.709, 0.714]

Как видно из таблицы 2.2, выбор интервала масштабирования начинается не 1й октавы, также как это наблюдается в результатах тестирования табл. 3.1, а с 3-й и 5й октав для разных рассматриваемых промежутков. Это объясняется присутствием мультифрактальности, в связи с чем, нижние уровни разложения отсекаются для проведения более детального анализа H.

2.3.3 Обнаружение скачков фрактальной размерности в реальном времени

Для решения задачи обнаружения аномалий в сетевом трафике в реальном времени рассмотрим метод скользящего окна. В качестве трассы сетевого трафика будем принимать сформированную на предыдущих шагах последовательность, а аномалиями являются изменение H. Задача обнаружения аномалий сводится к обнаружению скачков H.

Используя алгоритм расчета параметра H в реальном времени, будем вычислять коэффициенты H для каждого положения окна анализа как это представлено на рисунке 2.4.

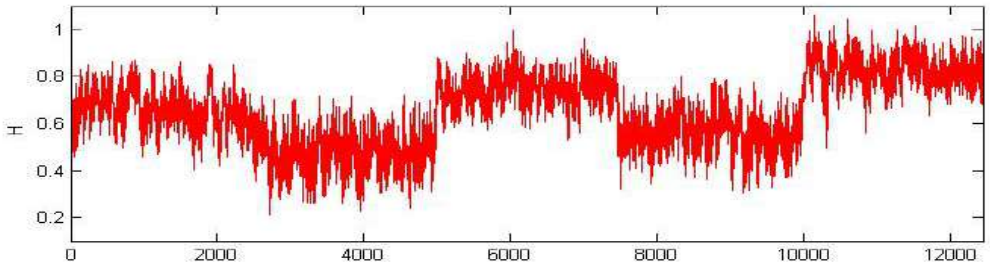


Рис. 2.4 - Последовательность коэффициентов параметра H, полученных при анализе, окно анализа $w = 1000$ коэффициентов, $\Delta t = 20$.

Для обнаружения скачков H требуется решить задачу вычисления пороговых значений H для времени t.

Вычисление адаптивных пороговых значений производится по следующему алгоритму:

1. *Возьмем окно анализа коэффициентов H размером w в положении* t_0, *как начальный интервал.*
2. *Возьмем фактор* $E = 0.94$
3. *Рассчитаем мат. ожидание M и СКО* σ *для взятого промежутка.*
4. *Рассчитаем* $\alpha = 2 \cdot \frac{\sigma}{M}$
5. *Рассчитаем* $\gamma_1 = (1 - \alpha) \cdot E$, $\gamma_2 = (1 + \alpha) \cdot E$
6. *Рассчитаем* $\delta_1 = (1 - \alpha) \cdot (1 - E)$, $\delta_2 = (1 + \alpha) \cdot (1 - E)$
7. Значение нижнего порога $T_1 = \gamma_1 \cdot \delta_1 + \delta_1 \cdot H_{t_0}$ и верхнего $T_2 = \gamma_2 \cdot \delta_2 + \delta_2 \cdot H_{t_0}$.
8. *Смещаем окно анализа H на шаг* Δt.
9. *Если в полученном окне анализа коэффициентов H число коэффициентов H, лежащих вне* $[T_1, T_2]$ *больше* величины $\frac{w}{2}$, *повторяем шаги 2-7. Иначе, сразу переходим к 8.*

В процессе анализа по приведенному выше алгоритму, получаем:

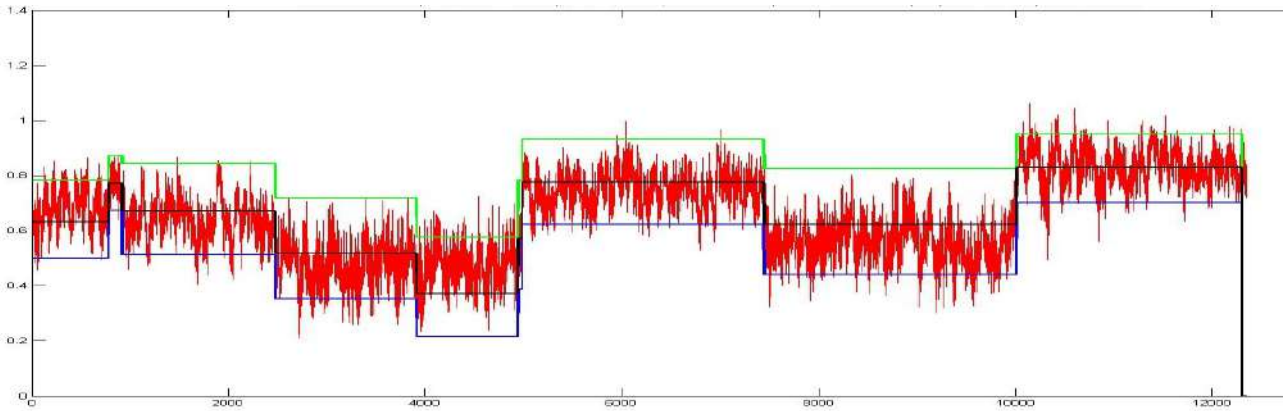


Рис. 2.5 - Результат расчета адаптивных пороговых значений, $w = 50, \Delta t = 20$

Как видно из рис. 2.5 в результате анализа последовательности коэффициентов H, получено 9 интервалов стационарности пороговых значений T_1, T_2 как представлено на рис. 2.6.

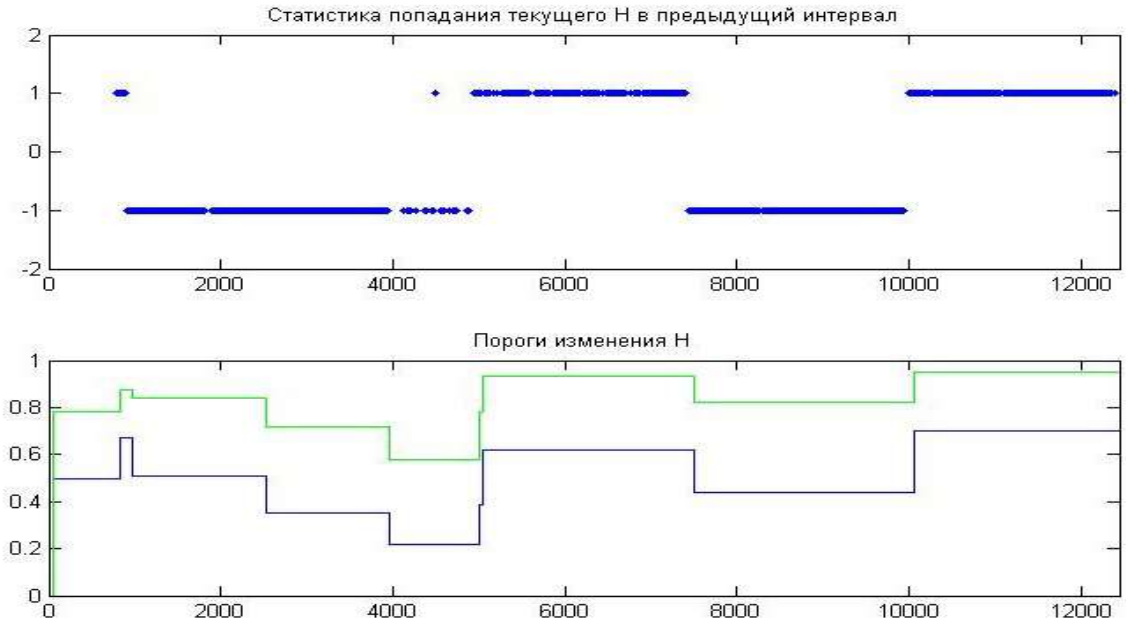


Рис.2.6 - Интервалы стационарности оценки показателя H

В таблице 2.3 отражены суммарные численные значения статистики попадания текущего значения *H* в предыдущий интервал.

Таблица 2.3 - Суммарная длительность для каждого участка *H*.

	H=0.7	H=0.5	H=0.8	H=0.6	H=0.9
+1		7 из 2500	801 из 2500	0 из 2500	1291 из 2500
-1		1089 из 2500	5 из 2500	2033 из 2500	0 из 2500

2.4 Вторичная фильтрация оценки показателя Херста

2.4.1 Алгоритм вторичной фильтрации оценок ФР

На практике при использовании оценки показателя Херста в скользящем окне, возникает проблема правильного обнаружения аномалий, т.к. оценка получается с высокой дисперсией и резкими скачками показателя Херста это можно заметить на рисунке 2.4. Для нейтрализации резких выбросов и уменьшения дисперсии предлагается воспользоваться процедурой трешолдинга – фильтрацией оценки [76, 82, 84, 85].

Пусть $\widehat{H}(t_m)$- оценка показателя Херста, определенная на интервале $m = 1,\dots L$, и пусть фильтрация полученной оценки по вейвлет-коэффициентам осуществляется в скользящем окне размера L. Смещение окна фильтрации производится с некоторым шагом $s \le L$. В результате при смещении окна фильтрации слева-направо оно «пробежит» z положений $Z = L/s$, $z = 1,\dots, Z$. Тогда формула для фильтрации по вейвлет коэффициентам с применением трешолдинга примет следующий вид:

$$\tilde{H}(t_m) = \sum_{l=1}^{L_0} a_l^{(H)} \varphi_l^{(H)}(t_m) + \sum_{j=1}^{J} \sum_{l=1}^{L_j} T\left(d_{j,l}^{(H)}\right) \psi_{j,l}^{(H)}(t_m), \qquad (2.15)$$

где $a_{j_0,l}^{(H)}, d_{j,l}^{(H)}$- аппроксимирующие и детализирующие коэффициенты оценки показателя Херста при z-м положении окна фильтрации, $T\left(d_{j,l}^{(H)}\right)$ – фильтрованные детализирующие вейвлет-коэффициенты; $a_{j_0,l}^{(H)} =< \widehat{H}(t_m), \varphi_l^{(H)} >$ – масштабный коэффициент аппроксимации, равный скалярному произведению оценки показателя Херста $\widehat{H}(t_m)$ и масштабной функции «самого грубого» масштаба J, смещенной на l единиц масштаба вправо от начала координат; $d_{j,l}^{(H)} =< \widehat{H}(t_m), \psi_{j,l}^{(H)} >$ – вейвлет-коэффициент детализации масштаба j, равный скалярному произведению оценки показателя Херста $\widehat{H}(t_m)$ и вейвлета масштаба j , смещенного на l единиц масштаба вправо от начала координат. Здесь $L_0 = 2^{J_{\max}}, (L_0 \le L)$, а $J_{\max} = [\log_2 L]$ – максимальное число масштабов разложения; $[\log_2 L]$ – целая часть числа.

Наибольшее распространение получили следующие виды трешолдинга [4,5]: жесткий трешолдинг - $T_h = d_{j,l}^{(H)} I\left(\left|d_{j,l}^{(H)}\right| > \tau\right)$; и мягкий трешолдинг - $T_s = sign(d)\left(\left|d_{j,l}^{(H)}\right| - \tau\right) I\left(\left|d_{j,l}^{(H)}\right| \ge \tau\right)$.

Процедура трешолдинга является известным инструментом "очистки" сигнала от шумов (высокочастотных компонент). Наибольшее распространение получили следующие виды трешолдинга – жесткий и мягкий трешолдинг.

При «жестком» трешолдинге все детализирующие вейвлет коэффициенты, превышающие некоторый порог, считаются принадлежащими к "оригинальной" оценке, а остальные относят к шуму и обнуляют:

$$f(d^{(m)}{}_{j,k}) = \begin{cases} d^{(m)}{}_{j,k}, & d^{(m)}{}_{j,k} > \tau \\ 0, & d^{m}{}_{j,k} \le \tau \end{cases}, \qquad (2.16)$$

где τ – пороговое значение.

На рис. 2.7 изображена характеристика «жесткого» трешолдинга.

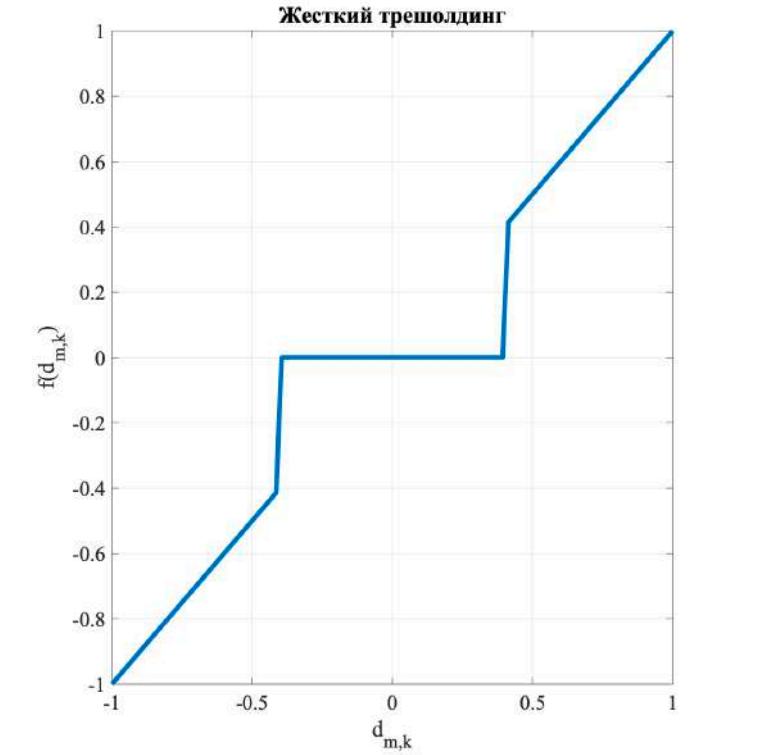


Рис.2.7 - Характеристика «жесткого» трешолдинга

Жесткий трешолдинг устанавливает определенный пороговый уровень для каждой последовательности ДВС и заменяет на 0 все компоненты последовательности меньше этого порога. Такой подход, совмещенный с адаптивным алгоритмом выбора порога, позволяет успешно удалять шумы без какой-либо дополнительной информации о сигнале.

«Мягкий» трешолдинг, при котором из коэффициентов детализации, превышающих установленный порог, вычитается его значение:

$$f(d^{(m)}_{j,k}) = \begin{cases} (|d^{(m)}_{j,k}| - \tau)\, sign(d^{(m)}_{j,k}) & d^{(m)}_{j,k} > \tau \\ 0, & d^{(m)}_{j,k} \le \tau \end{cases} \quad (2.17)$$

где $sign(d^{(m)}_{j,k})$ – оператор знака,

Характеристика «мягкого» трешолдинга представлена на рисунке 2.8.

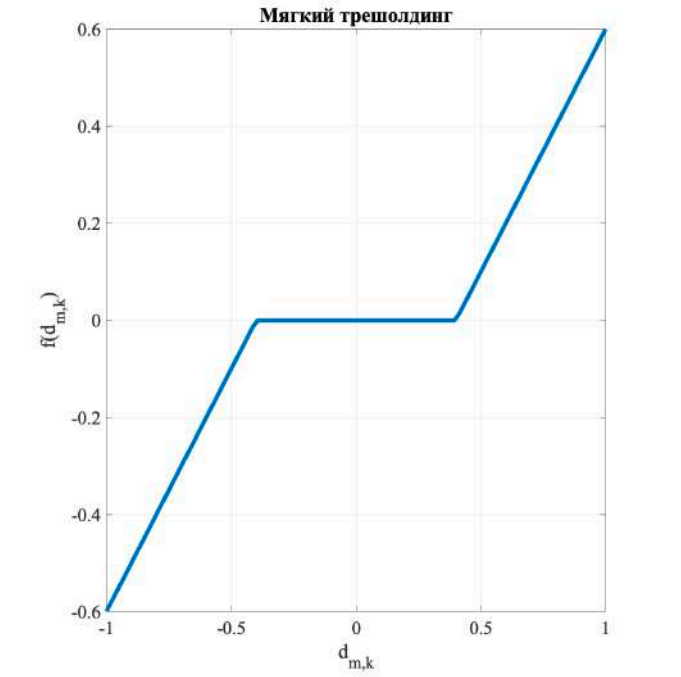


Рис.2.8 - Характеристика «мягкого» трешолдинга

В исследовании используется жесткий трешолдинг. Алгоритм формирования фильтрованной оценки, следующий:

1. Фильтрация производится в окне размером L = 500;
2. Производится 6-уровневое ДВП накопленной оценки показателей Херста;
3. Происходит удаление всех детализирующих вейвлет коэффициентов;
4. Применяется обратное ДВП.

В результате после указанного дополнительного преобразования формируется отфильтрованная оценка без аномальных выбросов.

2.4.2 Тестирование алгоритма фиксации скачков ФР с помощью алгоритма

Для тестирования работоспособности описанного алгоритма (2.15), был смоделирован фрактальный гауссовский шум длиной в 300 000 отсчетов с меняющимся показателем Херста в пределах [0.55:0.95]. Размер скользящего окна

M = 1000. На рис.2.9 показана тестовая последовательность, смоделированная при помощи генератора ФГШ, а также оценка показателя Херста в скользящем окне.

Структура моделируемого трафика представлена в таблице 2.4.

Таблица.2.4 - Показатель Херста на промежутках моделируемого трафика

Промежуток	Показатель Херста
0-50 000	0.7
50 000 – 100 000	0.5
100 000 – 150 000	0.8
150 000 – 200 000	0.5
200 000 – 250 000	0.9
250 000 – 300 000	0.6

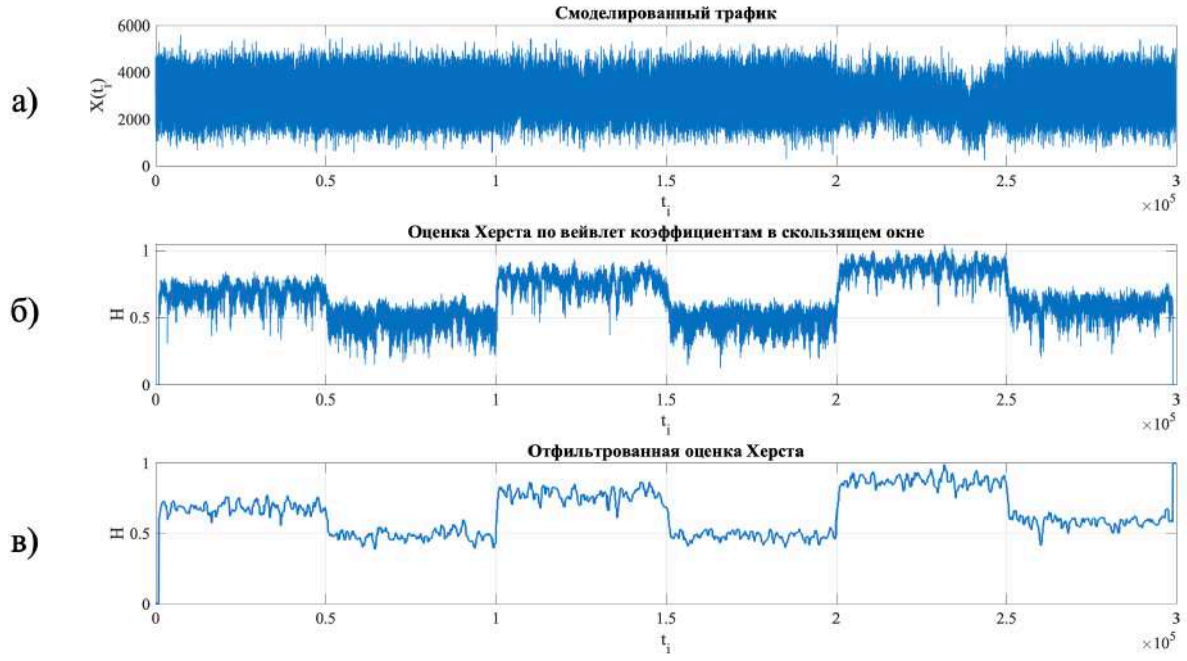


Рис 2.9 - а) Смоделированный трафик, б) полученная оценка показателя Херста в скользящем окне и в) отфильтрованная оценка показателя Херста

На рисунке 2.9а изображена реализация смоделированного трафика с разным показателем Херста. На рисунке 2.9б показана оценка в скользящем окне, как видно из полученного графика при использовании скользящего окна возникают сильные флуктуации, чтобы этого избежать и дать более точную оценку, в дополнительном

окне производится фильтрации, что проиллюстрировано рисунке 2.9.в. Как можно заметить алгоритм более эффективно оценивает скачки фрактальной размерности.

2.4.3 Выбор типа материнского вейвлета при фрактальном анализе

В работах [67,76,86,87] показано, что для оценки параметра Херста H, единственное свойство вейвлета, которое имеет значение – это число стремящихся к нулю моментов. Является ли вейвлет симметричным или нет, ортогональным, полу- или би-ортогональным базисом, ни теоретической, ни значительной практической разницы не имеет [73,88,89]. Однако оценка в задачах обнаружения имеет свои особенности, связанные с постановкой задачи [90,91]. Это связано с объемом анализируемой выборки.

Для выбора типа материнского вейвлета $\psi_{m,k}(t_i)$, используемого при обработке сгенерируем последовательность фрактального гауссовского шума (ФГШ) длинной 10 000 с показателем Херста H = 0.95.

На рис. 2.10 показаны текущие оценка показателя Херста в скользящем окне с использованием разных типов вейвлетов.

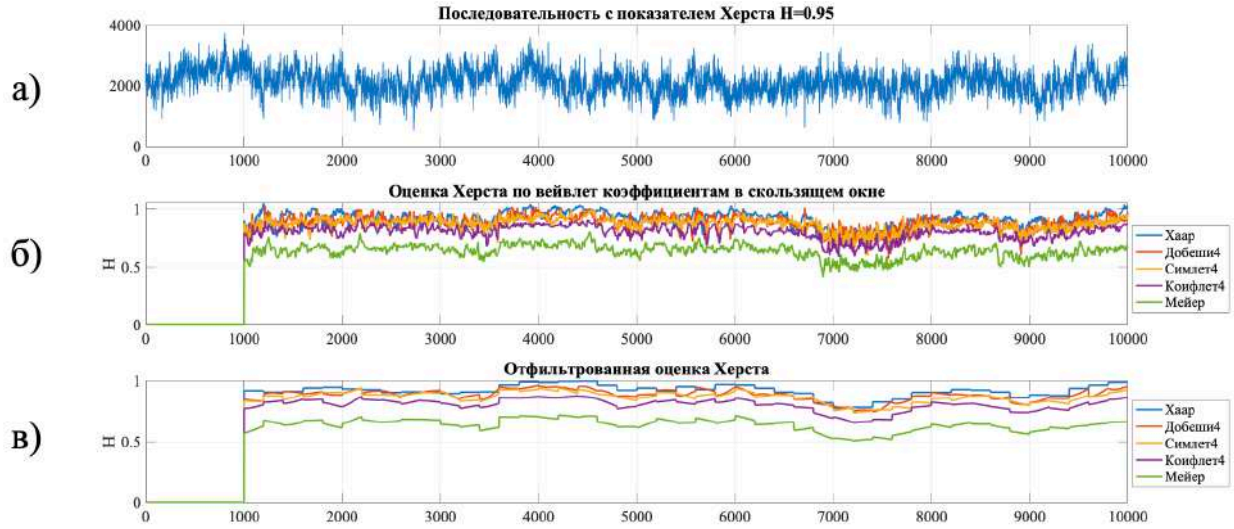
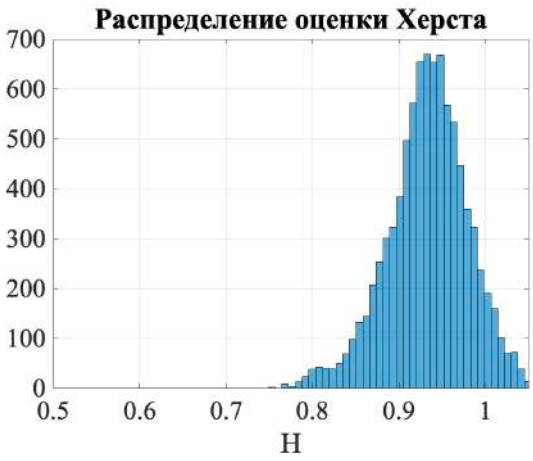
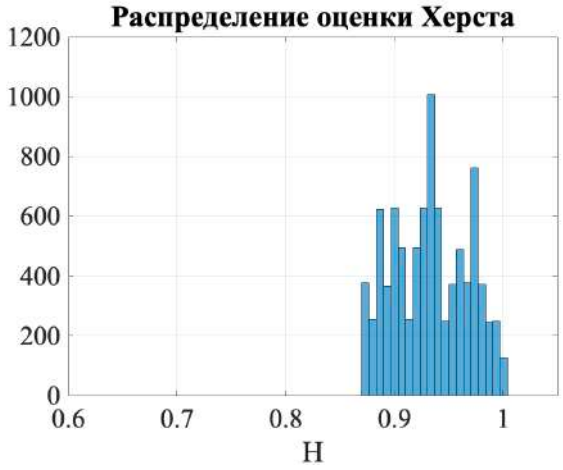
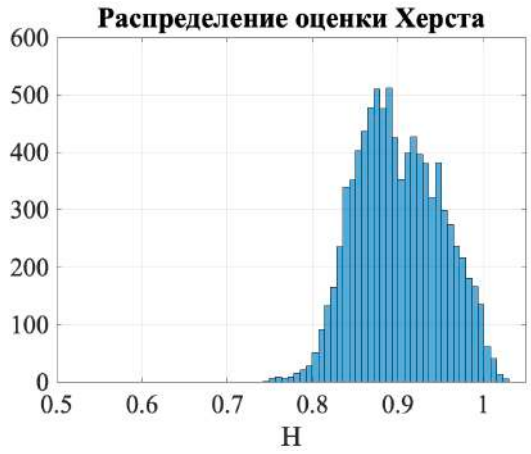


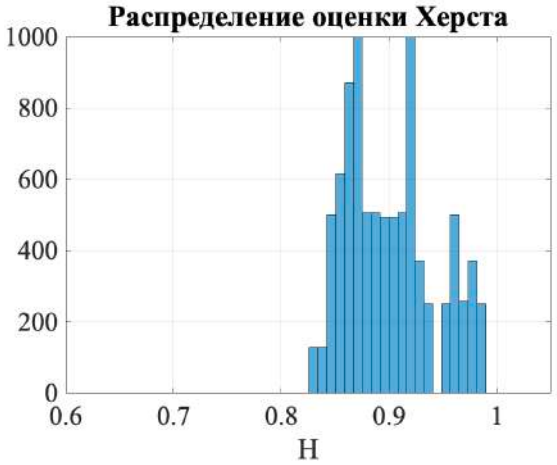
Рис. 2.10 - Текущие оценки показателя Херста в скользящем окне с использованием разных типов вейвлетов а) Сгенерированная последовательность с показателем Херста 0.95, б) оценка показателя Херста в скользящем окне с использованием разных типов вейвлетов и в) отфильтрованная оценка



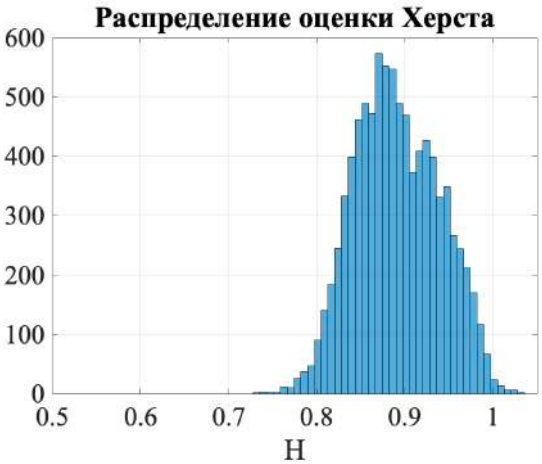


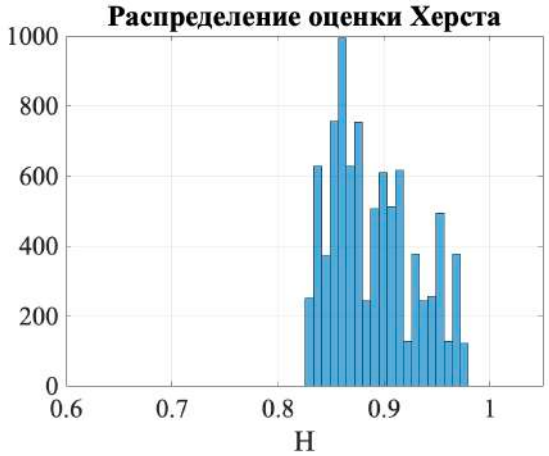
а) Хаар до и после фильтрации



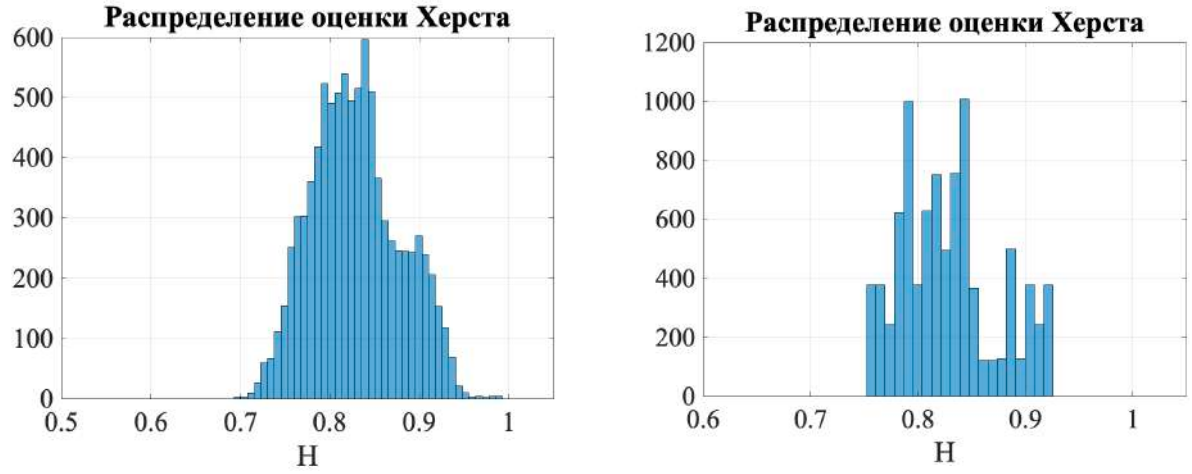


б) Добеши4 до и после фильтрации

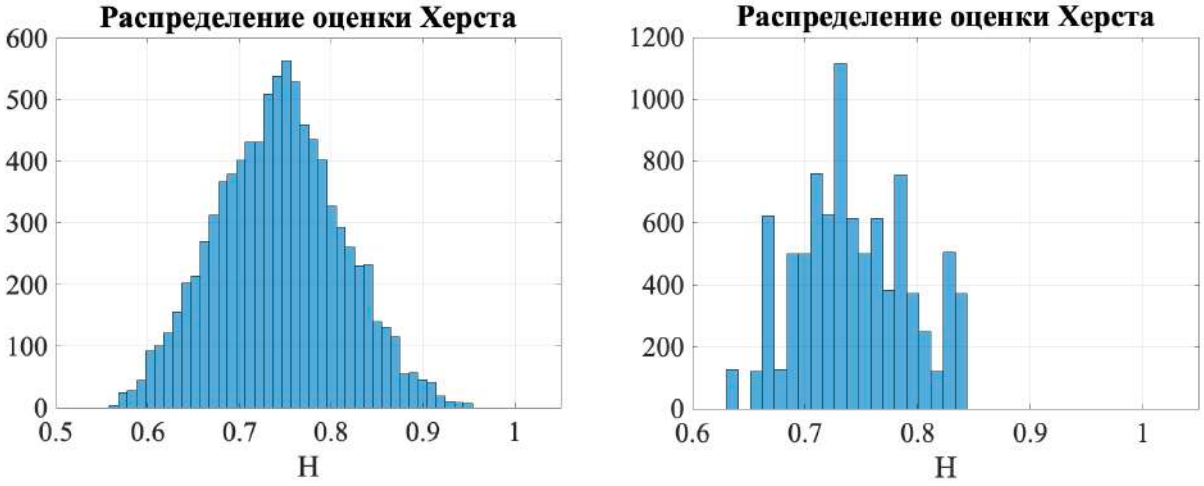




в) Симлет4 до и после фильтрации



г) Коифлет4 до и после фильтрации



д) Мейер до и после фильтрации

Рисунок 2.11 - Гистограммы распределений оценки Херста для ФГШ с показателем Херста H = 0.95 до и после фильтрации

В таблице 2.5 представлены оценки среднего значения и дисперсии показателя Херста при использовании разных материнских вейвлетов.

Таблица 2. 5. Средние значения и дисперсии оценок

Тип вейвлета	Ср. значение до фильтрации	Ср. значение после фильтрации	Дисперсия до фильтрации	Дисперсия после фильтрации
Хаар	0.9333	0.933	0.0022	0.0012
Добеши4	0.9008	0.9009	0.0025	0.0017
Симлет4	0.8912	0.8913	0.0023	0.0016
Коифлет4	0.8291	0.8293	0.0024	0.0020
Мейер	0.7430	0.7431	0.0047	0.0024

Из представленных численных значений видно, что наименьшую дисперсию имеют оценки показателя Херста после фильтрации при использовании вейвлета типа Хаар. Что означает, что именно этот вейвлет целесообразно использовать в качестве материнского при оценке показателя Херста.

Уязвимым местом данного алгоритма является выбор длительности скользящего окна. Учитывая, что длительность окна анализа должна быть достаточно большой, необходима корреляция между типом обнаруживаемых аномалий (атак) и размером окна анализа.

2.5 Экспериментальная оценка статистических характеристик фрактальной размерности КА

2.5.1 Характеристика трафика от устройств Интернета вещей (IoT) на примере базы Kitsune.

В качестве примера, на котором иллюстрируется влияние фрактальных характеристик анализируемого трафика на эффективность классификации КА, рассмотрена база Kitsune [92-94], в которой собран набор данных сетевого трафика от устройств Интернета вещей (IoT). Целью создания базы Kitsune являлось предоставление исследователям большого набор данных о реальных и маркированных вредоносных программах, и безопасном трафике Интернета вещей для разработки алгоритмов машинного обучения. Особенностью набора данных является отсутствие специализации устройств IoT, что позволяет проводить исследования трафика без уточнения дополнительной информации [92].

На рис. 2.12 представлена топология IoT-сети, использованной для сбора эмпирических данных; стрелочные индикаторы на схеме показывают направления распространения и точки возникновения атакующих воздействий. Захват сетевого трафика осуществлялся на уровне маршрутизатора в нескольких контрольных точках, промаркированных на рисунке цифрами, что позволяло фиксировать как транзитные потоки, так и локальные взаимодействия узлов. В каждом наборе

данных сначала собирался нормальный («чистый») трафик без атак порядка 1 млн. пакетов, пакеты с номером > 1 млн. содержали определенную компьютерную атаку.

В данном наборе содержится информация о четырех типах атак: разведка (Recon), человек посередине (MitM), отказ в обслуживании (DoS) и вредоносное ПО для ботнетов (Botnet Malware) Mirai. Mirai — это вредоносное ПО, которое заражает IoT-устройства (умные бытовые приборы с доступом в интернет), работающие на процессорах ARC, и превращает их в сеть дистанционно управляемых ботов, которых также называют «зомби». Этот ботнет часто используется для запуска DDoS-атак.

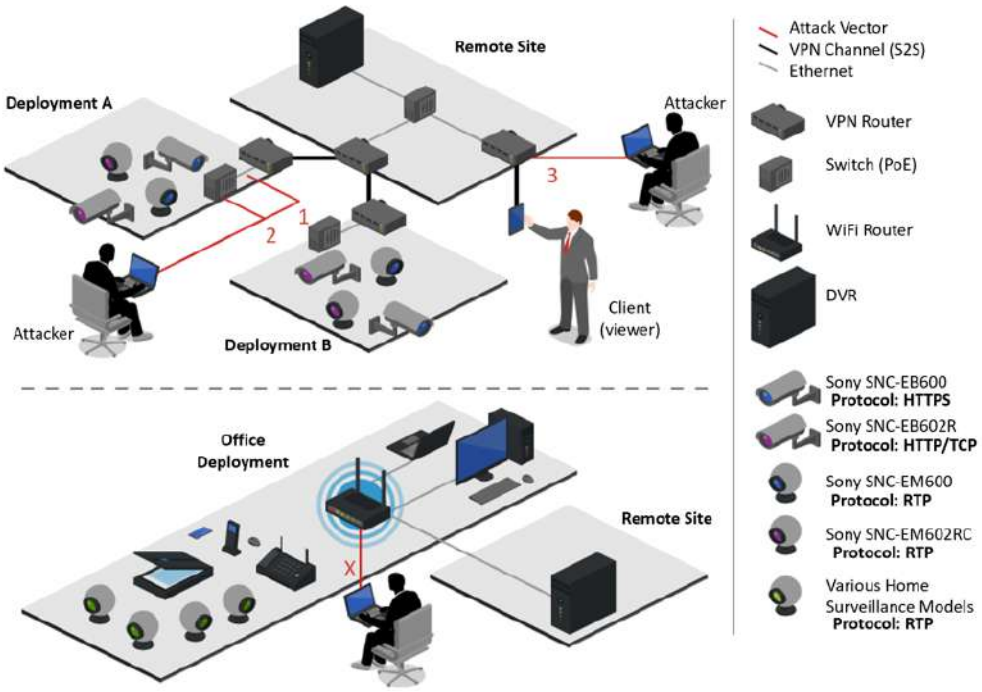


Рис. 2.12 - Топология исследуемой сетевой инфраструктуры

Для каждого типа атак имеется следующий набор данных:

- Предварительно обработанный набор данных, который готов для применения алгоритмов машинного обучения в формате .csv;
- Файл с метками, также в формате .csv;
- Исходный захваченный сетевой трафик в формате .pcap.

Каждая строка csv-файла представляет собой перехваченный и обработанный пакет. Каждая строка содержит информацию о временной статистике, которая описывает контекст передачи этого пакета, включая данные о хостах и протоколах, участвовавших в передаче. Эта информация содержит 115 различных

статистических данных (атрибутов), относящихся к отправителю пакета и трафику между отправителем и получателем.

Общее количество признаков (атрибутов), которые можно извлечь из одного временного окна анализа, составляет 23 атрибута. Для извлечения атрибутов используется пять окон анализа различной длительности: 100 мс, 500 мс, 1,5 с, 10 с и 1 минуту, что в совокупности позволяет создать 115 атрибутов. При отсутствии данных в пакете протокола TCP/UDP соответствующие функции обнуляются. В таблице 2.6 представлены типы и виды сетевых атак, которые содержатся в наборе данных Kitsune.

Таблица 2.6 - Информация об атаках

Тип атаки	Название атаки	Описание	Вектор атаки	Количество пакетов	Длительность, мин
Recon.	OS Scan	Атакующий сканирует хосты в сети и их операционные системы, пытаясь обнаружить возможные уязвимости	1	1 697 851	52,2
	Fuzzing	Атакующий сканирует на наличие уязвимостей web-сервер камер посредством отправки случайных команд	3	2 244 139	85,5
Man in the Middle	Video Injection	Злоумышленник встраивает записанное видео в общий видеопоток	1	2 472 401	33,4
	ARP MitM	Злоумышленник перехватывает весь LAN трафик посредством ARP атаки	1	2 504 267	28,2
	Active Wiretap	Злоумышленник перехватывает весь сетевой трафик через активную прослушку (сетевой мост), установленную на оголенном кабеле.	2	4 554 925	95,6
Denial of Service	SSDP Flood	Злоумышленник перегружает видеорегистратор, заставляя камеры рассылать спам на сервер рекламными объявлениями	1	4 077 266	40,8
	SYN DoS	Злоумышленник отключает видеопоток камеры, перегружая ее веб-сервер	1	2 771 276	52,8
	SSL Renegotiation	Злоумышленник отключает видеопоток камеры, отправляя на камеру множество пакетов повторного согласования SSL	1	6 084 492	65,6
Botnet Malware	Mirai	Злоумышленник заражает устройства IoT вредоносным ПО Mirai, используя учетные данные по умолчанию, а затем сканирует новую уязвимую сеть жертвы.	X	764 137	118,9

В исследовании анализировались фрактальные свойства трафика IoT до и во время воздействия атак: SSDP Flood (длительность 54 сек), Mirai (44 мин), атака типа OS Scan (длительность 29 сек), представленные на рисунке 2.13.

Для оценки фрактальных свойств использовался захваченный в скользящем окне трафик пакетов с интервалом захвата в 100 мс.

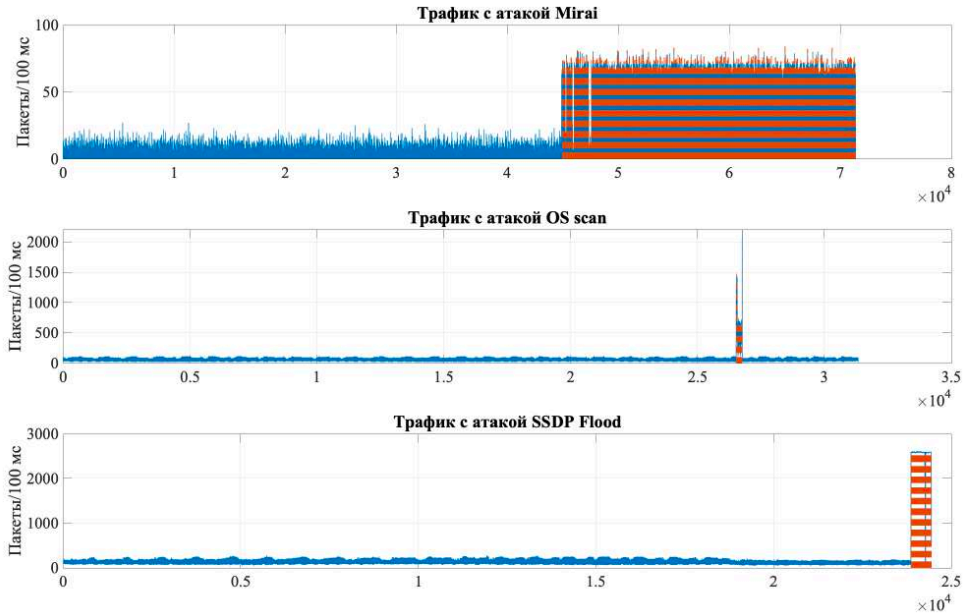


Рисунок 2.13 — Трафик IoT: нормальный трафик (голубой), трафик атак (оранжевый)

В таблице 2.7 представлены характеристики предварительно обработанного набора данных в формате csv, вектор меток, соответствующий исходному сетевому захвату в формате pcap.

Таблица 2.7 — Характеристики набора данных Kitsune

Тип атаки	**Название атаки**	**Количество пакетов**
Вредоносное ПО для ботнетов	Mirai	764,136
Отказ в обслуживании	SSL Renegotiation	2,207,570
Отказ в обслуживании	SSDP Flood	4,077,265
Отказ в обслуживании	SYN DoS	2,771,275
Человек посередине	ARP MitM	2,504,266
Человек посередине	Видеоинъекция	2,472,400
Человек посередине	Активная прослушка	2,278,688
Разведка	сканирование ОС	1,697,850
Разведка	Fuzzing	2,244,138

Данные об атаках были получены из коммерческой IP-системы наблюдения и сети, включающей в себя устройства интернета вещей (IoT). Каждый набор данных содержит миллионы сетевых пакетов и различные кибератаки. Для каждого типа атак имеется следующий набор данных:

- Предварительно обработанный набор данных, который готов для применения алгоритмов машинного обучения в формате .csv;
- Файл с метками, также в формате .csv.

Набор данных также содержит метки, описывающие взаимосвязь между потоками, связанными со вредоносными или возможными вредоносными действиями.

Для обнаружения вредоносных потоков на основе ручного анализа сети использовались следующие метки:

- Метка **«Атака»** указывает на то, что с зараженного устройства на другой хост произошла какая-то атака. Атакой будем называть любой поток, который, анализируя свою полезную нагрузку и поведение, пытается воспользоваться каким-либо уязвимым сервисом. Например, перебор какого-нибудь логина по телнету, внедрение команды в заголовок GET-запроса и т.п.
- Метка **«Доброкачественный»** указывает на то, что в соединениях не обнаружено никаких подозрительных или вредоносных действий.
- Метка **Mirai** указывает на то, что соединения имеют характеристики ботнета Mirai и добавляется, когда потоки имеют схожие шаблоны с наиболее распространенными известными атаками Mirai.
- Метка **C&C** указывает на то, что зараженное устройство было подключено к серверу CC. Эта активность была обнаружена при анализе захвата сетевых вредоносных программ, поскольку подключения к подозрительному серверу носят периодический характер, либо наше зараженное устройство загружает с него какие-то двоичные файлы, либо от него приходят и уходят какие-то IRC-подобные или декодированные заказы.

- Метка **DDoS** указывает на то, что зараженное устройство выполняет распределенную атаку типа «отказ в обслуживании». Эти потоки трафика обнаруживаются как часть DDoS-атаки из-за количества потоков, направленных на один и тот же IP-адрес.

При мониторинге компьютерной сети исходные («сырые») данные фиксировались на уровне пакетов, поступающих от набора устройств. Для каждого пакета записывались временная отметка и набор категориальных признаков, включая MAC-адрес, IP-адрес, номера портов источника и назначения и т. д. Далее поток пакетов преобразовывался в многомерные числовые векторы признаков с использованием метода демпфированной инкрементной статистики (DIS, Damped Incremental Statistics).

ДИС ассоциировалось с параметром $\lambda > 0$, а также с кортежем IS := (N, L_{S_i}, SS_i), где N количество, $L_{S_i} = \sum_{i=1}^{N} x_i$ линейная сумма, а $SS_i = \sum_{i=1}^{N} x_i^2$- квадрат суммы наблюдаемых на текущий момент экземпляров занесенных в инкрементную статистику. Каждая инкрементная статистика связана с потоками данных, определяемыми связкой MAC-адреса, IP-адресами, портами стека протоколов TCP/IP и четырьмя типами данных:

- IP отправителя (srcIP);
- MAC-адрес отправителя (srcMAC), включая пару (srcMAC, srcIP), ассоциированную с отправителем;
- Информация, ассоциированная с каналом передачи данных – пара IP-адресов отправителя – получателя (srcIP, dstIP);
- Сокет, ассоциированный с каналом передачи данных – в виде четверки «IP-адрес отправителя, порт отправителя, IP-адрес получателя, порт получателя (srcIP, srcPort, dstIP, dstPort).

Каждый новый пакет, поступающий на вход ДИС, обновлял статистику по правилам:

$$\gamma = 2^{-\lambda(t-t_{last})};\ \Delta IS_{\lambda} = \left(\gamma\omega + 1, \gamma LS + x, \gamma SS + x^2\right),$$

где t_{last} – отметка времени поступившего пакета, ассоциированного с потоком статистики; ΔIS_λ - приращение инкрементной статистики. Параметр λ определяет интенсивность затухания статистики во времени.

Признаки представляют собой инкрементальные (пошаговые) статистики поступающих данных. Так если S={x1,x2,...} представляет собой неограниченный поток данных, где $x_i \in R$, последовательность наблюдаемых размеров пакетов, то процедура обновления кортежа для вставки x_i в IS имеет вид IS ← (N+1, $L_{S_i}+x_i$, $SS_i+x_i^2$), а текущие статистики в любой момент времени имеют вид

$$\mu_{S_i} = \frac{1}{N}\sum_{i=1}^{N} x_i;\ \sigma_{S_i}^2 = \frac{1}{N}\left[\sum_{i=1}^{N} x_i^2 - \mu_S^2\right] \text{ и } \sigma_S=\sqrt{\sigma_S^2}.$$

Помимо перечисленных, при формировании атрибутов КА и нормального трафика список статистик вычисляемых из инкрементальной статистики $IS_{i,\lambda}$, включал также коэффициенты ковариации $cov(x_i, x_j)$ и корреляции R_{ij}, дополнительные двумерные статистики

$$M_{ij} = \sqrt{\mu_{S_i}^2 + \mu_{S_j}^2} \text{ и } Q_{ij} = \sqrt{(\sigma_{S_i}^2)^2 + (\sigma_{S_j}^2)^2}.$$

После предобработки, используя перечисленные статистики для пяти значений коэффициента «старения» данных λ: 5,3,1,0.1,0.01 сформировано 115 атрибутов [95].

С учетом того, что объем собранного трафика по каждому сценарию компьютерной атаки различается (число пакетов неодинаково), для каждой атаки формируются два файла в формате .csv:

1. файл с обезличенными экспериментальными данными (ЭД), содержащий по 115 признаков на запись;

2. файл с целевой переменной — бинарной меткой, указывающей на наличие либо отсутствие атаки.

Объем ЭД (число строк/записей) существенно варьирует между сценариями. Минимальный объем наблюдается для набора типа Mirai botnet (заражение IoT-сети вредоносным ПО) — около 750 тыс. записей. Максимальный — для атаки отказа в обслуживании SSL Renegotiation — свыше 6 млн. пакетов.

Для апробации разработанного алгоритма из полного множества датасетов были выбраны два набора: Mirai botnet и OS Scan. Последний содержит приблизительно 1,6 млн. записей ЭД.

Необработанные данные о сетевом трафике собирались (в формате pcap) с помощью зеркалирования портов на коммутаторе, через который обычно проходит трафик. Всякий раз, при поступлении пакета формировался *поведенческий снимок* хостов и протоколов, передавших этот пакет, который представляет собой набор из 23 признаков в пяти временных окнах L=5: 100 мс; 500 мс; 1,5 с; 10 с и 1 мин с учетом коэффициента «старения» λ =5; 3; 1; 0.1;0.01.

Итоговое признаковое описание рассмотренных КА формировалось путем извлечения 115 статистических характеристик сетевого трафика, вычисленных на пяти заданных временных интервалах. Полный перечень атрибутов приведен в табл. 2.8.

Таблица 2.8 — Перечень атрибутов в наборе данных Kitsune в разных временных окнах

№	**№ атрибутов в разных временных окнах**	**Атрибут**
1	1, 24, 47, 70, 93	Длина комбинации MAC-IP в битах, (μ)
2	2, 25, 48, 71, 94	Длина SrcIP в битах, (μ)
3	3, 26, 49, 72, 95	Длина Channel в битах, (μ)
4	4, 27, 50, 73, 96	Длина Socket в битах, (μ)
5	5, 28, 51, 74, 97	Длина комбинации MAC-IP в битах, (σ)
6	6, 29, 52, 75, 98	Длина SrcIP в битах, (σ)
7	7, 30, 53, 76, 99	Длина Channel в битах, (σ)
8	8, 31, 54, 77, 100	Длина Socket в битах, (σ)
9	9, 32, 55, 78, 101	Длина Channel в битах, (M_{ij})
10	10, 33, 56, 79, 102	Длина Socket в битах, (M_{ij})
11	11, 34, 57, 80, 103	Длина Channel в битах,(Q_{ij})
12	12, 35, 58, 81, 104	Длина Socket в битах,(Q_{ij})
13	13, 36, 59, 82, 105	Длина Channel в битах, ($Cov_{i,j}$)
14	14, 37, 60, 83, 106	Длина Socket в битах, ($Cov_{i,j}$)

Продолжение таблицы 2.8

№	№ атрибутов в разных временных окнах	Атрибут
15	15, 38, 61, 84, 107	Длина Channel в битах,(R_{ij})
16	16, 39, 62, 85, 108	Длина Socket в битах, (R_{ij})
17	17, 40, 63, 86, 109	Количество пакетов MAC-IP,(N)
18	18, 41, 64, 87, 110	Количество пакетов SrcIP в битах,(N)
19	19, 42, 65, 88, 111	Количество пакетов Channel в битах, (N)
20	20, 43, 66, 89, 112	Количество пакетов Socket в битах, (N)
21	21, 44, 67, 90, 113	Межпакетные задержки исходящего трафика, (N)
22	22, 45, 68, 91, 114	Межпакетные задержки исходящего трафика, Channel, (μ)
23	23, 46, 69, 92, 115	Межпакетные задержки исходящего трафика, Channel, (σ)

2.5.2 Статистические параметры фрактальной размерности КА IoT

Наиболее часто для оценки показателя Херста, характеризующего фрактальную размерность используются анализ нормированного размаха (R/S-метод), график изменения дисперсии и вейвлет-анализ [41,43].

Для оценки фрактальной размерности в режиме реального времени будем использовать оценки показателя Херста в скользящем окне в виде соотношения (2.15). Воспользовавшись соотношениями (1) и (2.15) для обработки экспериментальных данных трафика IoT, были получены статистические характеристики показателя Херста.

На рисунке 2.14 представлены зависимости вычисленных статистических параметров фрактальной размерности $M_{H,}$ и $D_{H,}$ для дампа трафика с атакой Mirai. Сравнительный анализ представленных зависимостей показывает, что методы оценки указанных статистических характеристик с помощью R/S-метода и вейвлет-анализа дают в целом близкие результаты. Разброс в оценке $M_{H,}$ составляет порядка 0,1 , а для $D_{H,}$ не превышает 0,03.

Различие в оценках объясняется скользящим характером оценок ФР в случае вейвлет -анализа.

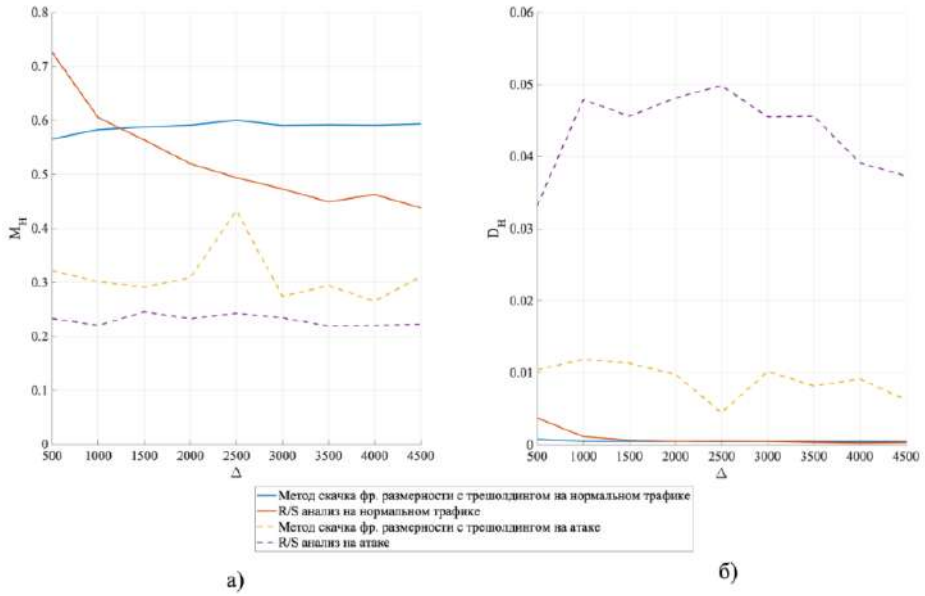


Рисунок 2.14 — Зависимости статистических параметров показателя H от размера окна анализа для дампа нормального трафика IoT и атаки Mirai: а) для нормального трафика в отсутствии атак; б) для трафика в условиях воздействия атаки.

Проиллюстрируем найденные оценки показателя Херста в виде гистограммы распределения, представленных на рисунке 2.15.

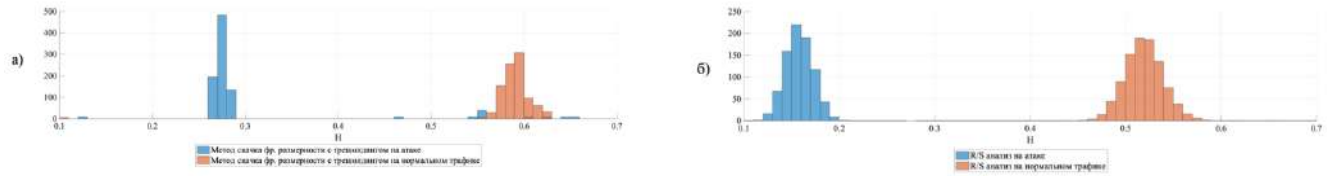


Рисунок 2.15 — Распределение показателя Херста для дампа нормального трафика IoT и атаки Mirai при Δ= 200 сек и использовании алгоритма а) алгоритма скачка фрактальной размерности с трешолдингом, б) R/S анализа

Качественный анализ полученных результатов показывает, что при воздействии атаки Mirai трафик IoT имеет показатель Херста в интервале 0 <H <0.5, что означает, то анализируемый случайный процесс не обладает самоподобием. В свою очередь, как это видно из рисунков 3 и 4 при отсутствии атак трафик фрактальными свойствами обладает, что может быть положено в основу алгоритма обнаружения атак в сетях IoT. На рисунке 2.16 показана оценка

показателя Херста в скользящем окне при использовании двух рассмотренных выше алгоритмов оценки.

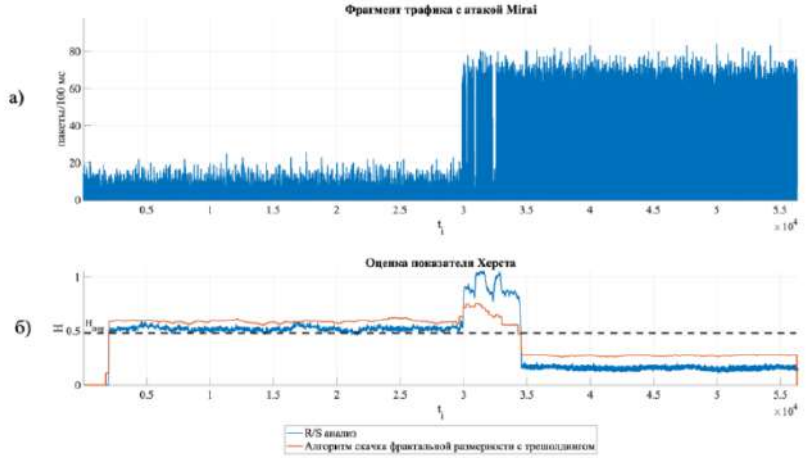


Рисунок 2.16 — Оценка H трафика IoT при воздействии атаки Mirai в скользящем окне размером Δ= 200 сек при использовании алгоритмов (1) и (2.15) а) фрагмент трафика с атакой Mirai, б) оценка показателя Херста в скользящем окне

Как видно из рисунка216 атака Mirai может быть уверенно обнаружена при превышении текущей оценки показателя Херста при соответствующем выборе порогового уровня $H_{пор}$. Данное свойство, когда трафик IoT при отсутствии и наличии атак отличается таким принципиальным образом наблюдается и для других случаев, анализ которых представлен ниже.

На рисунке 2.17 показана текущая оценка показателя Херста в скользящем окне при использовании двух алгоритмов оценки для атаки OS scan.

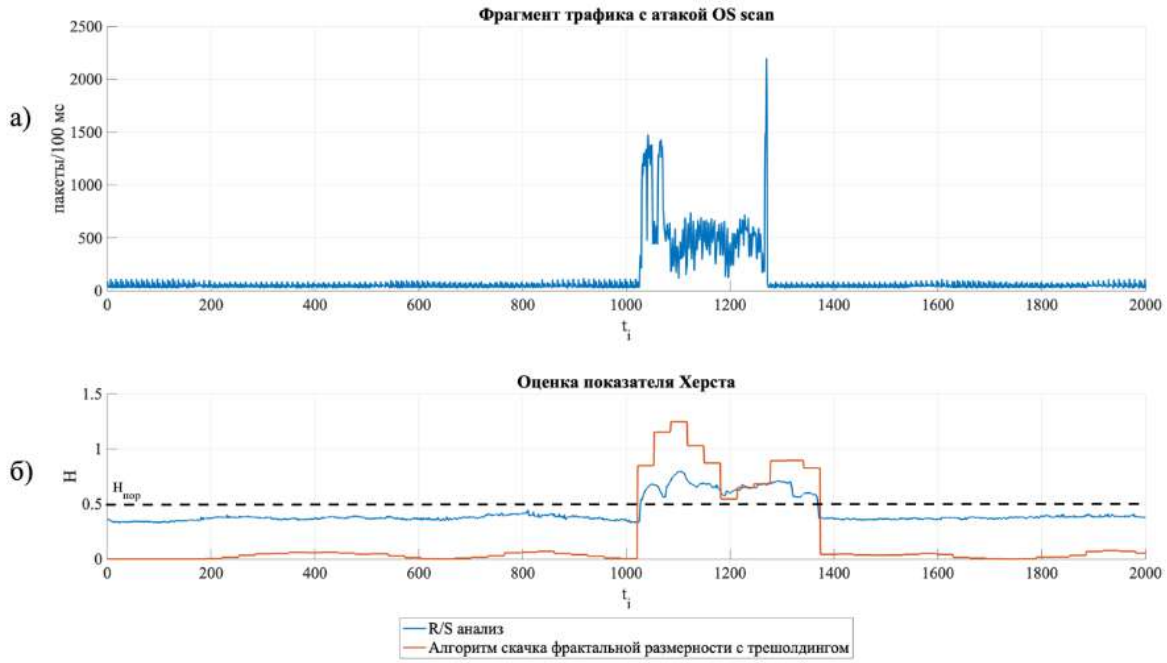


Рисунок 2.17 — Оценка H трафика IoT при воздействии атаки OS scan в скользящем окне размером $\Delta = 10$ сек при использовании алгоритмов (1) и (2.15); а) фрагмент трафика с атакой OS scan, б) оценка показателя Херста в скользящем окне

Анализ численных значений показателя Херста, представленных на рисунке 2.17 показывает, что трафик IoT при отсутствии атак не обладает фрактальными свойствами, а при появлении атаки OS scan наблюдаются, что может быть положено в основу алгоритма обнаружения. Данное явление можно объяснить спецификой трафика устройств IoT. Как и в случае атаки Mirai атака OS scan может быть уверенно обнаружена при превышении текущей оценки показателя Херста порогового уровня $H_{пор}$, как это показано на рисунке 2.17.

Аналогичные результаты наблюдаются и для атаки SSDP Flood. Численное значение показателя Херста для атаки SSDP Flood при использовании алгоритмов (1) и (2.15) представлены на рисунке 2.18.

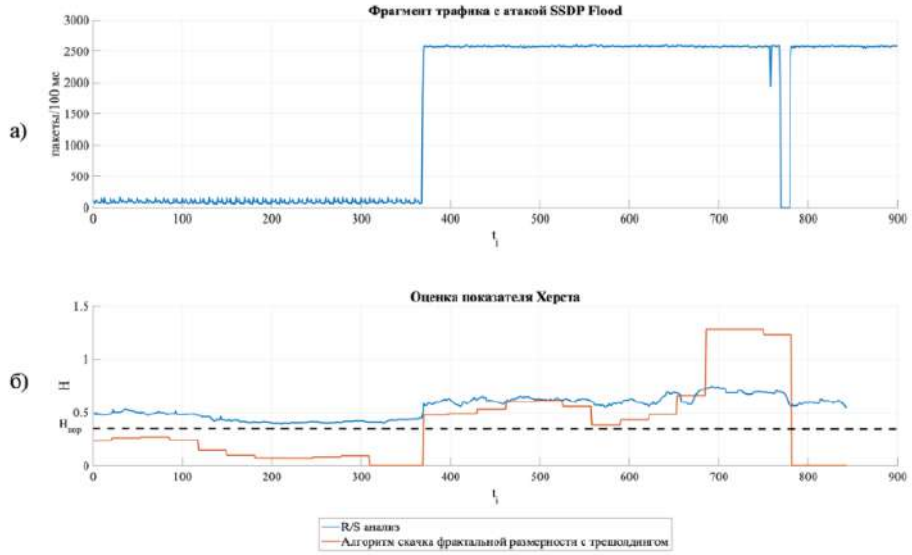


Рисунок 2.18 — Оценка H трафика IoT при воздействии атаки SSDP Flood в скользящем окне размером Δ=10 сек при использовании алгоритмов (1) и (2.15) ; а) фрагмент трафика с атакой SSDP Flood; б) оценка показателя Херста в скользящем окне

Сравнительный анализ зависимостей, представленных на рисунках 2.16…2.18, показывает, что лучшие результаты оценки фрактальной размерности атак показывает алгоритм (2.15) реализующий метод текущей оценки ФР, основанный на вейвлет-анализе с дополнительной фильтрацией в виде преобразования трешолдинга.

2.6 Выводы

1. В главе предложена модификация известного алгоритма обнаружения аномалий (атак) в сетевом трафике при использовании метода оценки скачка фрактальной размерности в режиме реального времени. Модификация заключается в дополнительной фильтрации текущей оценки показателя фрактальной размерности сетевого трафика на базе вейвлет разложения наблюдаемого трафика в текущем окне с применением трешолдинга в режиме реального времени. Добавление дополнительной фильтрации в алгоритм позволяет повысить точность

текущей оценки фрактальной размерности и достоверность обнаружения аномалии в сетевом трафике в режиме online.

2. Наименьшая дисперсия разброса оценок показателя Херста после дополнительной фильтрации наблюдается при использовании вейвлета типа Хаар, что означает, что именно этот вейвлет целесообразно использовать в качестве материнского. Представленные результаты иллюстрируют высокую эффективность разработанного алгоритма.

3. Проведенный сравнительный анализ наиболее известного и разработанного алгоритма оценки ФР на примере реальной базы данных КА в сетях интернета вещей (Приложение А) показал, что оценки ФР с помощью R/S-метода и вейвлет-анализа дают в целом близкие результаты. Разброс в оценке $M_{H,}$ составляет порядка 0,1 , а для $D_{H,}$ не превышает 0,03. Различие в оценках объясняется скользящим характером оценок ФР в случае вейвлет -анализа.

4. Разработанный алгоритм (2.15) позволяет осуществлять текущие оценки ФР в реальном времени в скользящем окне анализа, в то время как R/S-метод требует обработки всей наблюдаемой трассы целиком и формирование оценки только в конце интервала наблюдения

5. По результатам исследования сделан вывод о том, что сетевой трафик интернета вещей обладает свойствами самоподобия, в том случае если присутствуют привычные для обычной топологии сети устройства, такие как стационарные ПК и мобильные устройства. По итогам исследования были получены значения статистических параметров фрактальной размерности для нормального трафика и КА в разных точках описанной топологии сети IoT и разных типов атак.

Наблюдаемые различия фрактальных свойств трафика в IoT в нормальном режиме работы и при воздействии КА могут быть использованы при создании алгоритмов обнаружения компьютерных атак в сетях IoT

ГЛАВА 3 Обнаружение и классификация КА методами монофрактального анализа и машинного обучения

3.1 Постановка задачи

Статистический анализ измерений сетевого трафика в компьютерной сети показывает четкое присутствие у него фрактальных или самоподобных свойств [96-99].

Для построения эффективной системы сетевой защиты перспективным направлением является совместное использование фрактального анализа и интеллектуального анализа данных.

В работе [44] на примере базы данных KDD Cup1999 [100,101] показано положительное влияние оценки фрактальных свойств сетевого трафика и атак на качество бинарной классификации. В качестве дополнительного признака нормального трафика и сетевых атак предложено использовать среднее значение показателя Херста H.

В отличие от [44] предлагается дополнительно повысить эффективность классификации сетевых атак путем использования в качестве информационных признаков не только среднего значения, но и других статистических характеристик ФР атак и нормального трафика. В частности, это могут быть дисперсия, коэффициенты асимметрии и эксцесса, характеризующие форму и параметры распределения ФР.

Эффективность предлагаемого подхода может быть оценена путем оценки качества бинарной классификации сетевых атак и нормального трафика на примере использования базы данных (например UNSW-NB15 [102,103]) с помощью широкого класса алгоритмов машинного обучения

3.2 Результаты обнаружения КА в реальном времени методом монофрактального анализа

3.2.1 Обнаружение КА в реальном времени методом оценки скачков фрактальной размерности

Для оценки эффективности алгоритма обнаружения КА будем использовать традиционные подходы теории статистических решений в виде задачи проверки двух альтернативных гипотез: H_0 и H_1, которые выражают предположения об отсутствии или наличии КА в текущем интервале времени соответственно

Алгоритм обнаружения представляет собой операцию сравнения текущей оценки показателя Херста с пороговым уровнем

$$\widehat{H}(t_m) \geq H_{\text{пор}}. \quad (3.1)$$

Достоверность обнаружения оценивается формулой

$$P_{\text{ПО}} = P\{(\sum \widehat{H_i} > H_{\text{пор}}; i = \overline{1,n})|H_1\}. \quad (3.2)$$

Выбор порогового уровня $H_{\text{пор}}$ осуществляется исходя из заданной величины вероятности ошибки второго рода

$$P_{\text{ЛТ}} = \alpha = P\{(\sum \widehat{H_i} > H_{\text{пор}}; i = \overline{1,n})|H_0\}. \quad (3.3)$$

Здесь H_1 и H_0 гипотезы наличия и отсутствия КА в наблюдаемой последовательности длительности $\{i = \overline{1,n}\}$.

Из представленных на рисунке 3.1 текущих и усредненных оценок H видно, что атака может быть обнаружена с помощью сравнения полученной величины текущей оценки параметра H в скользящем окне с пороговым уровнем в режиме онлайн.

Порог определяется путем анализа решающей статистики на интервале обучения, для которого точно известно об отсутствии аномалий. При применении критерия Неймана-Пирсона пороговое значение H_пор находится из выражения α=const

$$\alpha = \int_{U_{пор}}^{\infty} w(K_i \mid 0)dK_i,\ P_{лт} = \int_{U_{пор}}^{+\infty} w(x)\,dx = const \qquad (3.4)$$

где $w(K_i|0)$ – функция плотности распределения вероятности i-го критерия при условии, что аномалия отсутствует;

Ошибка первого рода состоит в том, что нулевая гипотеза отвергается, то есть принимается гипотеза H_1, в то время как в действительности верна гипотеза H_0 (вероятность ложной тревоги $P_{ЛТ}$).

Ошибка второго рода состоит в том, что принимается гипотеза H_0, а в действительности верна гипотеза H_1 (вероятность пропуска вторжения $P_{ПВ}$).

Для любой заданной критической области будем обозначать через α вероятность ошибки первого рода, а через β вероятность ошибки второго рода. Следовательно, можно сказать, что при большом количестве выборок доля ложных заключений равна α, если верна гипотеза H_0, и β, если верна гипотеза H_1. При фиксированном объеме выборки выбор критической области W позволяет сделать, как угодно, малой либо α, либо β.

Рассмотрим эффективность алгоритма обнаружения КА (3.10) при использовании разработанного алгоритма оценки ФР с дополнительной фильтрацией (2.15) на реальных данных. В качестве исходных данных взята реализация сетевого трафика имеющая длительность N = 10 000, которая включает в себя как нормальный трафик, так и аномалию в виде атаки Neptune (SYN-flood) представленная на рисунке 3.1. Размер окна анализа был выбран M = 1000, использовался вейвлет Хаар.

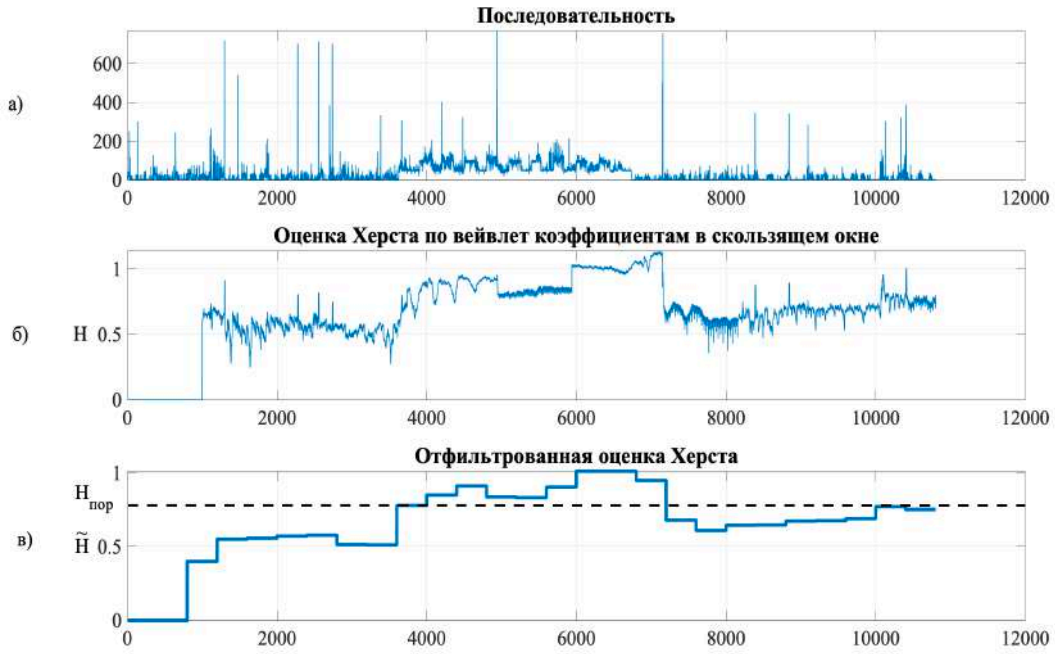


Рис.3.1 — Оценка показателя Херста в скользящем окне а) график реализации трафика с атакой Neptune, б) оценка Херста в скользящем окне и в) отфильтрованная оценка

Как видно из представленных на рисунке 3.1 текущих и усредненных оценок показателя Херста КА может быть обнаружена с помощью оценки фрактальных свойств трафика в скользящем окне в режиме онлайн.

Оценить достоверность обнаружения КА можно воспользовавшись представленными на рисунке 3.2 гистограммами распределения показателя Херста до атаки и во время нее.

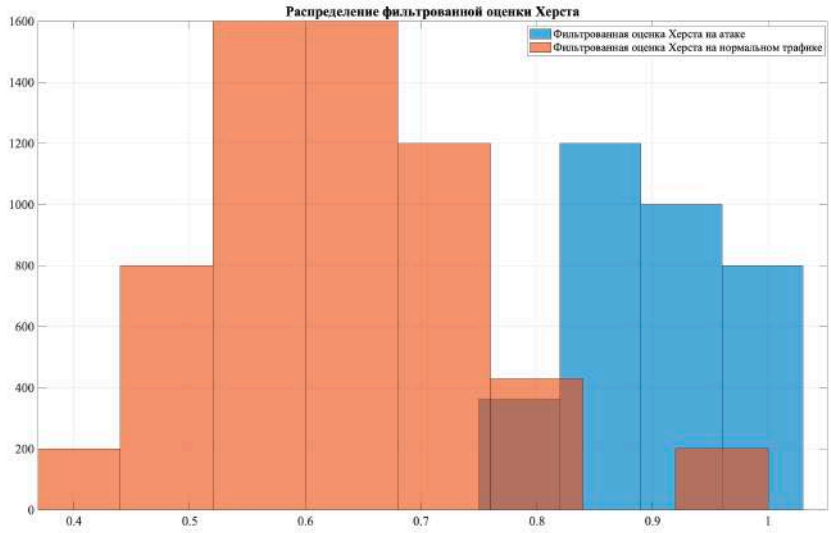
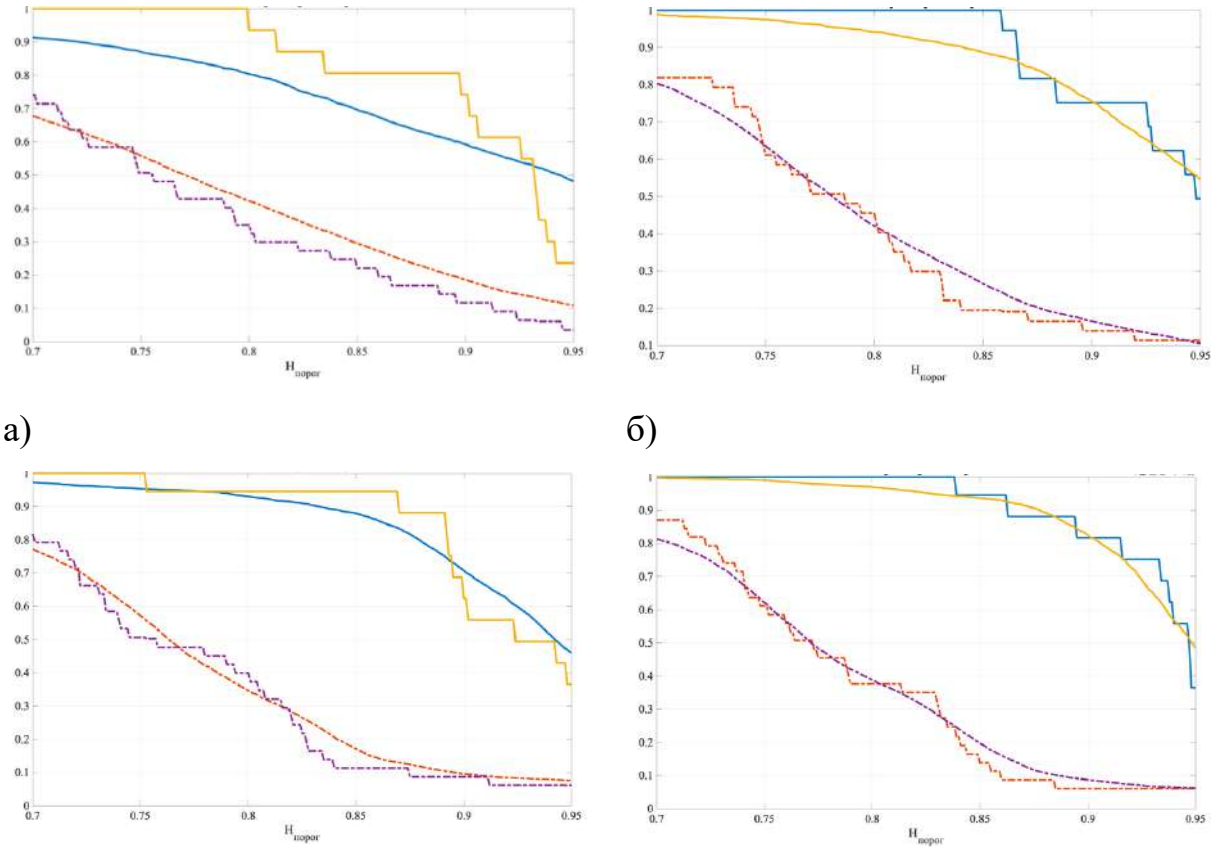


Рис 3.2 — Гистограммы распределения оценки показателя Херста до атаки и на атаке

Как видно при выборе порогового значения $H_{\text{пор}}$= 0,75 атака может быть уверенно обнаружена. На рисунке 3.3 представлены зависимости характеристик вероятности правильного обнаружения Рпо и ошибок первого рода α в зависимости от порога обнаружения при разной длине окна обнаружения М до и после фильтрации.



а) б)

в) г)

Рис.3.3 — График зависимости Рпо и α от порога обнаружения при использовании разной длины окна обнаружения до и после фильтрации а) при М = 200, б) при М = 500, в) при М = 700, г) при М = 1000

Как видно из полученных зависимостей процедура трешолдинга позволяет улучшить характеристики обнаружения в некоторых случаях до 10%. Однако при увеличении размера окна обнаружения процедура трешолдинга слабо влияет на характеристики.

На рисунке 3.4 построены зависимости характеристик вероятности правильного обнаружения и ложного срабатывания от порога обнаружения при разном уровне разложения при фильтрации оценки показателя Херста.

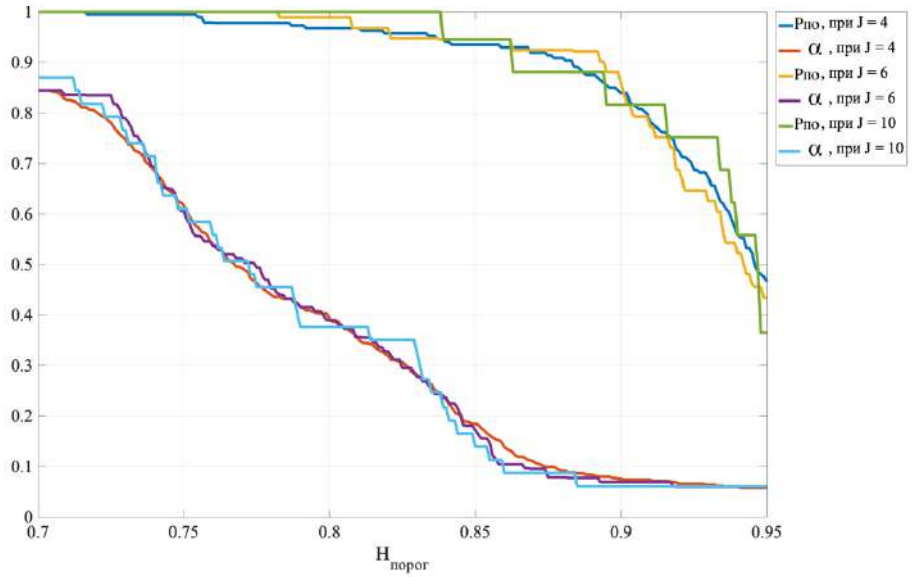


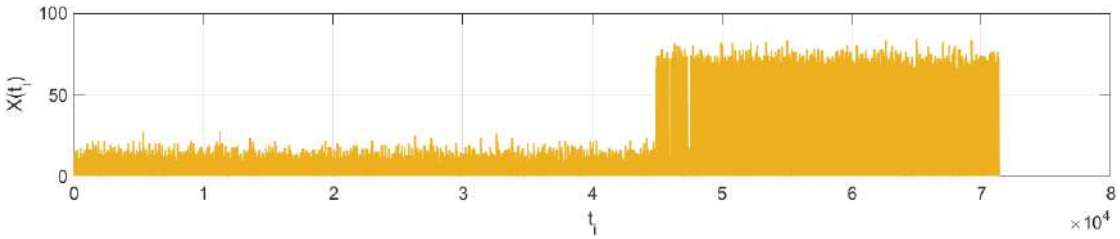
Рис.3.4 — График зависимости Рпо и α от порога обнаружения при разных уровнях вейвлет разложения при фильтрации

Как видно из полученных зависимостей, при уровне разложения J = 10 достигается минимальная вероятность ложной тревоги при пороге $H_{пор}$ = 0.85. При увеличении уровня разложения удается добиться уменьшения ложных срабатываний, однако при этом уменьшается и вероятность правильного обнаружения.

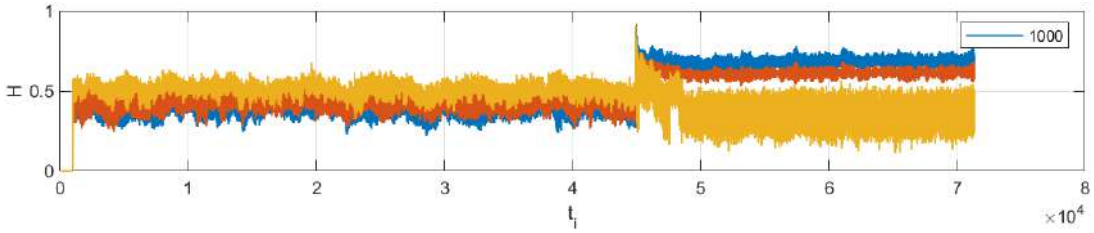
3.2.2 Обнаружение КА в реальном времени методом оценки скачков фрактальной размерности для сетевого трафика IoT

В качестве второго примера эффективности обнаружения КА на основе оценок скачков фрактальной размерности КА [104] рассмотрим характеристики обнаружения рассмотренного алгоритма обнаружения (3.1) для атак, наблюдаемых в сетях IoT. Фрактальные характеристики атак такого вида рассмотрены в главе 2.

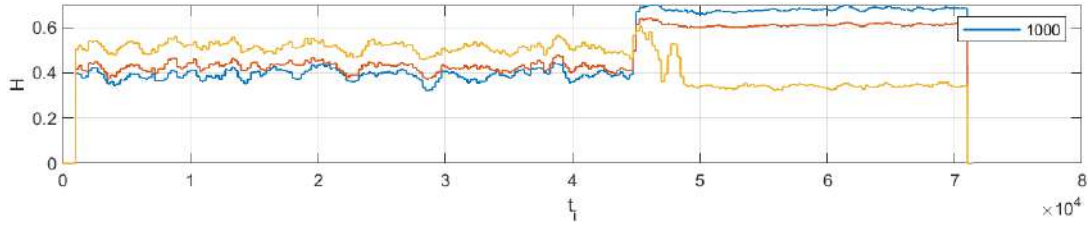
На рисунке 3.5 представлены графики сетевого трафика, с помощью которых протестирован алгоритм оценки скачка фрактальной размерности на экспериментальных данных используя вейвлет Хаара при окне анализа размером Δ= 1000 отсчетов.



а)



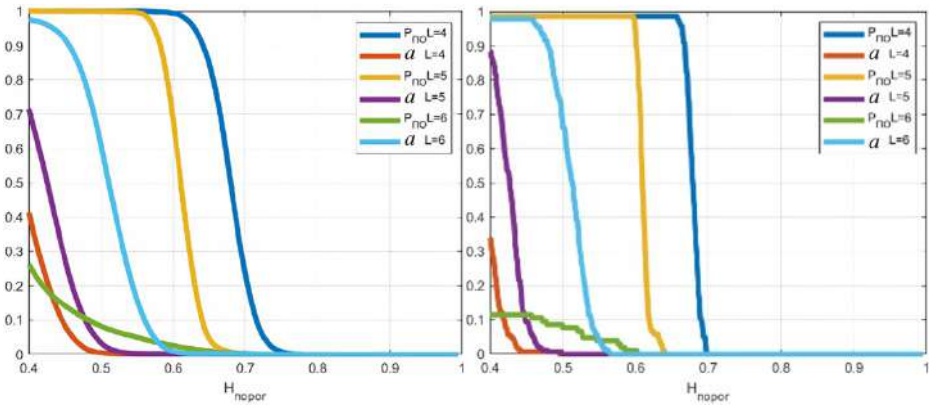
б)



в)

Рисунок 3.5 – Реализации сетевого трафика и оценки показателя Херста для КА типа Mirai в сети IoT при Δ= 1000 отсчетов: а) график реализации сетевого трафика; б) оценка Херста в скользяще м окне; в) Оценка показателя Херста после вторичной фильтрации

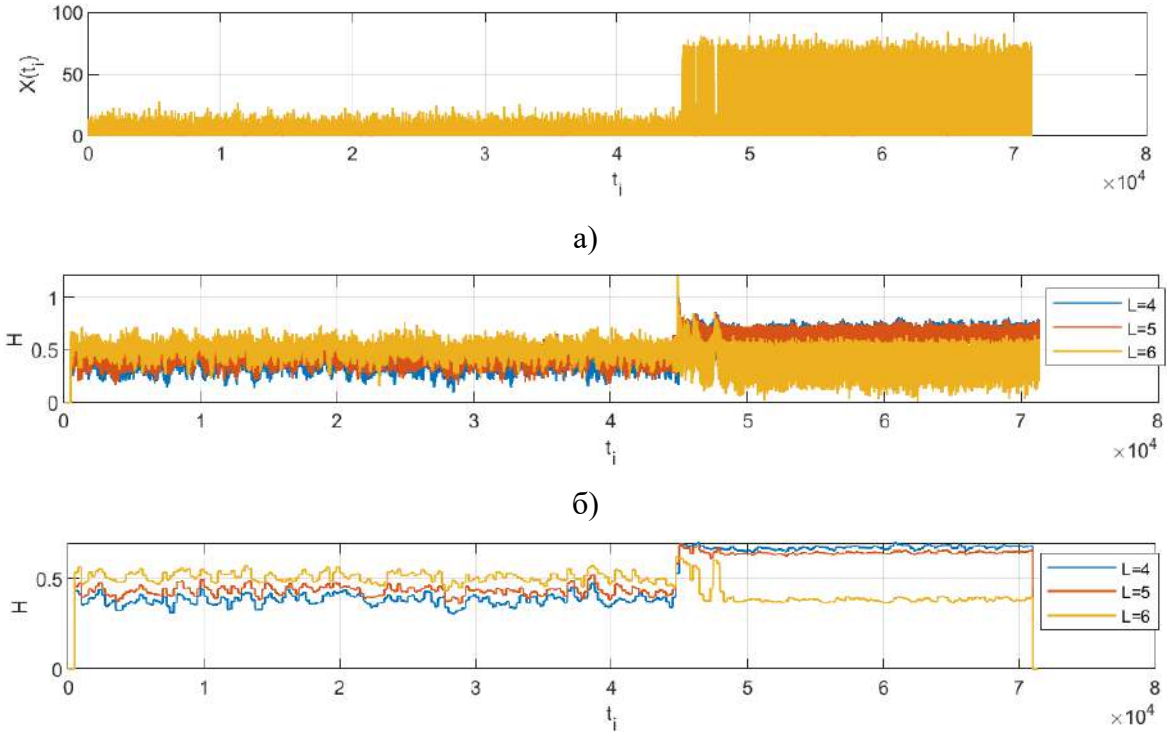
Зависимости характеристик вероятности обнаружения КА в зависимости от количества уровней разложения представлены на рисунке 3.6 а для оценки без применения процедуры фильтрации и на рисунке 3.6б с применением процедуры фильтрации.



а) б)

Рисунок 3.6 – Характеристики вероятности обнаружения КА типа Mirai в зависимости от уровня разложения при Δ= 1000 отсчетов а) без применения фильтрации; б) с применением процедуры фильтрации.

На рисунках 3.7 представлены графики сетевого трафика и результаты оценки скачка фрактальной размерности на экспериментальных данных используя вейвлет Хаара при окне Δ= 500 отсчетов.



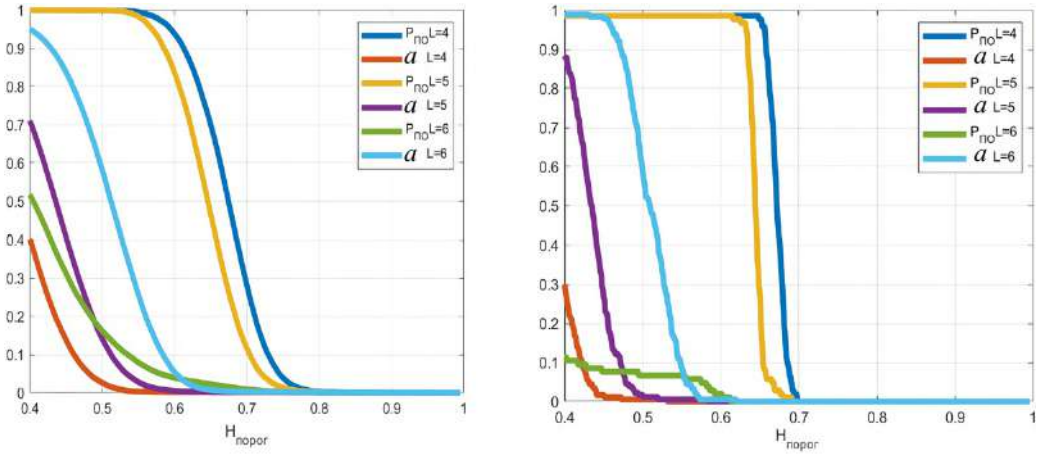
а)

б)

в)

Рисунок 3.7 – Реализации сетевого трафика и оценки показателя Херста для КА типа Mirai в сети IoT при Δ= 500 отсчетов: а) график реализации сетевого трафика; б) оценка Херста в скользяще м окне; в) Оценка показателя Херста после вторичной фильтрации

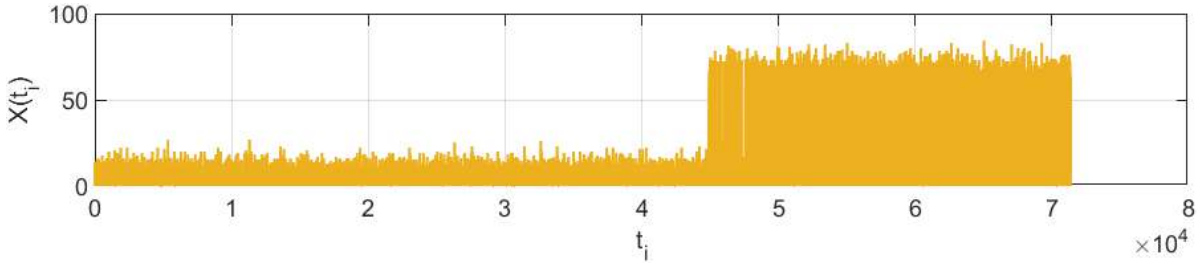
Зависимости характеристик вероятности обнаружения КА в зависимости от количества уровней разложения представлены на рисунке 3.8а для оценки без применения процедуры фильтрации и на рисунке 3.8б с применением процедуры фильтрации для окна анализа Δ= 500 отсчетов.



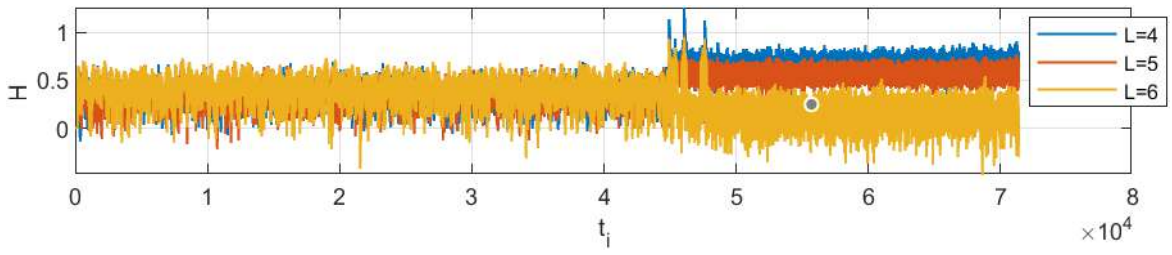
а) б)

Рис. 3.8 — Характеристики вероятности обнаружения КА типа Mirai в зависимости от уровня разложения при Δ= 500 отсчетов а) без применения фильтрации; б) с применением процедуры фильтрации.

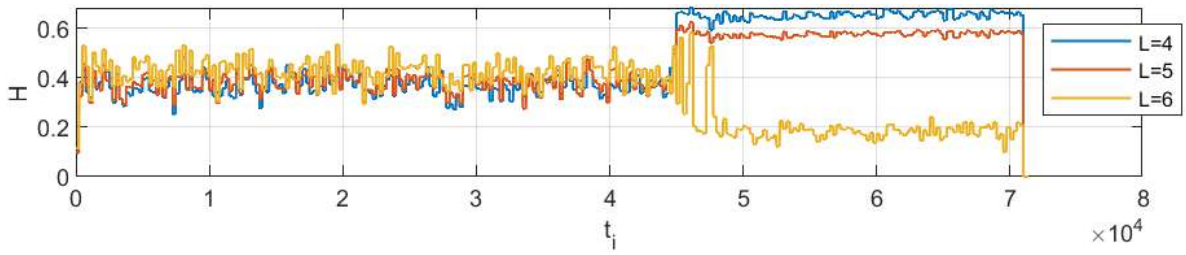
На рисунках 3.9 представлены графики сетевого трафика и результаты оценки скачка фрактальной размерности на экспериментальных данных используя вейвлет Хаара при окне Δ= 200 отсчетов.



а)



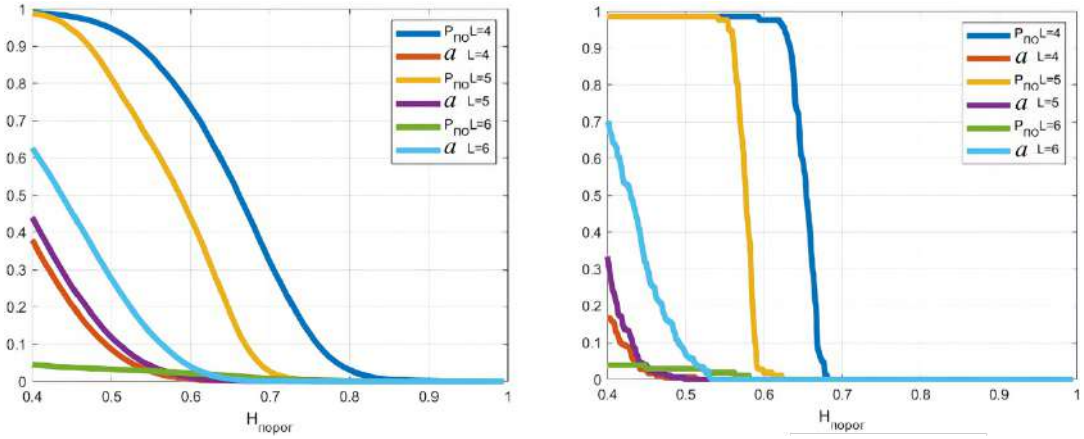
б)



в)

Рисунок 3.9 – Реализации сетевого трафика и оценки показателя Херста для КА типа Mirai в сети IoT при Δ= 200 отсчетов: а) график реализации сетевого трафика; б) оценка Херста в скользяще м окне; в) Оценка показателя Херста после вторичной фильтрации

Зависимости характеристик вероятности обнаружения КА в зависимости от количества уровней разложения представлены на рисунке 3.10 а для оценки без применения процедуры фильтрации и на рисунке 3.10б с применением процедуры фильтрации для окна анализа Δ= 200 отсчетов.



а) б)

Рис. 3.10 — Характеристики вероятности обнаружения КА типа Mirai в зависимости от уровня разложения при Δ= 500 отсчетов а) без применения фильтрации; б) с применением процедуры фильтрации

Сравнительный анализ представленных зависимостей показывает высокую эффективность разработанного алгоритма оценки ФР с использованием вторичной фильтрации коэффициентов детализации вейвлет разложения.

Наилучшие результаты демонстрирует случай выбора числа уровней разложения J = 4, а величина рекомендуемого порогового уровня $H_{пор}$ = 0,65. При этом $P_{по}$ = 1, а вероятность ошибок второго рода не превышает 10(-3)

3.2.3 Выводы по итогам оценки достоверности обнаружения КА по скачкам ФР

Как видно из представленных на рисунках 3.3 и 3.4 параграфа 3.2.1 и 3.6; 3.8; 3.10 параграфа 3.2.2 атака может быть обнаружена с высокой достоверностью с помощью оценки фрактальных свойств трафика в скользящем окне в режиме онлайн путем сравнения текущей оценки $\widehat{H}(t_m)$ с пороговым уровнем.

Как видно из полученных зависимостей для различной природы КА процедура трешолдинга позволяет улучшить характеристики обнаружения до 10%. При увеличении размера окна процедура трешолдинга незначительно влияет на характеристики обнаружения

Показано, что для получения достоверной оценки значения показателя Херста необходимо использовать вейвлеты типа Хаара, показавшего наилучшие результаты.

Как видно из полученных зависимостей наиболее важными параметрами для обнаружителя являются: размер окна обнаружения M и порог обнаружения $H_{пор}$. При правильном подборе этих параметров обеспечивается высокая вероятность правильного обнаружения $P_{п0}$ = 0.85...0,95 и низкая вероятность ошибок первого рода $P_{ЛФ}$=0.05...0,001.

Для оптимизации выбора длительности окна анализа и усреднения при вторичной фильтрации должна оцениваться корреляция между типом обнаруживаемых аномалий (атак) и размером окна анализа.

3.3 Бинарная классификация КА методами машинного обучения с учетом статистических характеристик ФР

Эффективность рассмотренного алгоритма КА может быть дополнительно повышена за счет использования многочисленных атрибутов КА и использования алгоритмов машинного обучения для бинарной и/или многоклассовой

классификации. Так, например в случае использования характеристик КА в сетях IoT используются 115 атрибутов. При использовании UNSW-NB15 используются 49 атрибутов.

3.3.1 Набор данных

Таблице 3.1 представлена статистика набора данных UNSW-NB15, которая представляет период моделирования, номера потоков, общее количество байтов от источника, байтов получателя, количество пакетов источника, количество пакетов назначения, типов протоколов, количества нормальных и ненормальных записей и количество уникальных IP-адресов источника / назначения [102,103].

Таблица 3.1 — Статистика база данных

		1й день (16 часов)	2й день (15 часов)
No_of_flows		987627	976882
Src_bytes		4860168866	5940523728
Des_bytes		44743560943	44303195509
Src_Pkts		41168425	41129810
Des_Pkts		53402915	52585462
Типы протоколов	TCP	771488	720665
	UDP	301528	688616
	ICMP	150	374
	Others	150	374
Нормальная запись		1064987	1153774
Атака		22215	299068
Количество уникальных IP-адресов источника		40	41
Количество уникальных IP-адресов назначения		44	45

Составленные признаки из сырых данных набора представлены в *Таблице 1 Приложения В*. Признаки с 1 по 35 представляют интегрированную собранную информацию из данных пакетов. Большинство признаков генерируется из заголовков пакетов, а дополнительные признаки 35-47 создаются на основе потока.

Учитывая, что классы в наборе данных UNSW-NB15 не сбалансированы, т.е. количество записей с классами *normal* и *dos* в несколько раз превосходит количество записей по другим классам необходимо использовать *нормализацию* набора данных. Нормализация проводилась по принципу *мини-макс* в соответствии с *формулой* $x' = \frac{x - \min(X)}{\max(X) - \min(X)}$, где min(X) и max(X) – минимальное и максимальное значение поля из всего набора данных.

С помощью признаков 1-5 и 29, 30 из исходных данных были выделены потоковые данные с разделением по каждой категории. Фрагмент нормального трафика UNSW-NB15 представлен на рисунке 3.11.

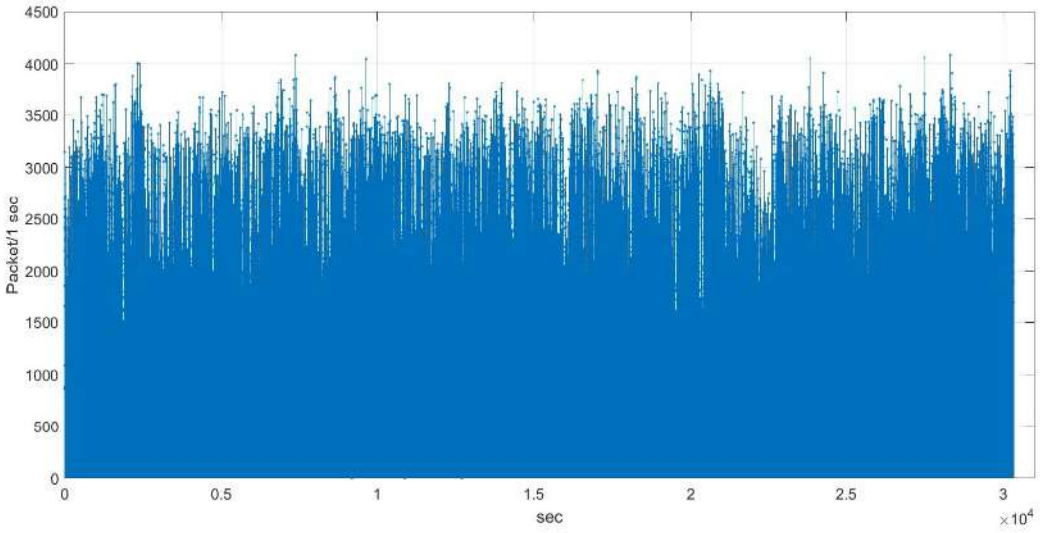


Рисунок 3.11 — Фрагмент нормального трафика UNSW-NB15

Используя экспериментально снятые характеристики атак и нормального трафика, можно оценить статистические характеристики ФР атак и нормального трафика на этапе обучения и использовать их затем на этапе классификации.

3.3.2 Дополнительные фрактальные признаки атак при машинном обучении

Для повышения эффективности бинарной классификации анализируемого набора данных предлагается (в отличие от работы [44]) ввести дополнительные признаки (атрибуты) для каждого из типов обнаруживаемых атак.

При проведении численных расчетов учитывались только реализации атак, для которых количество наблюдений n>100. В этом случае погрешность оценки показателя Херста не превышала 5%.

В качестве совокупности фрактальных атрибутов предлагается использовать экспериментально полученные статистические характеристики ФР какие как: среднее значение ФР (показатель Херста) *MH*, дисперсию показателя Херста *DH*, коэффициенты асимметрии Касс, и эксцесса Кэ, характеризующие форму плотности распределения вероятностей фрактальной размерности w(H).

В таблице 3.2 представлены результаты оценки указанных выше статистических параметров показателя Херста *H* для атак всех категорий трафика при количестве реализаций атак равном N.

При вычислениях не были учтены атаки Shellcode и Worms, поскольку для них отсутствовали продолжительные интервалы необходимые для оценки параметров фрактальной размерности.

Таблица 3.2 — Статистические характеристики распределения w(H) для атак

Тип атаки	(N)	*Мн*	*Dн*	Касс	Кэ
Normal	20	0.6949	0.0009	0.3137	0.4431
Analysis	9	0.6685	0.0084	0.2493	1.1772
Backdoors	8	0.6121	0.0030	0.8678	0.4829
DoS	18	0.5900	0.0051	1.0607	2.5674
Exploit	21	0.7251	0.0060	0.4528	0.3805
Fuzzers	23	0.6891	0.0045	0.1573	1.2453
Generic	15	0.6726	0.0083	0.3544	1.3438
Reconnaissance	9	0.6026	0.0013	0.1751	1.0603

В соответствии с полученными результатами в *таблицу 1 Приложения В* признаков набора данных UNSW-NB15для обучающих и тестовых подвыборок были добавлены 4 новых признака представленных в *таблице 3.3*.

Таблица 3.3 — Дополнительные признаки атак и нормального трафика

№	Признак	Описание
Дополнительные признаки фрактальной размерности		
50	herst_avg	Математическое ожидание ФР для распределения w(H)
51	herst_desp	Дисперсия D(H) для распределения w(H)
52	herst_skew	Коэффициент асимметрии Kacc для распределения w(H)
53	herst_kurtosis	Коэффициент эксцесса Кэ для распределения w(H)

Если в таблице 1 *Приложения В* запись отсутствовала, то дополнительный признак принимался равным нулю. Это означает, что дополнительный признак отсутствует и для данной категории атаки в процессе классификации не принимается во внимание.

На рисунках 3.12 и 3.13 представлены гистограммы позволяющие оценить значимость признаков при учете введенных дополнительных параметров ФР. Важность введенных признаков вычислялась с помощью коэффициента Джини [39], лежащем в основе принятия решений алгоритмов DTC (рисунок 3.12) и RF (рисунок 3.13).

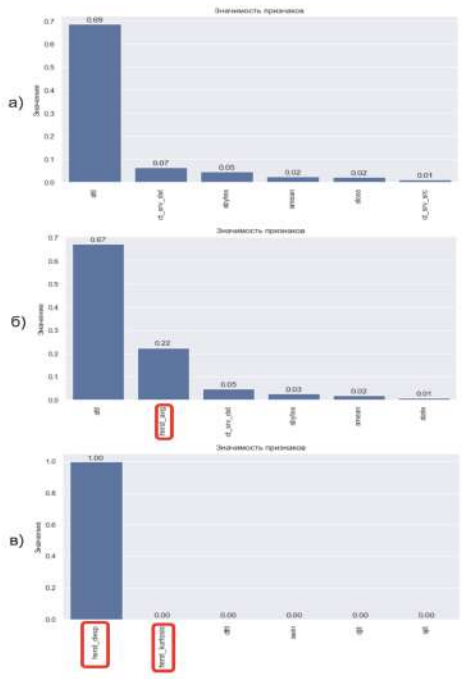


Рисунок 3.12 – Значимость первых 6 признаков для алгоритма *DTC* в задаче классификации а) без учета ФР; б) с учетом параметра herst_avg(50); в) с учетом всех статистических параметров ФР из *таблицы 3.3*.

Сравнение гистограмм 3.12а и 3.12б показывает, что для алгоритма *DTC* учет только одного дополнительного атрибута в виде среднего значения параметра Херста herst_avg ставит его на второе место по значимости при классификации атак. Однако если появляется возможность оценить дополнительные параметры ФР, то наибольшей значимостью будут обладать атрибуты herst_desp и herst_kurtosis. В соответствии с таблицей 3.3 атрибут herst_desp характеризует разброс параметра Херста относительно среднего значения. Параметр herst_kurtosis, характеризующий форму распределения параметра Херста w(H) имеет хотя и важное, но существенно меньшее значение.

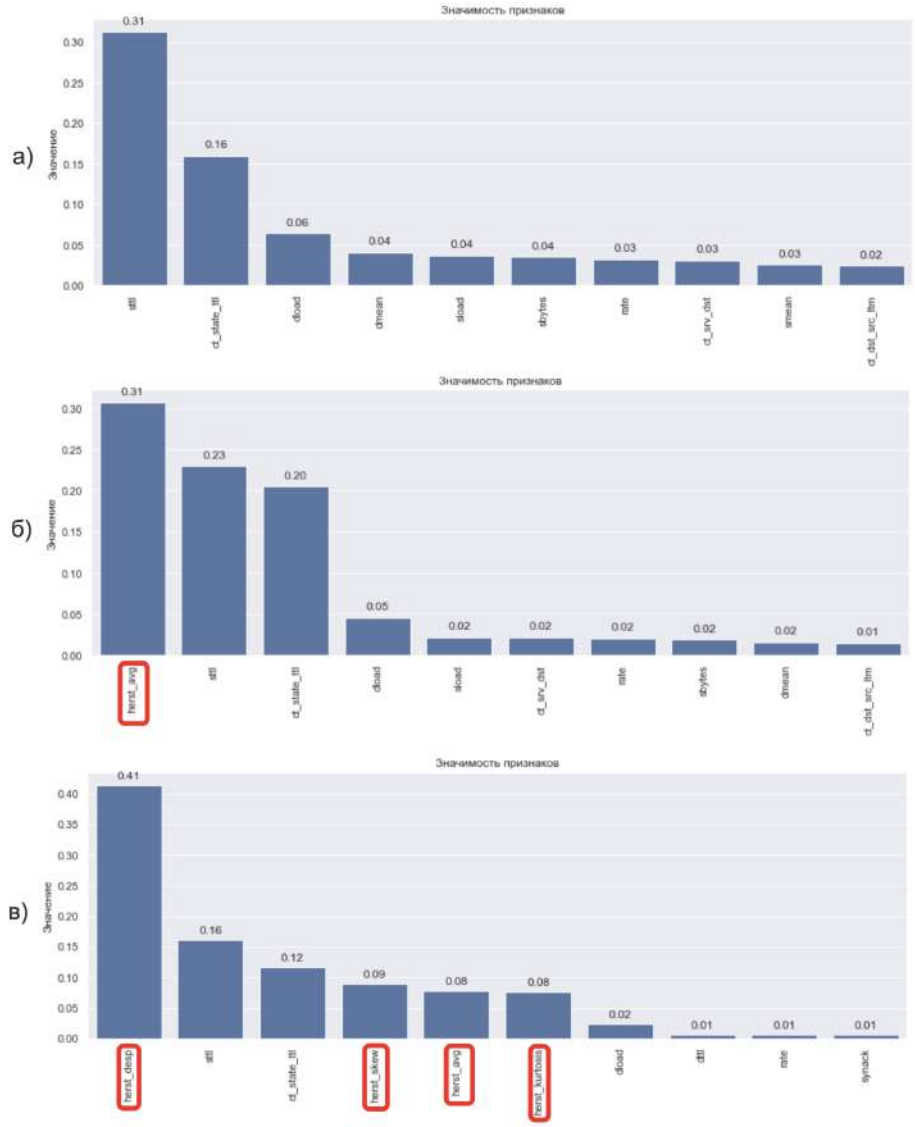


Рисунок 3.13 – Значимость первых 10 признаков для алгоритма *RF* в задаче классификации: а) без учета ФР; б) с учетом параметра herst_avg(50); в) с учетом всех статистических параметров ФР из *таблицы 3.3.*

Как видно из рисунка 3.13а для алгоритма *RF* на качество классификации влияет большее число признаков, по сравнению с алгоритмом DTC. Однако и в этом случае учет только одного дополнительного атрибута herst_avg ставит его на первое место по значимости.

Однако если появляется возможность оценить дополнительные параметры ФР, характеризующие форму и параметры распределения Херста w(H) наибольшей значимостью будут обладать атрибут herst_desp .

В соответствии с таблицей4 атрибут herst_desp характеризует разброс параметра Херста относительно среднего значения. Параметры herst_skew, herst_kurtosis, характеризующие форму распределения w(H) имеют несколько меньшее значение, занимают по степени важности 4-е и 6-е место.

Из представленных гистограмм можно видеть, что дополнительные статистические атрибуты, представленные в таблице 3.3 оказывают существенное влияние на алгоритм принятия решения.

3.3.3 Результаты бинарной классификации

Рассмотрим результаты сравнительного анализа влияния статистических характеристик w(H) на качество бинарной классификации атак. Для бинарной классификации все категории атак были приведены к одной категории “Attack”. В результате классификация сводится к задаче идентификации двух классов: Attack и Normal. Анализировались три режима работы.

1. Классификация только при использовании исходных признаков 1…49 приведенных в таблице 1 Приложения В. Результаты классификации представлены на рисунках 3.14–3.15 (а);
2. Классификация при добавлении к набору признаков 1…49 одного дополнительного признака №50 - herst_avg (50) - среднего значения показателя Херста. Результаты классификации, соответствующие этому случаю приведены на рисунках 3.14–3.15 (б);

3. Классификация при добавлении к набору признаков 1…49 всех четырех статистических признаков №№ 50…53 приведенных в таблице 3.3: herst_stat **(**herst_avg; herst_desp; herst_skew; herst_kurtosis**)**. Результаты классификации, соответствующие этому случаю приведены на рисунках 3.14–3.15 (в).

При классификации не использовались признаки 1–4, 29, 30 из таблицы 1 Приложения В, поскольку они отсутствовали в исходных обучающих и тестовых выборках.

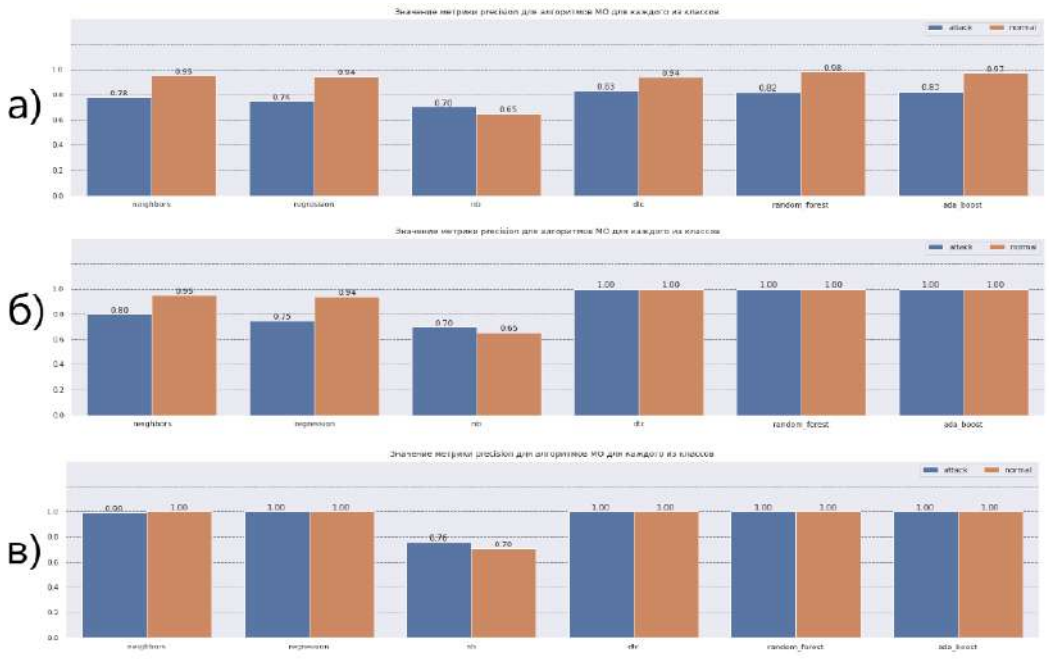


Рисунок 3.14 – Значения метрики precision для классификаций а) без учета ФР, б) с учетом параметра herst_avg(50) в) с учетом всех статистических параметров из herst_stat *таблицы 3.3.*

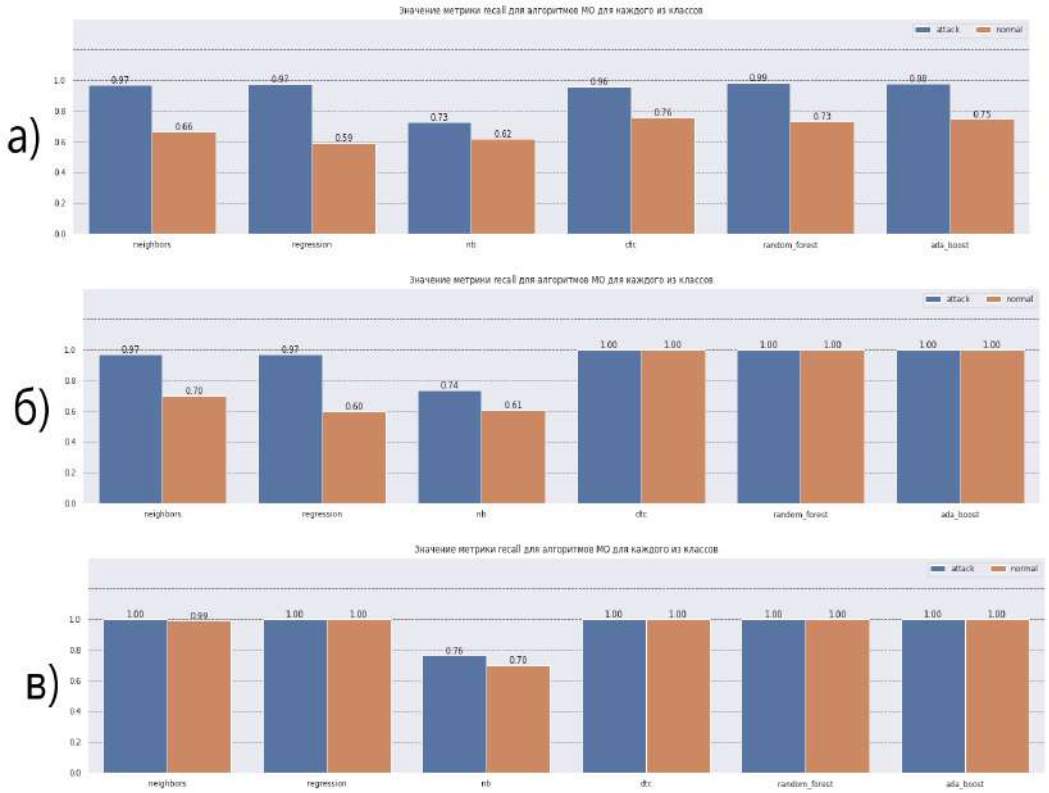


Рисунок 3.15 – Значения метрики recall для классификаций а) без учета ФР, б) с учетом параметра herst_avg(50) в) с учетом всех статистических параметров herst_stat из таблицы 3.3.

Из представленных результатов видно, что эффективность использования дополнительных атрибутов в виде статистических параметров ФР атак herst_stat и нормального трафика наиболее заметна для алгоритмов классификации *k-NN* и *LR*. Для этих алгоритмов выигрыш от использования дополнительных атрибутов достигает 21% для метрики precision при наличии атак и 41% при их отсутствии.

Выигрыш в метрике f1-score скромнее и составляет около 7%. Для метрики AUC-PR выигрыш составляет 7-8%.

Наибольший эффект достигается от использования в качестве дополнительного признака среднего значения фрактальной размерности - *Мн*. При использовании алгоритмов классификации DTC и RF выигрыш от использования дополнительного атрибута *Мн* оставляет около 15–20% практически для всех рассмотренных метрик.

Более существенным выигрыш от использования дополнительных атрибутов оказывается в сокращении времени обучения и тестирования. Эти результаты приведены в таблице 3.4.

Таблица 3.4 — Быстродействие алгоритмов классификаций

Алгоритмы\доп признаки	**нет**			**herst_avg**			**herst_stat**		
	обуч.	**предск.**	**всего**	**обуч.**	**предск.**	**всего**	**обуч.**	**предск.**	**всего**
k-NN	76,01	34,84	110,85	94,03	45,78	139,81	**67,57**	**27,44**	**95,01**
LR	6,84	0,01	6,85	7,17	0,01	7,18	**4,65**	**0,005**	**4,65**
NB	0,56	0,01	0,57	0,53	0,02	0,55	**0,48**	**0,01**	**0,49**
DTC	2,32	0,09	2,41	1,47	0,11	1,58	**0,59**	**0,09**	**0,68**
RF	16,49	0,35	16,84	8,21	0,27	8,48	**4,59**	**0,24**	**4,83**
Ada Boost	547,08	14,87	561,95	596,65	15,22	611,87	**469,23**	**13,49**	**482,72**

Наиболее эффективными здесь оказываются также алгоритмы DTC и RF. В случае алгоритма DTC использование одного дополнительного параметра в виде среднего значения ФР привело к снижению времени на обучение и тестирование более чем в 1,5 раза, а для алгоритма «случайный лес» в 1,98 раза.

Использование всех четырех дополнительных атрибутов herst_stat **(**herst_avg; herst_desp; herst_skew; herst_kurtosis, представленных в таблице 4 повысило из значимость и привело к снижению времени на обучение и тестирование для алгоритма «дерево решения» в 3,54 раза, а для алгоритма «случайный лес» в 3,48 раза. Абсолютные цифры оказались меньше у алгоритма «дерево решений» и составили 0,68 сек, в то время как для «случайный лес» - 4,83 сек.

3.4 Выводы

1. Из представленных текущих и усредненных оценок показателя Херста атака может быть обнаружена с помощью оценки фрактальных свойств трафика в скользящем окне в режиме онлайн путем сравнения текущей оценки $\widehat{H}(t_m)$ с пороговым уровнем. Процедура трешолдинга позволяет улучшить характеристики обнаружения до 10%. При увеличении размера окна процедура трешолдинга незначительно влияет на характеристики обнаружения. Показано, что для получения

достоверной оценки значения показателя Херста необходимо использовать вейвлеты типа Хаара

2. Из полученных зависимостей видно, что при уровне разложения J = 10 при пороге $H_{пор}$ = 0.85 достигается вероятность правильного обнаружения $P_{по}$ > 0.85 и вероятность ложной фиксации $P_{ЛФ}$<0.05 минимальная вероятность ложной тревоги. При увеличении уровня разложения во время фильтрации удается добиться уменьшения числа ложных срабатываний.

3. Наилучшими параметрами для обнаружения КА типа Mirai в сетях IoT являются: длина окна обнаружения M = 1000 и порог обнаружения $H_{пор}$ = 0.8. При таких параметрах обеспечивается вероятность правильного обнаружения $P_{по}$ > 0.9 и вероятность ложной фиксации $P_{ЛФ}$<0.001.

4. Введение дополнительных статистических параметров фрактальной размерности, характеризуемых средним значением параметра Херста Мн, дисперсией Dн Касс, и Кэ характеризующими форму распределения w(H) положительно влияет на качество и скорость бинарной классификации атак. Сравнительный анализ дополнительных атрибутов показал, что наибольшей значимостью при использовании алгоритма DTC являются атрибуты Мн и Dн. При использовании алгоритма RF наибольшей значимостью обладает атрибут Dн. Однако велико значение и атрибутов Касс, и Кэ характеризующих форму распределения w(H).

5. Из представленных результатов видно, что эффективность использования дополнительных атрибутов в виде статистических параметров ФР атак herst_stat и нормального трафика наиболее заметна для алгоритмов классификации k-NN и LR. Для этих алгоритмов выигрыш от использования дополнительных атрибутов достигает 21% для метрики precision при наличии атак и 41% при их отсутствии.

Выигрыш в метрике f1-score скромнее и составляет около 7% . Для метрики AUC-PR выигрыш составляет 7–8%.

Наибольший эффект достигается от использования в качестве дополнительного признака среднего значения фрактальной размерности - *Мн*. При использовании алгоритмов классификации DTC и RF выигрыш от использования

дополнительного атрибута *Мн* оставляет около 15-20% практически для всех рассмотренных метрик.

6. Более существенным выигрыш от использования дополнительных атрибутов оказывается в сокращении времени обучения и тестирования. Для алгоритмов DTC и RF наибольший эффект от использования дополнительных атрибутов (*Мн*, *Дн, Касс*, и *Кэ)* оказывается в сокращении времени обучения и тестирования и составляет около 3,5 раз для каждого из алгоритмов.

7. Использование в качестве дополнительных информационных признаков среднего значения, дисперсии, коэффициентов асимметрии и эксцесса, характеризующих форму и параметры распределения статистических характеристик распределения ФР позволяет повысить качество бинарной классификации в среднем на 10%. Наибольший эффект от учета дополнительных статистических параметров ФР заметен для алгоритмов классификации k-NN и LR.

ГЛАВА 4 Метод повышения эффективности классификации КА с использованием мультифрактального анализа

4.1 Мультифрактальный анализ компьютерных атак

Учитывая, что свойство самоподобия наблюдается в широких временных масштабах (например, при различном временном разрешении на уровне бит, пакетов, потоков и т.д.), наличие в сигнале продолжительных атак и аномальной активности изменяет самоподобную природу трафика, приводит к мультифрактальной структуре обрабатываемых процессов [105, 106].

Информация о различии ФР обрабатываемых процессов (если они доступны для обработки) при разном разрешении по времени (мультифрактальности) может быть использована для модификации рассмотренных алгоритмов обнаружения/ классификации КА и может привести к улучшению показателей классификации методами машинного обучения [107-109].

Если фрактал может быть представлен одной величиной — фрактальной размерностью D, то для описания мультифрактала требуется множество таких размерностей. В связи с этим для описания мультифрактала широко используется мультифрактальный спектр,

Чтобы обнаружить связь между поведением исследуемого процесса и его мультифрактальными характеристиками введем другое понятие мультифрактального спектра фрактальной размерности (МСФР) исследуемого процесса.

Под МСФР будем понимать последовательность текущих оценок ФР $\widehat{H}_{t_{Д_i}}$ в окне анализа Δ фиксированной длины $\Delta{=}const$ в зависимости от интервала разрешения (времени дискретизации $t_Д$):

$$\{\widehat{H}_{t_{Д_i}} = f\left(t_{Д_i}\right);\ i = \overline{1,L};\ t_{Д_i} \in \Delta;\ \Delta = const\}. \quad (4.1)$$

На разных временных шкалах (при разном временном разрешении) величина ФР изменяется, так что наблюдаемый процесс можно считать мультифрактальным. В общем случае оценка ФР является случайной величиной $\widehat{H} \in N(m_{\widehat{H}}, \sigma^2_{\widehat{H}})$ и полно характеризуется моментами распределения – средним значением $m_{\widehat{H}}$ и дисперсией $\sigma^2_{\widehat{H}}$ оценки.

Для оценки характеристик МСФР рассматриваемых процессов в сетях IoT в виде (4.1) были выбраны следующие параметры : окно оценки ФР Δ= 2000 отсчетов ; количество окон L=5, так что $i = \overline{1,5}$; время дискретизации наблюдаемых процессов в анализируемых пяти окнах : $t_{Д_1} = 100$мс; $t_{Д_2} = 500$мс; $t_{Д_3} = 1$сек; $t_{Д_4} = 2$сек; $t_{Д_5} = 10$сек; соотвественно.

Для оценки текущих значений ФР в режиме реального времени предлагается использовать оценки фрактальной размерности (показателя $\widehat{H}$) в скользящем окне методами дискретного вейвлет-анализа [75].

Рассмотрим процесс формирования оценки ФР на примере трафика IoT при воздействии атаки Mirai в скользящем окне размером Δ= 2000 отсчетов представленный на рисунке 2.

Пусть $\{X(ti), \overline{\imath = 1, I}\}$ будет дискретным случайным процессом, определенным на интервале $i = 1 \ldots I$ и пусть разложение трафика по вейвлет коэффициентам осуществляется в скользящем окне размера Δ. Смещение окна анализа осуществляется с шагом К ≤ Р. В результате при смещении окна анализа слева направо положение окна пробежит m положений $M = \frac{\text{P}}{K}, m = \overline{1, M}$. Тогда вейвлет-коэффициенты детализации при m -ом положении окна $d^m_{j,k}$ могут быть найдены в конце анализируемого интервала.

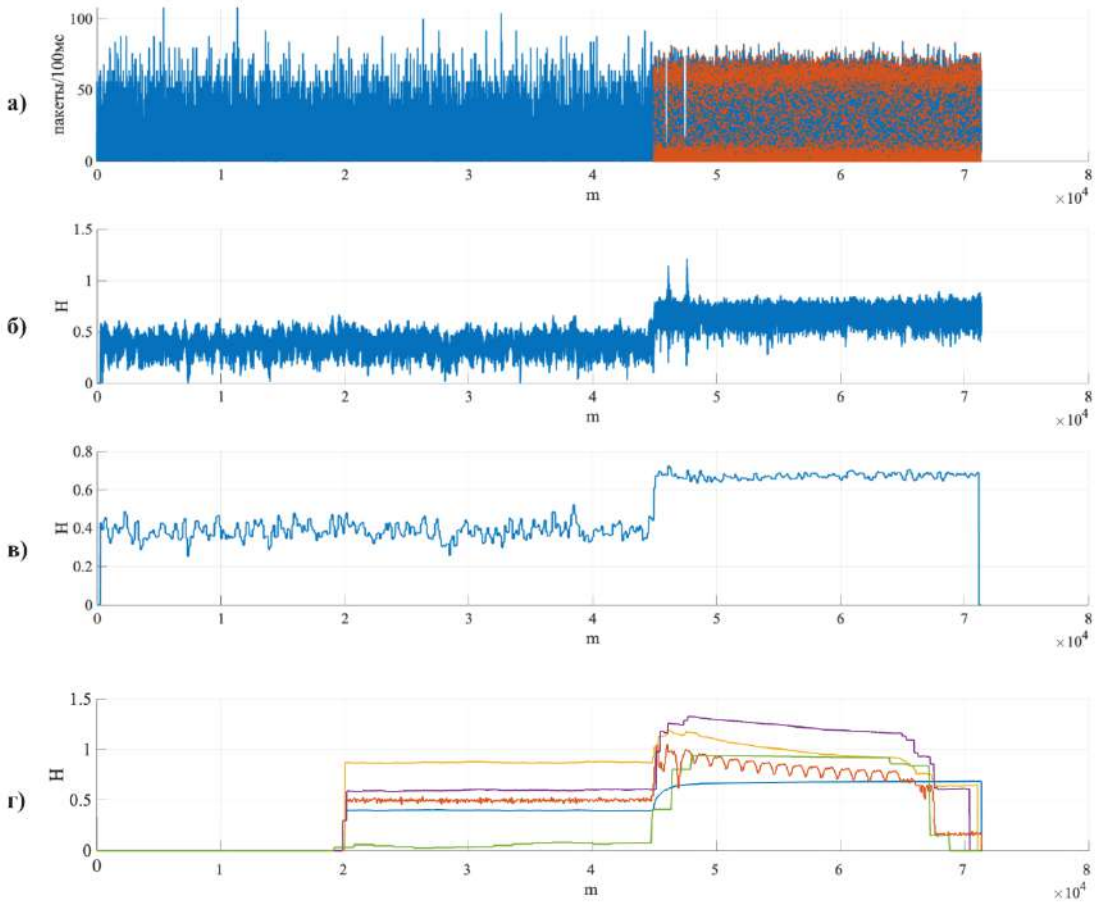


Рисунок 4.1 – Оценка ФР трафика IoT при воздействии атаки Mirai в скользящем окне размером а) фрагмент трафика с атакой Mirai, б) Текущая оценка $\widehat{H}$ в скользящем окне без фильтрации; в) оценка $\widehat{H}$ в скользящем окне с фильтрацией; г) Оценка параметров МСФР в скользящем окне при $i = \overline{1,5}$.

На практике при использовании оценки показателя Херста в скользящем окне Δ, оценка формируется с высокой дисперсией и резкими скачками показателя Херста, как это можно заметить на рисунке 2б. Для нейтрализации резких выбросов и уменьшения дисперсии в [45,75,76] предлагается воспользоваться процедурой трешолдинга (thresholding) – фильтрацией оценки, рассмотренной в главе 2.

По итогам исследования были получены значения МСФР для нормального трафика в разных точках описанной топологии сети IoT и разных типов КА. В таблице 4.1 приведены статистические характеристики оценок показателя Херста $\widehat{H}$ в скользящем окне с применением процедуры трешолдинга для пяти окон оцениванияя размером 100 мс, 500 мс, 1,5 с, 10 с и 1 мин соответственно с учетом коэффициентов «старения» λ (λ =5, 3, 1, 0.1, 0.01).

Таблица 4.1 — Статистические характеристики оценки трафика IoT с трешолдингом

$t_{Д_i}$	$m_{\widehat{H}}$ нормального трафика	$\sigma^2_{\widehat{H}}$ нормального трафика	$\sigma_{\widehat{H}}$ нормального трафика	$m_{\widehat{H}}$ атаки	$\sigma^2_{\widehat{H}}$ атаки	$\sigma_{\widehat{H}}$ атаки
100 мс	0.3983	0.00003	0.0019	0.6745	0.000075	0.0087
500 мс	0.5285	0.00096	0.0098	0.8089	0.0065	0.0804
1 сек	0.6987	0.000069	0.0084	1.073	0.0054	0.0732
2 сек	0.4080	0.0027	0.0522	1.1703	0.0027	0.052
10 сек	0.0646	0.0002	0.0143	0.9303	0.0004	0.007

Количественный анализ полученных результатов показывает, что в отсутствии КА трафик IoT характеризуется оценками среднего значения $m_{\widehat{H}}$ в интервале {0 ….0.5}, для интервалов дискретизации $t_{Д_1} = 100$мс; $t_{Д_4} = 2$сек и $t_{Д_5} = 10$сек, что означает, то анализируемый случайный процесс не обладает самоподобием. При $t_{Д_2} = 500$мс и $t_{Д_3} = 1$сек значение $m_{\widehat{H}}$ лежит в диапазоне {0,5...1,0}, что свидетельствует о наличии фрактальных свойств у нормального трафика при этом временном разрешении.

Для КА типа Mirai фрактальными свойствами атака обладает при $t_{Д_1} = 100$мс; $t_{Д_2} = 500$мс и $t_{Д_5} = 10$ сек.

В этом случае значение $m_{\widehat{H}}$ лежит в диапазоне {0,5...1,0}, что свидетельствует о наличии фрактальных свойств у КА при этом временном разрешении.

При $t_{Д_3} = 1$сек; $t_{Д_4} = 2$сек параметр $m_{\widehat{H}}$>1, что указывает на наличие аномалий или на нестационарность обрабатваемого процесса.

Указанные значения ФР могут быть использованы в качестве дополнительных атрибутов алгоритма обнаружения атак в сетях IoT для атаки Mirai. На рисунке 4.2 показаны оценки $\widehat{m_{\widehat{H}}}$ в скользящем окне Δ при различном временном разрешении.

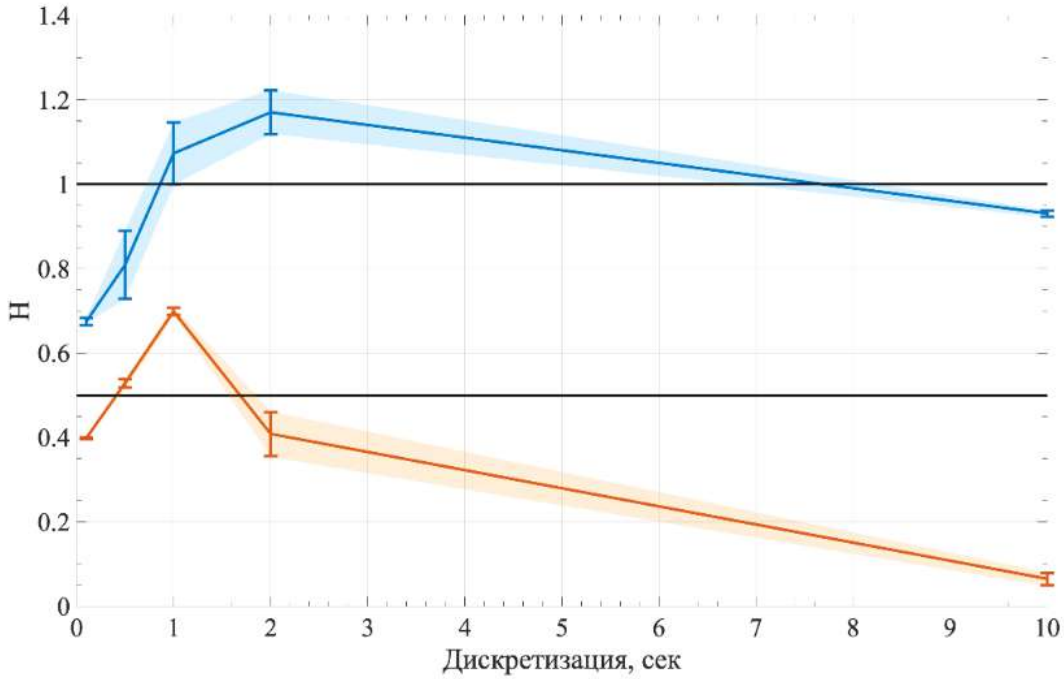


Рисунок 4.2 — Оценка показателя Херста на атаке Mirai и нормального трафика отфильтрованная оценка без аномальных выбросов при разном временном разрешении

Величина $\widehat{H}$ обычно характеризует степень самоподобия процесса следующим образом. Случай 0.5<H<1,0 характеризует трендоустойчивый процесс, обладающий длительной памятью, и является самоподобным. Случай 0 <H <0.5 характерен для случайного процесса, не обладающего самоподобием. Случай H>1,0 соответствует аномалии (нестационарности) анализируемого процесса.

Используя численные значения среднего $m_{\widehat{H}}$ и СКО фрактальной размерности $\sigma_{\widehat{H}}$ нормального трафика и КА представленные в таблице 2 предлагается добавить к уже имеющимся атрибутам значения МСФР нормального трафика и КА типа атаки Mirai, пяти элементов характеризующих $\{\widehat{H}_{t_{Д_i}}, i = \overline{1,5}\}$ как это показано в строке №24 таблицы 4.2. В результате количество атрибутов для нормального трафика и КА типа Mirai, увеличивается до 120.

Таблица 4.2 — Перечень атрибутов в наборе данных Kitsune в разных временных окнах в совокупности с параметрами МСФР

	№ атрибутов в разных	**Атрибут**
1	1, 24, 47, 70, 93	Длина комбинации MAC-IP в битах, (μ)
2	2, 25, 48, 71, 94	Длина SrcIP в битах, (μ)
3	3, 26, 49, 72, 95	Длина Channel в битах, (μ)
4	4, 27, 50, 73, 96	Длина Socket в битах, (μ)
5	5, 28, 51, 74, 97	Длина комбинации MAC-IP в битах, (σ)
6	6, 29, 52, 75, 98	Длина SrcIP в битах, (σ)
7	7, 30, 53, 76, 99	Длина Channel в битах, (σ)
8	8, 31, 54, 77, 100	Длина Socket в битах, (σ)
9	9, 32, 55, 78, 101	Длина Channel в битах, (M_{ij})
10	10, 33, 56, 79, 102	Длина Socket в битах, ($M_{ij)}$
11	11, 34, 57, 80, 103	Длина Channel в битах, (Q_{ij})
12	12, 35, 58, 81, 104	Длина Socket в битах, (Q_{ij})
13	13, 36, 59, 82, 105	Длина Channel в битах, ($Cov_{i,j}$)
14	14, 37, 60, 83, 106	Длина Socket в битах, ($Cov_{i,j}$)
15	15, 38, 61, 84, 107	Длина Channel в битах, (R_{ij})
16	16, 39, 62, 85, 108	Длина Socket в битах, $\left(R_{ij}\right)$
17	17, 40, 63, 86, 109	Количество пакетов MAC-IP, (N)
18	18, 41, 64, 87, 110	Количество пакетов SrcIP в битах, (N)
19	19, 42, 65, 88, 111	Количество пакетов Channel в битах, (N)
20	20, 43, 66, 89, 112	Количество пакетов Socket в битах, (N)
21	21, 44, 67, 90, 113	Межпакетные задержки исходящего трафика, (N)
22	22, 45, 68, 91, 114	Межпакетные задержки исходящего трафика, Channel, (μ)
23	23, 46, 69, 92, 115	Межпакетные задержки исходящего трафика, Channel, (σ)
24	116,117,118,119,120	МСФР данных в окне разрешения $\left\{\widehat{H}_{t_{Д_i}}, i = \overline{1,5}\right\}$

Введенный метод оценки мультифрактального спектра фрактальной размерности (МСФР) в виде последовательности текущих оценок ФР $\widehat{H}_{t_{Д_i}}$ в окне анализа Δ фиксированной длины Δ=const в зависимости от интервала разрешения.

Найденные экспериментальные значения параметров МСФР, представленные в виде дополнительных атрибутов в таблице 4.2 (атрибуты №116…120) представляют собой текущие оценки ФР $\widehat{H}_{t_{Д_i}}$ в окне анализа Δ для различных интервалов разрешения.

Полученные дополнительные атрибуты могут быть использованы для повышения достоверности обнаружения и качества классификации КА методами машинного обучения в сетях IoT.

Предлагаемый способ оценки МСФР может быть положен в основу нового метода повышения качества классификации КА с использованием методов машинного обучения.

4.2 Метод классификации КА с учетом параметров МСФР

Оценим эффективность метода добавления МСФР к исходным данным на примере набора данных Kitsune [110-114]. Набор данных Kitsune содержит 115 атрибутов метрического типа. Для оценки эффективности проведем два эксперимента:

– Решение задачи бинарной классификации КА типа «Mirai Botnet» для двух случаев: Kitsune без модификаций; Kitsune с добавлением МСФР.

– Решение задачи многоклассовой классификации КА типов «Mirai Botnet» и «OS Scan» для двух случаев: Kitsune без модификаций; Kitsune с добавлением МСФР.

Для решения задачи классификации выбран алгоритм типа «Случайный лес» (Random Forest) в стандартной реализации библиотекой scikit-learn. Выбор алгоритма обусловлен широтой применения указанного алгоритма для решения задач однозначной классификации [115-125].

С целью дополнительного уточнения степени влияния МСФР на результаты классификации эксперименты проводились для двух наборов гиперпараметров «Случайного леса»: «глубина решающего дерева» = {2, 5}. Глубина дерева решений — это гиперпараметр, который определяет количество уровней или узлов от корня до

любого листа. Глубина дерева определяется количеством уровней, не включая корневой узел.

Сведем параметры экспериментов в таблицу (табл. 4.3).

Таблица 4.3 — Параметры проводимых экспериментов для оценки эффективности добавления МСФР

№ эксперимента	**Тип задачи**	**«Глубина решающего дерева»**	**Добавление МСФР для КА «Mirai Botnet»**
1	Бинарная классификация: Mirai Botnet и Normal	2	нет
		5	нет
		2	да
		5	да
2	Многоклассовая классификаци: Mirai Botnet, OS scan и Normal	2	нет
		5	нет
		2	да
		5	да

Структура данных Kitsune сформирована для решения задач бинарной классификации. Для каждой КА авторами представлен отдельный набор данных. В каждом наборе данных содержатся записи моментов нормального функционирования КС и записи, маркированные соответствующей КА. Размерность каждого набора данных одинакова – 115 атрибутов. Количество записей в каждом наборе данных разное.

Объем набора данных для КА «Mirai Botnet» - 764 136 шт. записей, из них 121 620 шт. (16%) относятся к КА. Объем набора данных для КА «OS Scan» - 1 697 850 шт. записей, из них 65 700 шт. (4%) относятся к КА, а 1 632 150 шт. относятся к нормальному трафику

Для проведения эксперимента №2 наборы данных для КА «Mirai Botnet» и «OS Scan» объединялись посредством операции конкатенации. При проведении эксперимента с МСФР, для всех записей, не относящихся к исходному набору КА «Mirai Botnet», атрибуты 116 … 120, связанные с МСФР, считались равными 0.

Дополнительно оценим влияние добавления МСФР по информативности атрибутов (индекс Джини) [39] в каждом из двух экспериментов. Индекс Джини, обычно используемый в деревьях решений и других алгоритмах машинного обучения является показателем для измерения того, как часто случайно выбранный элемент будет неправильно идентифицирован. Индекс Джини - рассчитывается путем суммирования квадратов вероятностей каждого результата в распределении и вычитания результата из 1. Индекс Джини представляется формулой:

$$Gini(T) = 1 - \sum_{i=1}^{n} p_i^2 , \quad (4.2)$$

где T – множество объектов обучающей выборки; n – количество классов; p_i – вероятность встречаемости класса i в множестве T.

4.3 Информативная значимость атрибутов КА при учете дополнительных параметров МСФР

Для оценки влияния на качество классификации КА введенных дополнительных параметров МСФР была оценена их информационная значимость в случае бинарной и многоклассовой классификации [108,109]. Результаты оценки информативной значимости по индексу Джини без добавления МСФР и с добавлением МСФР – приведены в виде гистограмм на рис.4.3. Оценка информативности проводилась относительно классовых меток о наличии (отсутствии) КА «*Mirai Botnet*».

Для сопоставления размерности гистограмм, в первом случае оценка важности по представленным в таблице 1 атрибутам 116–120 присвоена равной 0.

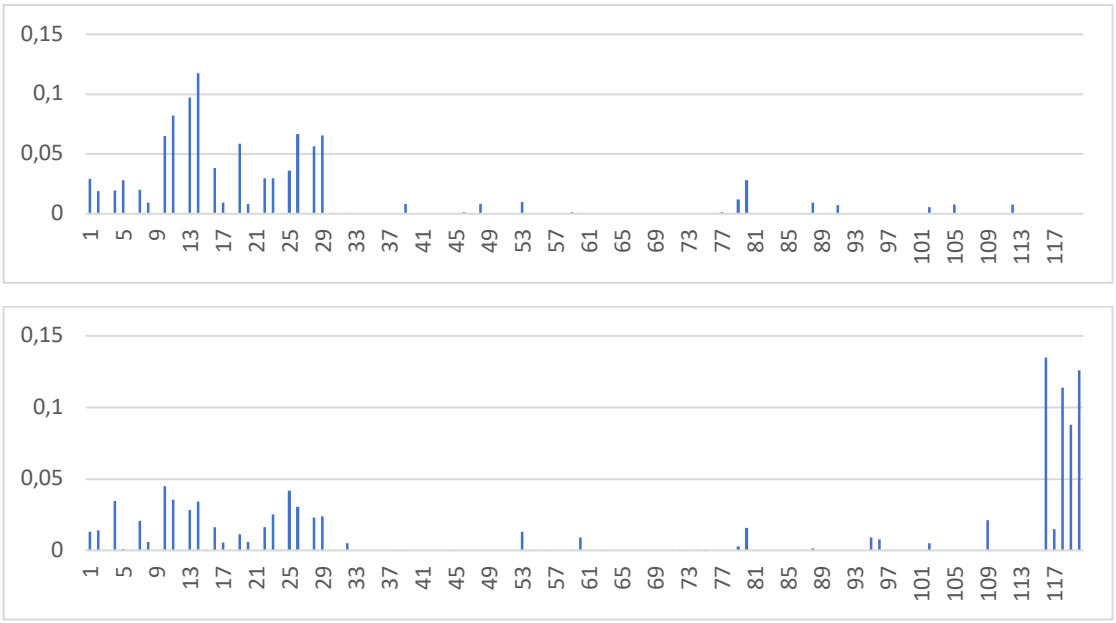


Рисунок 4.3 — Оценка информативной значимости атрибутов в задаче бинарной классификации КА «*Mirai Botnet*» по индексу Джини для двух случаев: а) без добавления МСФР (атрибуты 116–120 приравнены 0); б) с добавлением МСФР.

Анализ распределения на рис. 4.3.а показал, что наиболее информативными являются атрибуты КС, полученные во временном окне 100 мс (см. табл. 4.1 и $\lambda = 5$).

Был проведен анализ первых 15 наиболее значимых атрибутов для двух случаев - без добавления МСФР и с добавлением МСФР. Для иллюстрации приводится модифицированная таблица 4.4. Атрибуты, имеющие ранг 1 … 15, имеют цветовой маркер:

- Желтый, если атрибут находится в распределении без добавления МСФР;
- Зеленый, если атрибут находится в распределении с добавлением МСФР;
- Фиолетовым, если атрибут находится в двух распределениях одновременно.

Таблица 4.4 — Распределение первых 15 атрибутов для данных с и без добавления МСФР для случая бинарной классификации

№	№ атрибутов в разных временных окнах	№	№ атрибутов в разных временных окнах	№	№ атрибутов в разных временных окнах
1	**1**, 24, 47, 70, 93	9	9, 32, 55, 78, 101	17	17, 40, 63, 86, **109**
2	2, **25**, 48, 71, 94	10	**10**, 33, 56, 79, 102	18	18, 41, 64, 87, 110
3	3, **26**, 49, 72, 95	11	**11**, 34, 57, **80**, 103	19	**19**, 42, 65, 88, 111
4	**4**, 27, 50, 73, 96	12	12, 35, 58, 81, 104	20	20, 43, 66, 89, 112
5	**5**, **28**, 51, 74, 97	13	**13**, 36, 59, 82, 105	21	21, 44, 67, 90, 113
6	6, **29**, 52, 75, 98	14	**14**, 37, 60, 83, 106	22	**22**, 45, 68, 91, 114
7	7, 30, 53, 76, 99	15	15, 38, 61, 84, 107	23	**23**, 46, 69, 92, 115
8	8, 31, 54, 77, 100	16	**16**, 39, 62, 85, 108	24	**116**, 117, **118**, **119**, **120**

В число первых 15 наиболее значимых атрибутов, вычисленных для случая без добавления МСФР, попало 10 атрибутов, вычисленных во временном окне 100 мс; 4 атрибута, вычисленных для временного окна 500 мс; 1 атрибут (связанный с дисперсией длины Channel в битах), вычисленный для временного окна 10 с. Анализ наиболее значимых атрибутов выявил только 2 «дублирования» по разным временным окнам (атрибуты №5 и №28 – σ длин комбинаций MAC-IP в битах и атрибуты №11 и №80, дисперсия длины Channel в битах), в остальном все значимые атрибуты уникальны и не пересекаются.

«Концентрация» наиболее значимых атрибутов в области $\lambda = 5$ может быть обусловлена возможностью детектирования КА «Mirai Botnet» во временном окне 100 мс. Атрибуты, вычисленные в других временных окнах, являются вспомогательными.

Добавление МСФР в атрибутное пространство изменяет распределение его информационной значимости по оси ординат (атрибуты 1 … 115 снизили значимость, в среднем, на 50%, однако их ранжирование практически не претерпело изменений).

Анализ 15 наиболее значимых атрибутов с учетом добавления МСФР показал, что 6 из 15 атрибутов (40%) – уникальны. В их число включается 4 атрибута, связанных с МСФР.

7 атрибутов из 15 вычислены во временном окне 100 мс. Четыре атрибута - вычислены для временного окна 500 мс. Один атрибут вычислен для временного окна 1.5 с. Один атрибут вычислен для временного окна 2 с и 2 атрибута вычислены для временного окна 10 с.

Анализ атрибутов № 116 … 120, связанных с МСФР, демонстрирует корреляцию, близкую к линейной, между МСФР и классовыми метками о наличии (отсутствии) КА «*Mirai Botnet*». Столь высокая корреляция обусловлена тем, что во время проведения КА «*Mirai Botnet*» ряд атрибутов КС, связанных с сетевым взаимодействием (в табл. 4.4, атрибуты №10, №11, №13 и №14, связаны с количеством исходящих пакетов), резко меняют свое распределение (количество пакетов резко возрастает).

Таким образом, добавление МСФР в атрибутное пространство изменяет распределение его информационной значимости по оси ординат. Так атрибуты 1 … 115 снизили значимость в среднем на 50%, однако их ранжирование практически не претерпело изменений.

Оценка информативности атрибутов в задаче многоклассовой классификации КА «*Mirai Botnet*» и «*OS Scan*» по критерию Джини представлена на рисунке 4. 4.

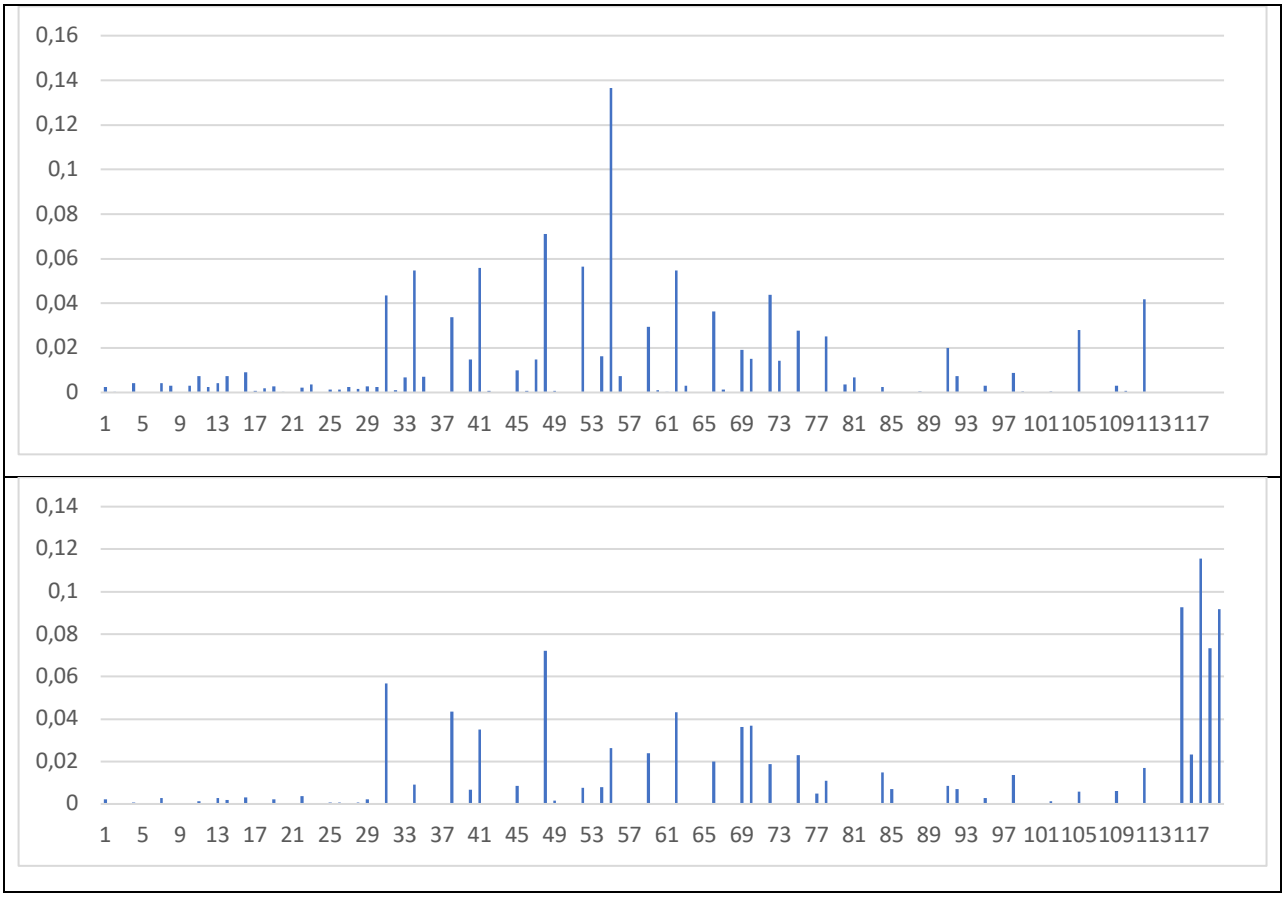


Рисунок 4.4 – Оценка информативной значимости атрибутов в задаче многоклассовой классификации КА «*Mirai Botnet*» и «*OS Scan*» по критерию Джини для двух случаев: а) без добавления фрактальной размерности (атрибуты 116–120 приравнены 0); б) с добавлением фрактальной размерности.

В сравнении с рисунком 4.3 из данных представленных на рисунке 4.4 видно, что распределение атрибутного пространства «сдвинуто» в сторону более широкого временного окна 500 мс (атрибуты с 24 по 46) и 1,5 с (атрибуты с 47 по 69).

Аналогично случаю бинарной классификации, был проведен анализ первых 15 наиболее значимых атрибутов для двух случаев - без добавления МСФР и с добавлением МСФР. Для иллюстрации последующих выводов атрибуты, приводится модифицированная таблица 4.5. Атрибуты, имеющие ранг 1… 15, имеют цветовой маркер:

- Желтый, если атрибут находится в распределении без добавления МСФР;

- Зеленый, если атрибут находится в распределении с добавлением МСФР;
- Фиолетовым, если атрибут находится в двух распределениях одновременно.

Таблица 4.5 — Распределение первых 15 атрибутов для данных с и без добавления МСФР для случая многоклассовой классификации

№	№ атрибутов в разных временных окнах	№	№ атрибутов в разных временных окнах	№	№ атрибутов в разных временных окнах
1	1, 24, 47, **70**, 93	9	9, 32, **55**, **78**, 101	17	17, 40, 63, 86, 109
2	2, 25, **48**, 71, 94	10	10, 33, 56, 79, 102	18	18, **41**, 64, 87, 110
3	3, 26, 49, **72**, 95	11	11, **34**, 57, 80, 103	19	19, 42, 65, 88, 111
4	4, 27, 50, 73, 96	12	12, 35, 58, 81, 104	20	20, 43, **66**, 89, **112**
5	5, 28, 51, 74, 97	13	13, 36, **59**, 82, **105**	21	21, 44, 67, 90, 113
6	6, 29, **52**, **75**, 98	14	14, 37, 60, 83, 106	22	22, 45, 68, 91, 114
7	7, 30, 53, 76, 99	15	15, **38**, 61, 84, 107	23	23, 46, **69**, 92, 115
8	8, **31**, 54, 77, 100	16	16, 39, **62**, 85, 108	24	**116, 117, 118, 119, 120**

Как видно, в число первых 15 наиболее значимых атрибутов, вычисленных для случая без добавления МСФР, не попало ни одного атрибута, вычисленного для временного окна в 100 мс. Основная концентрация атрибутов наблюдается на интервал 500 мс. …. 1,5 с и составляет 67%, остальные атрибуты распределены в диапазоне 2 с и 10с. «Сдвиг» информационной значимости атрибутов в область более широких временных окон может быть обусловлен наличием атаки второго типа – «OS Scan», а также большого количества данных о нормальном функционировании КС. С учетом объединения наборов данных (для КА «Mirai Botnet», «OS Scan») доля «нормальных» записей в итоговом наборе составляет 92% (2 274 666 шт.) против 84% (642 516 шт.) в исходном наборе данных «Mirai Botnet».

При классификации двух КА в условиях усилившегося дисбаланса классов, временное окно в 100 мс не является достаточно информативным. Больше

информации может быть извлечено из атрибутов, полученных на временных окнах от 500 мс и выше.

Анализ 15 наиболее значимых атрибутов с учетом добавления МСФР позволил сделать выводы, схожие со случаем бинарной классификации. Семь из 15 атрибутов (47%) – уникальны. В их число входят 5 атрибутов (против 4 атрибутов в случае бинарной классификации), связанных с МСФР. Линейная корреляция между МСФР и классовыми метками о наличии или отсутствии КА «*Mirai Botnet*» сохраняется.

Таким образом добавление фрактальной размерности КА «*Mirai Botnet*» в атрибутное пространство изменяет распределение информативности атрибутов аналогично эксперименту с бинарной классификацией. Изменение по оси ординат не столь выраженно, поскольку фрактальная размерность добавлена только для КА «*Mirai Botnet*».

Полученные дополнительные атрибуты могут быть использованы для повышения достоверности обнаружения и качества классификации КА методами машинного обучения в сетях IoT.

Найденные распределения информационной значимости атрибутов нормального трафика и КА, могут быть использованы для решения задачи классификации КА в сетях IoT методами машинного обучения.

Для задачи бинарной классификации КА типа «Mirai Botnet» для двух случаев: без добавления и с добавлением МСФР, получена оценка информативной значимости атрибутов по индексу Джини. Показано, что наиболее информативными являются атрибуты КС, полученные во временном окне 100 мс.

Добавление МСФР в атрибутное пространство изменяет распределение его информационной значимости. Атрибуты № 116 … 120, связанные с МСФР, демонстрируют корреляцию, близкую к линейной, между МСФР и классовыми метками о наличии (отсутствии) КА «*Mirai Botnet*».

Показано, что основная концентрация наиболее значимых атрибутов приходится на интервал 500 мс – 1,5 с (67%), остальные распределены в диапазоне 2с и 10с. «Сдвиг» информационной значимости атрибутов в область более широких

временных окон обусловлен наличием атаки второго типа – «OS Scan», а также большого количества данных о нормальном функционировании КС.

4.4 Результаты многоклассовой классификации КА с учетом МСФР

В результате проведенного эксперимента по многоклассовой классификации получены результаты, представленные в (табл. 4.6) и (табл.4.7). В табл.4.6 приведены результаты оценки качества классификации [108,109] при глубине решающих деревьев *RF depth* 1, а в табл. 4.7 при глубине решающих деревьев *RF depth2*.

Обе таблицы разделены на две части:

В первой части приведены результаты классификации для экспериментальных данных *без добавления* спектра МСФР для КА *«Mirai botnet»* для классовых меток $Label_{\text{experiment}} = (normal, mirai\,botnet, OS\,scan)$, оцененных методом OVR.;

Во второй части приведены результаты классификации для экспериментальных данных с добавлением спектра МСФР для КА *«Mirai botnet»* для классовых меток $Label_{\text{experiment}} = (normal, mirai\,botnet, OS\,scan)$, оцененных методом OVR.

Как видно без добавления МСФР для *«Mirai botnet»,* качество классификации КА *«OS scan»* относительно *«Mirai botnet»* и *«Normal»* близка к идеальной ($AUC_{OVR\ «OS\ Scan»}$ = 0.997). Качество классификации *«Mirai botnet»* относительно *«OS scan»* и *«Normal»* ниже и составляет по метрике $AUC_{OVR\ «Mirai»}$ = 0.937. Оценка качества *«Normal»* относительно *«Mirai botnet»* и *«OS scan»* определяется ошибками классификации для КА.

После добавления МСФР для КА *«Mirai botnet»,* качество классификации *«Mirai botnet»* относительно *«OS scan»* и *«Normal»* возрастает до значений, близких к 1 (выигрыш 7,6% по $AUC_{OVR\ «Mirai»}$). Очевидно, что наблюдаемые ошибки вызваны недостаточной глубиной решающих деревьев.

Анализ оценки качества классификации *«OS Scan»* относительно *«Mirai botnet»* и *«Normal»* выявил незначительное ухудшение показателей эффективности. Анализ структуры алгоритма построения решающих деревьев *RF* показывает, что

деревья формируют решающие правила на основании энтропии по иерархическому принципу. Наибольшая энтропия «сконцентрирована» в атрибутах №116 … 120, и как минимум одно решающее правило каждого дерева (из двух возможных при глубине depth 1) относится к данному множеству. Поскольку атрибуты №116 … 120 не информативны для КА *«OS scan»*, решающие деревья классифицируют данную КА хуже, чем *«Mirai botnet»*.

Таблица 4.6 — Оценки качества многоклассовой классификации алгоритмом RF с depth 1 методом OVR для каждой классовой метки для двух наборов экспериментальных данных для КА «Mirai botnet»

Метрики	Экспериментальные данные без					
	Без добавления МСФР для КА *«Mirai botnet»*			После добавления МСФР для КА *«Mirai botnet»*		
	«Mirai botnet» относительно *«OS scan»* и *«Normal»*	*«OS scan»* относительно *«Mirai botnet»* и *«Normal»*	*«Normal»* относительно *«Mirai botnet»* и *«OS scan»*	*«Mirai botnet»* относительно *«OS scan»* и *«Normal»*	*«OS scan»* относительно *«Mirai botnet»* и *«Normal»*	*«Normal»* относительно *«Mirai botnet»* и *«OS scan»*
accuracy	0,966	0,999	0,966	0,999	0,999	0,999
precision	0,993	1	0,956	1	1	0,999
recall	0,876	0,993	0,998	0,999	0,993	1
f_{score}	0,931	0,997	0,977	0,999	0,996	0,999
ROC AUC_{OVR}	0,937	0,997	0,942	0,999	0,996	0,999

Содержимое табл. 4.6 визуализировано на гистограмме, представленной на рис. 4.5. Построено 5 групп гистограмм по каждой метрике оценки качества классификации. В каждой группе значения упорядочены по двум «тройкам»:

- Экспериментальные данные без добавления спектра МСФР для *«Mirai botnet»: «Mirai botnet»* относительно *«OS scan»* и *«Normal»; «OS scan»*

относительно «Mirai botnet» и «Normal»; «OS scan» относительно «Mirai botnet» и «Normal».

- Экспериментальные данные с добавлением спектра МСФР для *«Mirai botnet»: «Mirai botnet»* относительно *«OS scan»* и *«Normal»; «OS scan» относительно «Mirai botnet» и «Normal»; «OS scan» относительно «Mirai botnet» и «Normal».*

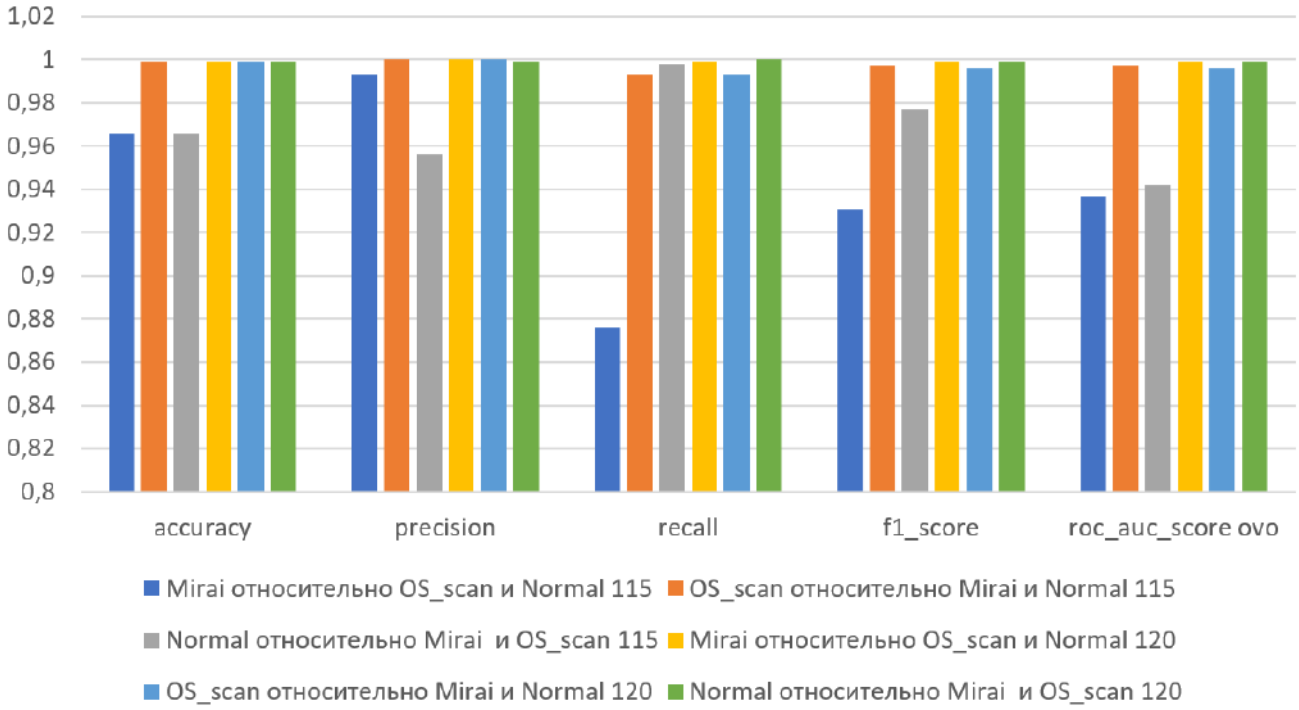


Рис. 4.5 — Визуализация оценки качества многоклассовой классификации алгоритмом RF с глубиной решающего дерева depth 1 OVR для каждой классовой метки для двух наборов атрибутов экспериментальных данных.

Численные значения оценок качества многоклассовой классификации алгоритмом RF с глубиной решающего дерева *depth2* методом OVR для каждой классовой метки для двух наборов экспериментальных данных приведены в табл. 4.7.

В сравнении с данными (табл. 4.7), видно, что при глубине решающего дерева depth 5, каждая из двух КА классифицируется с точностью, близкой к идеальной.

Таблица 4.7 — Сравнительная таблица оценки эффективности многоклассовой классификации алгоритмом RF методом OVR для каждой классовой метки для двух наборов экспериментальных данных

Метрики	Экспериментальные данные					
	Без добавления спектра МСФР в КА *«Mirai botnet»*			после добавления спектра МСФР в КА *«Mirai botnet»*		
	«Mirai botnet» относительно «OS scan» и «Normal»	«OS scan» относительно «Mirai botnet» и «Normal»	«Normal» относительно «Mirai botnet» и «OS scan»	«Mirai botnet» относительно «OS scan» и «Normal»	«OS scan» относительно «Mirai botnet» и «Normal»	«Normal» относительно «Mirai botnet» и «OS scan»
accuracy	0.999	0.999	0.999	1	0.999	0.999
precision	1.0	1.0	0.999	1	1	0.999
recall	0.999	0.991	1.0	1	0.998	1.0
f_{score}	0.999	0.995	0.999	1	0.999	0.999
ROC AUC_{OVR}	0.999	0.995	0.999	1	0.999	0.999

Содержимое табл.4.7 визуализировано на гистограмме рис. 4.6. Для каждой метрики оценки эффективности классификации построено пять групп гистограмм.

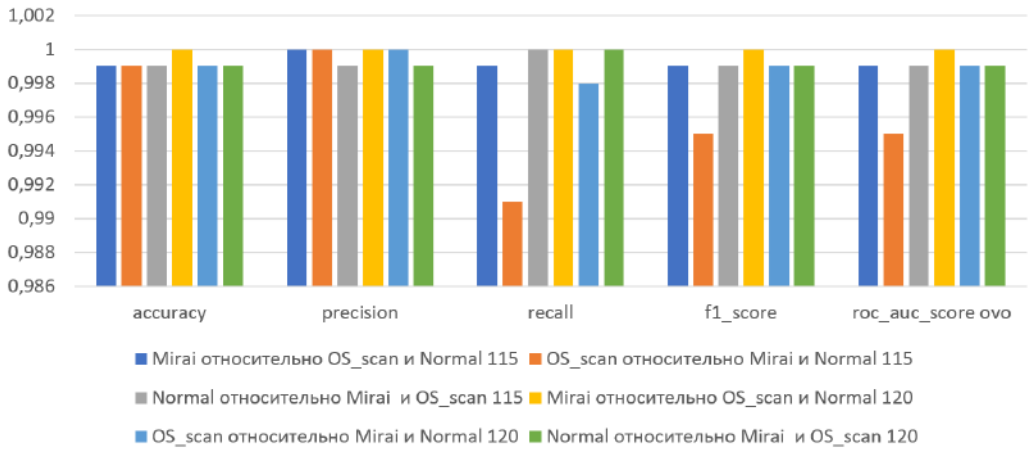


Рис.4.6 — Визуализация оценки эффективности многоклассовой классификации алгоритмом RF с глубиной решающего дерева depth 2 OVR для каждой классовой метки для двух наборов атрибутов экспериментальных данных.

Как видно добавление в качестве дополнительных атрибутов МСФР для КА *«Mirai botnet»,* повышает точность классификации *«Mirai botnet»* относительно *«OS scan»* и *«Normal»* до 1. Это означает, что все записи, связанные с КА *«Mirai botnet»* в тестовой выборке, классифицированы корректно.

Сравнительный анализ эффективности классификации *«OS scan»* относительно *«Mirai botnet»* и *«Normal»* представленных в таблице 4.7 выявил незначительное увеличение качества классификации, связанное с перераспределением информативной значимости атрибутного пространства. В отличие от эксперимента с глубиной решающего дерева *depth* = 2, глубины *depth* = 5 «хватает» для построения эффективных решающих правил.

4.5 Выводы

Введено понятие *мультифрактального спектра фрактальной размерности (МСФР)* в виде последовательности текущих оценок ФР $\widehat{H}_{t_{Д_i}}$ в окне анализа Δ фиксированной длины Δ=const в зависимости от интервала разрешения.

Проведена оценка эффективности добавления МСФР к исходным данным.

Предлагаемый способ оценки МСФР положен в основу нового метода повышения качества классификации КА с использованием методов машинного обучения.

Проведена оценка качества классификации при добавлении МСФР к исходным данным. Оценка проведена для двух групп параметров: информативность атрибутов и эффективность классификации алгоритмом Random Forest. Оценка оценивалась при проведении двух экспериментов: решение задачи бинарной классификации КА типа «Mirai Botnet» (первый эксперимент) и многоклассовой классификации КА типов «Mirai Botnet» и «OS Scan» для наборов данных Kitsune без модификаций; для набора данных Kitsune с добавлением МСФР.

Показано, что в случае бинарной классификации добавление МСФР КА «*Mirai Botnet*» в атрибутное пространство позволяет однозначно классифицировать указанную КА без ложноположительных и ложноотрицательных результатов классификации.

В случае многоклассовой классификации, при добавлении МСФР, точность классификации *«Mirai botnet»* алгоритмом Random Forest при глубине решающего дерева depth = 2 относительно *«OS scan»* и *«Normal»* возрастает до значений, близких к 1 (выигрыш 7,6% по $AUC_{OVR\ «Mirai»}$). Наблюдаемые ошибки вызваны недостаточной глубиной решающих деревьев. Добавление в качестве дополнительного параметра фрактальной размерности для КА *«Mirai botnet»* при глубине решающего дерева depth = 5*,* повышает точность классификации *«Mirai botnet»* относительно *«OS scan»* и *«Normal»* до 1. Добавление МСФР при глубине решающего дерева depth = 5*,* позволяет достичь идеальной классификации КА ($AUC_{OVR\ «Mirai»} = 1$).

Для проведения эксперимента №2 наборы данных для КА «Mirai Botnet» и «OS Scan» объединялись посредством операции конкатенации. При проведении эксперимента с МСФР, для всех записей, не относящихся к исходному набору КА «Mirai Botnet», атрибуты 116 … 120, связанные с МСФР, считались равными 0.

В эксперименте, связанном с решением задачи бинарной классификации КА типа «Mirai Botnet» для двух случаев: Kitsune без модификаций; Kitsune с добавлением МСФР, получена оценка информативности атрибутов в задаче бинарной классификации КА «*Mirai Botnet*» по индексу Джини. Показано, что наиболее информативными являются атрибуты КС, полученные во временном окне 100 мс.

Исследовано распределения первых 15 атрибутов для двух случаев. Показано, что «концентрация» наиболее значимых атрибутов в области $\lambda = 5$ обусловлена возможностью детектирования КА «Mirai Botnet» во временном окне 100 мс. Добавление МСФР в атрибутное пространство изменяет распределение его информационной значимости. Анализ атрибутов № 116 … 120, связанных с МСФР, показывает корреляцию, близкую к линейной, между МСФР и классовыми метками о наличии (отсутствии) КА «*Mirai Botnet*».

Добавление МСФР КА «*Mirai Botnet*» в атрибутное пространство для случая бинарной классификации позволяет однозначно классифицировать указанную КА (без ложноположительных и ложноотрицательных результатов классификации). Добавление МСФР позволяет достичь идеальной классификации КА ($ROC_{AUC} = 1$) при любой глубине решающего дерева.

В эксперименте, связанном с решением задачи многоклассовой классификации КА типов «Mirai Botnet» и «OS Scan» для двух случаев: Kitsune без модификаций; Kitsune с добавлением МСФР, получена оценка информативности атрибутов в задаче бинарной классификации КА «*Mirai Botnet*» по индексу Джини и проведено сравнение с случаем бинарной классификации.

Обнаружено изменение распределения атрибутов по временным окнам для выборки из первых 15 наиболее значимых атрибутов. Основная концентрация наиболее значимых атрибутов приходится на интервал 500 мс – 1,5 с (67%), остальные распределены в диапазоне 10 с и 1 мин. «Сдвиг» информационной значимости атрибутов в область более широких временных окон обусловлен наличием атаки второго типа – «OS Scan», а также большого количества данных о нормальном функционировании КС.

При добавлении МСФР точность классификации *«Mirai botnet»* алгоритмом Random Forest при глубине решающего дерева depth = 2 относительно *«OS scan»* и *«Normal»* возрастает до значений, близких к 1 (выигрыш 7,6% по $AUC_{OVR\ «Mirai»}$). Наблюдаемые ошибки вызваны недостаточной глубиной решающих деревьев. Добавление фрактальной размерности для КА *«Mirai botnet»* при глубине решающего дерева depth = 5, повышает точность классификации *«Mirai botnet»* относительно *«OS scan»* и *«Normal»* до 1. Следовательно, добавление МСФР при глубине решающего дерева depth = 5, позволяет достичь идеальной классификации КА ($AUC_{OVR\ «Mirai»} = 1$).

ЗАКЛЮЧЕНИЕ

В диссертационной работе решена актуальная научная задача, заключающаяся в разработке научно-методического аппарата для повышения качества обнаружения и классификации атак в компьютерных сетях путем комбинации методов мультифрактального анализа и машинного обучения.

Задача имеет важное значение для «раннего» выявления атак в сетях, находящихся под воздействием как известных, так и неизвестных атак, а также прогнозирования их присутствия/отсутствия в трафике. Это подтверждается следующими полученными научными и практическими результатами:

1. Разработана и программно реализована новая модель оценки фрактальных параметров компьютерных атак, отличающаяся от известных наличием дополнительной фильтрацией, повышающей точность оценки в скользящем окне фрактальной размерности атак на 15…40% для различных типов материнских вейвлетов, что, в свою очередь, в онлайн режиме повышает достоверность обнаружения атак до 10% по сравнению с известными аналогами.

2. Для повышения точности классификации методами машинного обучения предложено использовать в качестве дополнительных информационных атрибутов атак среднее значение, дисперсию, коэффициенты асимметрии и эксцесса плотности распределения фрактальной размерности, что повышает точность классификации в среднем на 10%.

3. Для различных экспериментальных баз данных, с использованием разработанных алгоритмов, определены статистические параметры фрактальной размерности сетевого трафика при наличии и отсутствии атак, позволяющие использовать их в алгоритмах обнаружения и классификации.

4. Учет дополнительных статистических параметров фрактальной размерности, характеризующих плотность распределения показателя Херста w(H), улучшает качество и быстродействие бинарной классификации, а наиболее эффективными являются алгоритмы DTC и RF.

5. Использование одного дополнительного параметра (среднего значения) приводит к снижению времени на обучение и тестирование для алгоритма DTC в 1,5 раза, а для RF – в 2 раза. Использование 4-х дополнительных атрибутов приводит к снижению времени на обучение и тестирование для алгоритмов DTC и RF в 3,5 раза.

6. Введено понятие и определена модель мультифрактального спектра фрактальной размерности в виде последовательности текущих оценок ФР в окне анализа фиксированной длины (в зависимости от выбираемого интервала разрешения), которое важно для формализации новых полезных признаков классификации компьютерных атак. Показана целесообразность использования характеристик МСФР, для повышения точности классификации атак за счет увеличения информативности обрабатываемых потоков.

7. Разработаны метод и соответствующий алгоритм композиции машинного обучения и мультифрактального анализа, повышающие точность многоклассовой классификации атак на 7-10%, обоснованы границы изменения входных параметров алгоритма, обеспечивающие нормальное функционирование предложенных алгоритмов.

Результаты проведенного диссертационного исследования соответствуют паспорту специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Рекомендации. Результаты диссертационного исследования целесообразно внедрять в системы мониторинга корпоративных сетей в качестве надстроек к системам анализа сетевого трафика и управления событиями безопасности. Практическая ценность разработанного подхода состоит в раннем фиксировании изменений состояния трафика и последующей классификации инцидентов. Для этого рекомендуется использовать онлайн-оценку показателя Херста с последующей обработкой детализирующих вейвлет-коэффициентов как детектор смены режима. Наиболее устойчивые оценки на практике дают материнский вейвлет типа Хаар и временные окна порядка от 100 мс до 2-х минут; пороговые значения показателя Херста следует калибровать на эталонном «нормальном»

профиле сетевого трафика корпоративной сети. В задачах классификации полезно включать в признаковое описание не только сам показатель Херста, но и его статистические характеристики (среднее значение, дисперсия, асимметрия, эксцесс), что заметно повышает точность при умеренных вычислительных затратах. В условиях ограниченных ресурсов оправдано применение решающих деревьев и их ансамблей.

Для устойчивого многоклассового распознавания атак целесообразно дополнять признаки параметрами мультифрактального спектра, то есть оценками, которые отражают поведение трафика на разных временных масштабах. Такая комбинация улучшает полноту и точность распознавания компьютерных атак и снижает остаточные ошибки при усложнении моделей. Перед внедрением в корпоративную среду необходима первичная настройка на репрезентативных срезах реального трафика конкретной организации с параллельной проверкой на известных наборах данных (DARPA, UNSW-NB15, Kitsune), что обеспечивает переносимость решений между традиционными сегментами и IoT-инфраструктурой при корректной калибровке параметров. Разработанный программный инструментарий рекомендуется также использовать (и уже используется) в учебном процессе при подготовке специалистов по информационной безопасности.

Перспективы дальнейшей разработки темы связаны с повышением устойчивости и интерпретируемости детектирования в нестационарных сетевых условиях. Методически важно развить адаптивные онлайн-процедуры учета «дрейфа концепции»: динамическую нормализацию данных, самонастройку порогов и размеров окон, а также автоматический выбор материнского вейвлета в зависимости от текущей динамики трафика. Отдельной задачей видится строгая оценка доверительных интервалов для параметров мультифрактального спектра с заданными уровнями ошибок первого и второго рода на различных временных масштабах. Практически значимым направлением является распространение методики на шифрованный трафик (TLS/QUIC), промышленные и

киберфизические сети, где традиционные содержательные признаки ограничены, а фрактальные характеристики сохраняют информативность.

Логичным шагом дальнейших исследований в данном направлении является интеграция предложенных алгоритмов в модуль предиктивной аналитики, ориентированный на раннее предупреждение о приближении к критическим состояниям сети по динамике показателя Херста и метрик мультифрактального спектра. Реализация перечисленных направлений позволит дополнительно повысить достоверность обнаружения и точность классификации атак, снизить стоимость программной реализации разработанных моделей, обеспечить практическую реализуемость предложенного подхода в широком спектре эксплуатационных сценариев.

СПИСОК ЛИТЕРАТУРЫ

1. Raimundo, M., Okamoto Jr., J. Application of Hurst Exponent (H) and the R/S Analysis in the Classification of FOREX Securities // International Journal of Modeling and Optimization. – 2018. – Vol. 8. – P. 116–124.

2. Sánchez-Granero, M., Fernández-Martínez, M., Trinidad-Segovia, J. Introducing fractal dimension algorithms to calculate the Hurst exponent of financial time series // Eur. Phys. J. B. – 2012. – Vol. 85. – Art. 86.

3. Grillo, D., Lewis, A., Pandya, R. Personal Communication Services and Teletraffic Standardization in ITU-T // The Fundamental Role of Teletraffic in the Evolution of Telecommunications Networks : proceedings of the 14th International Teletraffic Congress - ITC 14, Antibes Juan-les-Pins, France, 6-10 June, 1994 / ed. by J. Labetoulle and J.W. Roberts. – Elsevier Science, 1994. – P. 1–12.

4. Strelkovskaya, I., Solovskaya, I., Makoganiuk, A. Spline-Extrapolation Method in Traffic Forecasting in 5G Networks // Journal of Telecommunications and Information Technology. – 2019. – № 3. – P. 8–16.

5. Carvalho, P., Abdalla, H., Soares, A., Solis, P., Tarchetti, P. Analysis of the influence of self-similar traffic in the performance of real time applications [Электронный ресурс]. – URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.599.4041&rep=rep1&type=pdf (дата обращения: 21.06.2024).

6. Ruoyu, Ya., Wang, Yi. Hurst Parameter for Security Evaluation of LAN Traffic // Information Technology Journal. – 2012. – Vol. 11. – P. 269–275.

7. Ably, P., Flandrin, P., Taqqu, M., Veitch, D. Self-Similarity and long-range dependence through the wavelet lens // Theory and Applications of Long-Range Dependence / ed. by P. Doukhan, G. Oppenheim, M.S. Taqqu. – Boston : Birkhauser Press, 2002. – P. 345–379.

8. Минькович, Т.В. Информационные технологии: понятийно-терминологический аспект // ОТО. – 2012. – Т. 2. – С. 371–389.

9. Расторгуев, С.П. Информационные войны в сети Интернет / С.П. Расторгуев, М.В. Литвиненко ; под ред. А.Б. Михайловского. – М. : АНО «Центр стратегических оценок и прогнозов», 2014. – 128 с.

10. Макаренко, С.И. Терминологический базис в области информационного противоборства / С.И. Макаренко, И.И. Чукляев // Вопросы кибербезопасности. – 2014. – № 1 (2). – С. 13–21.

11. Михайлов, А.П. Модели информационной борьбы / А.П. Михайлов, Н.А. Маревцева // Математическое моделирование. – 2011. – Т. 23. – № 10. – С. 19–32.

12. ISO/IEC TR 27019:2013 Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry. – 2013.

13. Kendrick, D. Cluster randomised controlled trial evaluating an injury prevention program / D. Kendrick, L. Groom, J. Stewart // Injury Prevention. – 2016. – Vol. 13, № 2. – P. 93–98.

14. Fang, X. Managing Smart Grid Information in the Cloud: Opportunities, Model, and Applications / X. Fang, S. Misra, G. Xue, D. Yang // IEEE Network. – 2017. – July. – DOI: 10.1109/MNET.2012.6246750.

15. Prasad, I. Smart Grid Technology: Application and Control // International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering. – 2014. – Vol. 3, Issue 5.

16. Müller, K. Verordnete Sicherheit - das Schutzprofil für das Smart Metering Gateway - Eine Bewertung des neuen Schutzprofils // Datenschutz und Datensicherheit. – 2014. – Vol. 35, No. 8. – P. 547–551.

17. Protection Profile for the Security Module of a Smart Metering System. – Federal Office for Information Security, 2015. – V.1.0.

18. Anwar, A. Cyber Security of Smart Grid Infrastructure / A. Anwar, A. Mahmood // The State of the Art in Intrusion Prevention and Detection. – CRC Press, 2014. – DOI: 10.1201/b16390-9.

19. Bale, J. Facilitated Risk Analysis Process. Risk management in information technology using facilitated risk analysis process (FRAP) / J. Bale, E. Sediyono // Academic information systems of Satya Wacana Christian University. – 2015.

20. Tankard, C. Advanced persistent threats and how to monitor and deter them // Network Security. – 2011. – Vol. 2011, No. 8. – P. 16–19.

21. Parikh, T.P. Cyber security: Study on Attack, Threat, Vulnerability / T.P. Parikh, A.R. Patel // International Journal of Research in Modern Engineering and Emerging Technology. – 2017. – Vol. 5, Issue: 6.

22. Sterbenz, J.P. Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines / J.P. Sterbenz [et al.] // Computer Networks. – 2010. – Vol. 54, No. 8. – P. 1245–1265.

23. El Fray, I. A comparative study of risk assessment methods, MEHARI & CRAMM with a new formal model of risk assessment (FoMRA) in information systems // Proceedings of the 11th IFIP TC 8 international conference on Computer Information Systems and Industrial Management. – 2012.

24. Syalim, A. Comparison of Risk Analysis Methods: MEHARI, MAGERIT, NIST800-30 and Microsoft’s Security Management Guide [Электронный ресурс] / A. Syalim. – URL: http://itslab.inf.kyushu-u.ac.jp (дата обращения: 21.06.2024).

25. Mehari – Overview. – Club de la Securit´e de l'Information Francais (CLUSIF), 2010.

26. Microsoft security center of excellence [Электронный ресурс]. – URL: http://www.microsoft.com/rus/technet/security (дата обращения: 21.06.2024).

27. Cyber Security Trends You Can't Ignore in 2021 [Электронный ресурс]. – URL: https://purplesec.us/cyber-security-trends-2021/ (дата обращения: 24.04.2021).

28. Cybersecurity Statistics and Trends for 2021 [Электронный ресурс]. – URL: https://www.varonis.com/blog/cybersecurity-statistics/ (дата обращения: 24.04.2021).

29. Clincy, V. Web Application Firewall: Network Security Models and Configuration / V. Clincy, H. Shahriar // Proceedings of the 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC). – 2018. – P. 835–836.

30. Ad-IoT: Anomaly detection of IoT cyberattacks in smart city using machine learning / A. Alrashdi [et al.] // 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC). – 2019. – P. 0305–0310.

31. Industrial internet of things: Recent advances, enabling technologies and open challenges / W.Z. Khan [et al.] // Computers and Electrical Engineering. – 2020. – Vol. 81. – Art. 106522.

32. Interoperability in internet of things: Taxonomies and open challenges / M. Noura, M. Atiquzzaman, M. Gaedke // Mobile networks and applications. – 2019. – Vol. 24(3). – P. 796–809.

33. Internet of things: A general overview between architectures, protocols and applications / M. Lombardi, F. Pascale, D. Santaniello // Information. – 2021. – Vol. 12(2). – Art. 87.

34. Resul, D.A.S. Analysis of cyberattacks in IoT-based critical infrastructures / D.A.S. Resul, M.Z. Gündüz // International Journal of Information Security Science. – 2020. – Vol. 8(4). – P. 122–133.

35. Браницкий, А.А. Анализ и классификация методов обнаружения сетевых атак / А.А. Браницкий, И.В. Котенко // Труды СПИИРАН. – 2016. – Вып. 2(45). – С. 207–244.

36. Chandola, V. Anomaly Detection for Discrete Sequences: A Survey / V. Chandola, A. Banerjee, V. Kumar // IEEE transactions on knowledge and data engineering. – 2012. – Vol. 24, no. 5.

37. Hruschka, E.R. A survey of evolutionary algorithms for clustering / E.R. Hruschka, R.J. Campello, A.A. Freitas, A.C. Carvalho // IEEE Transactions on Systems, Man and Cybernetics, Part C: Applications and Reviews. – 1999. – Vol. 29. – P. 433–439.

38. Vapnik, V.N. The Nature of Statistical Learning Theory. – New York, USA : Springer Verlag, 1995.

39. Шелухин, О.И. Классификация IP-трафика методами машинного обучения / О.И. Шелухин, С.Д. Ерохин, А.В. Ванюшина ; под ред. О.И. Шелухина. – Москва : Горячая линия-Телеком, 2018. – 284 с.

40. Self-similar network traffic and performance evaluation / ed. by K. Park, W. Willinger. – 2000.

41. Шелухин, О.И. Самоподобие и фракталы / О.И. Шелухин, А.В. Осин, С.М. Смольский // Телекоммуникационные приложения. – М. : Физматлит, 2008. – С. 362.

42. Sheluhin, O.I. Self-similar processes in telecommunications / O.I. Sheluhin, S.M. Smolskiy, A.V. Osin. – John Wiley & Sons, 2007. – 320 p.

43. Шелухин, О.И. Сетевые аномалии. Обнаружение, локализация, прогнозирование. – М. : Горячая линия –Телеком, 2019. – 448 с.

44. Sheluhin, O. Influence of Fractal Dimension Statistical Charachteristics on Quality of Network Attacks Binary Classification / O. Sheluhin, M. Kazhemskiy // Conference of Open Innovations Association, FRUCT. – 2021. – No. 28. – P. 407-413. – EDN XMLZKW.

45. Sheluhin, O.I. Detection of Network Anomalies with the Method of Fixing Jumps of the Fractal Dimension in the Online Mode / O.I. Sheluhin, S.Y. Rybakov, A.V. Vanyushina // Wave Electronics and Its Application in Information and Telecommunication Systems. – 2022. – Vol. 5, No. 1. – P. 430-435. – EDN UEYFUM.

46. Шелухин, О.И. Влияние фрактальной размерности на качество классификации компьютерных атак методами машинного обучения / О.И. Шелухин, С.Ю. Рыбаков, А.В. Ванюшина // Наукоемкие технологии в космических исследованиях Земли. – 2023. – Т. 15, № 1. – С. 57-64. – DOI 10.36724/2409-5419-2023-15-1-57-64. – EDN EVELAW.

47. Котенко, И.В. Метод раннего обнаружения кибератак на основе интеграции фрактального анализа и статистических методов / И.В. Котенко, И.Б. Саенко, О.С. Лаута, А.М. Крибель // Первая миля. – 2021. – № 6 (98). – С. 64-71.

48. Перов, Р.А. Комплексная методика обнаружения кибератак на основе интеграции фрактального анализа и статистических методов / Р.А. Перов, О.С. Лаута, А.М. Крибель, Ю.М. Федулов // Наукоемкие технологии в космических исследованиях Земли. – 2022. – Т. 14. № 2. – С. 44-51.

49. Kotenko, I. Anomaly and cyber attack detection technique based on the integration of fractal analysis and machine learning methods / I. Kotenko, I. Saenko, O. Lauta, A. Kribel // Informatika i avtomatizaciâ. – 2022. – Vol. 21(6). – P. 1328–1358.

50. Карачанская, Е.В. Метод выявления аномалий сетевого трафика, основанный на его самоподобной структуре / Е.В. Карачанская, Н.И. Соседова // Безопасность информационных технологий. – 2019. – Том 26, № 1. – С. 98-110.

51. Vieira, F.H.T. A Network Traffic Prediction Approach Based on Multifractal Modeling / F.H.T. Vieira, G.R. Bianchi, L.L. Lee // J. High Speed Netw. – 2010. – Vol 17(2). – P. 83–96.

52. Зегжда, П.Д. Мультифрактальный анализ трафика магистральных сетей интернет для обнаружения атак отказа в обслуживании / П.Д. Зегжда, Д.С. Лаврова, А.А. Штыркина // Проблемы информационной безопасности. Компьютерные системы. – 2018. – № 2. – С. 48–58.

53. Лаврова, Д.С. Оценка киберустойчивости информационно-технологических систем на основе самоподобия / Д.С. Лаврова, Д.П. Зегжда, П.Д. Зегжда, А.А. Штыркина // Методы и технические средства обеспечения безопасности информации : материалы 25-й научно-технической конференции. – Спб. : Изд-во Политехн. Ун-та, 2016. – С. 101–104.

54. Штыркина, А.А. Обнаружение аномалий в трафике магистральных сетей Интернет с использованием мультифрактального анализа / А.А. Штыркина, П.Д. Зегжда, Д.С. Лаврова // Методы и технические средства обеспечения безопасности информации. – 2018. – № 27. – С. 14–15.

55. Шелухин, О.И. Обнаружение аномальных выбросов в реальном масштабе времени методами мультифрактального анализа / О.И. Шелухин, А.В. Панкрушин // Нелинейный мир. – 2016. – Т. 14, № 2. – С. 72-82. – EDN VTZNTH.

56. Sheluhin, O.I. Network Traffic Anomalies Detection Using a Fixing Method of Multifractal Dimension Jumps in a Real-Time Mode / O.I. Sheluhin, I.Y. Lukin // Automatic Control and Computer Sciences. – 2018. – Vol. 52, No. 5. – P. 421-430. – DOI 10.3103/S0146411618050115. – EDN OJQHKD.

57. Треногин, Н.Г. Фрактальные свойства сетевого трафика в клиентсерверной информационной системе / Н.Г. Треногин, Д.Е. Соколов // Вестник НИИ Сибир. гос. ун-та телекоммуникаций и информатики. – Новосибирск: Изд-во СибГУТИ, 2003. – С. 163–172.

58. Петров, В.В. Исследование самоподобной структуры телетрафика беспроводной сети / В.В. Петров, В.В. Платов // Радиотехнические тетради. – 2004. – № 30. – С. 58–62.

59. Лаврова, Д.С. Подход к разработке SIEM-системы для Интернета вещей // Проблемы информационной безопасности. Компьютерные системы. – 2016. – № 2. – С. 50–60.

60. Lavrova, D.S. An approach to developing the SIEM system for the Internet of Things // Automatic Control and Computer Sciences. – 2016. – № 8. – P. 673–681.

61. Масловская, А.Г. Вейвлет-мультифрактальный анализ индуцированного электронным зондом тока переполяризации сегнетоэлектрических кристаллов / А.Г. Масловская, Т.К. Барабаш // Вестник Саратовского государственного технического университета. – 2011. – Т. 4, № 4 (62).

62. Басараб, М.А. Оценка влияния трешолдинга на достоверность обнаружения аномальных вторжений в компьютерные сети статистическим методом / М.А. Басараб, О.И. Шелухин, И.А. Коновалов // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение. – 2018. – № 5. – С. 56-67. – DOI 10.18698/0236-3933-2018-5-56-67.

63. Шелухин, О.И. Мультифрактальные свойства трафика реального времени / О.И. Шелухин, А.В. Осин // Электротехнические и информационные комплексы и системы. – 2006. – Т. 2, № 3.

64. Шелухин, О.И. Фрактальные процессы в телекоммуникациях / О.И. Шелухин, А.М. Тенякшев, А.В. Осин. – М. : Радиотехника, 2003.

65. Theory and applications of long-range dependence / ed. by P. Doukhan, G. Oppenheim, M. Taqqu. – Springer Science & Business Media, 2002.

66. Филимонов, А.В. Мультифрактальные модели временных рядов : препринт Р1/2010/06. – Нижний Новгород : НФ ГУ-ВШЭ, 2010. – 45 с.

67. Шелухин, О.И. Мультифракталы. Инфокоммуникационные приложения : учебное пособие. – Москва : Горячая линия-Телеком, 2014. – 579 с. – ISBN 978-5-9912-0142-1.

68. Bhuyan, M.H. Network anomaly detection: Methods, systems and tools / M.H. Bhuyan, D.K. Bhattacharyya, J.K. Kalita // IEEE Commun. Surv. Tutorials. – 2013. – vol. 60, no. 1. – P. 303–336.

69. Chandola, V. Anomaly detection for discrete sequences: A survey / V. Chandola, A. Banerjee, V. Kumar // IEEE Trans. Knowl. Data Eng. – 2012. – vol. 24, no. 5.

70. Мандрикова, О.В. Критерии выбора вейвлет-функции в задачи аппроксимации природных временных рядов сложной структуры / О.В. Мандрикова, Ю.А. Полозов // Информационные технологии. – 2012. – № 1. – С. 31-36. – EDN OOGVDV.

71. Шелухин, О.И. Скрытие информации в аудиосигналах с использованием детерминированного хаоса / О.И. Шелухин, С.Ю. Рыбаков, Д.И. Магомедова // Наукоемкие технологии в космических исследованиях Земли. – 2021. – №1.

72. Sheluhin, O.I. Wavelet type selection in the problem of anomaly intrusions detection in computer networks using multifractal analysis methods / O.I. Sheluhin, J.W. Sirukhi, A.V. Pankrushin // T-Comm: Телекоммуникации и транспорт. – 2015. – Т. 9. No 4. – С. 88-92.

73. Mallat, S. A wavelet tour of signal processing 3 ed.: The Sparse Way. – 2005.

74. Abry, P. Wavelet analysis of long-range dependent traffic / P. Abry, D. Veitch // IEEE Trans. on Info. Theory. – 1998. – vol. 44, no. 1. – P. 2-15.

75. Шелухин, О.И. Модификация алгоритма обнаружения сетевых атак методом фиксации скачков фрактальной размерности в режиме online / О.И.

Шелухин, С.Ю. Рыбаков, А.В. Ванюшина // Труды учебных заведений связи. – 2022. – Т. 8, № 3. – С. 117-126. – DOI 10.31854/1813-324X-2022-8-3-117-126. – EDN OULDYS.

76. Sheluhin, O.I. Detection of Network Anomalies with the Method of Fixing Jumps of the Fractal Dimension in the Online Mode / O.I. Sheluhin, S.Y. Rybakov, A.V. Vanyushina // Wave Electronics and Its Application in Information and Telecommunication Systems. – 2022. – Vol. 5, No. 1. – P. 430-435. – EDN UEYFUM.

77. Delignières, D. Correlation Properties of (Discrete) Fractional Gaussian Noise and Fractional Brownian Motion // Mathematical Problems in Engineering. – 2015. – Art. 485623. – DOI:10.1155/2015/485623.

78. Li, M. Generalized fractional Gaussian noise and its application to traffic modeling // Physica A: Statistical Mechanics and Its Applications. – 2021. – Vol. 579. – Art. 126138. – DOI:10.1016/j.physa.2021.126138.

79. Li, M. Revisiting fractional Gaussian noise / M. Li, X. Sun, X. Xiao // Physica A: Statistical Mechanics and Its Applications. – 2019. – Vol. 514. – P. 56–62. – DOI:10.1016/j.physa.2018.09.008.

80. Brouste, A. One-step estimation for the fractional Gaussian noise at high-frequency / A. Brouste, M. Soltane, I. Votsi // ESAIM: Probability and Statistics. – 2020. – Vol. 24. – P. 827–841. – DOI:10.1051/ps/2020022.

81. Sørbye, S.H. Fractional Gaussian noise: Prior specification and model comparison / S.H. Sørbye, H. Rue // Environmetrics. – 2017. – Vol. 29(5-6). – Art. e2457. – DOI:10.1002/env.2457.

82. Sheluhin, O.I. Detection of anomalous intrusions into computer networks by statistical methods / O.I. Sheluhin, A.S. Filinova, A.V. Vasina // T-Comm. – 2015. – V. 9. № 10. – P. 42-49.

83. Basarab, M.A. Evaluation of the influence of thresholding on the reliability of detection of anomalous intrusions into computer networks by a statistical method / M.A. Basarab, O.I. Sheluhin, I.A. Konovalov // Vestnik of Moscow State Technical University named after N.E. Bauman. Series Instrument Engineering. – 2018. – № 5. – P. 56-67. – DOI 10.18698/0236-3933-2018-5-56-67.

84. Kaur, G. Study of self-similarity for detection of rate-based network anomalies / G. Kaur, V. Saxena, J. Prakash // Int. J. Secur. Its Appl. – 2017. – vol. 11, no. 8. – P. 27–44.

85. Riedi, R.H. A Multifractal Wavelet Model with Application to Network Traffic / R.H. Riedi, M.S. Crouse, V.J. Ribeiro, R.G. Baraniuk. – Apr. 1999.

86. Sheluhin, O.I. Intrusion detection in computer networks. Network anomaly / O.I. Sheluhin, D.Zh. Sakalema, A.S. Filinova. – Moscow : Hotline - Telecom, 2013. – 220 p.

87. Infinitely divisible cascade analysis of network traffic data / D. Veitch [et al.] // Proceedings of the International Conference on Acoustics, Speech, and Signal Processing (Istanbul, Turkey). – June 2000.

88. Abry, P. Wavelet analysis of long-range dependent traffic / P. Abry, U. Veitch // IEEE Trans, on Info, Theory. – 1998. – Vol, 44. No. I. – P. 2-15.

89. Wavelets for the analysis, estimation, and synthesis of scaling data / P. Abry [et al.] // Self-similar Network Traffic and Performance Evaluation / ed. by K. Park, W. Willinger. – John Wiley & Sons, 2000. – P. 39-88.

90. Sheluhin, O.I. Analysis of changes in the fractal properties of telecommunication traffic caused by abnormal invasions / O.I. Sheluhin, A.A. Antonion // T-Comm. – 2014. – No. 6. – P. 61-64.

91. Sheluhin, O.I. Integrated Model for information Communication Systems and Networks. Design and Development / O.I. Sheluhin, A.A. Atayero. – USA : IGI Global, 2012. – 462 p.

92. Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection / Y. Mirsky [et al.]. – 2018. – DOI: 10.14722/ndss.2018.23211.

93. Malicious Packet Classification Based on Neural Network Using Kitsune Features / K. Miyamoto [et al.]. – 2022. – DOI: 10.1007/978-3-031-08277-1_25.

94. Alabdulatif, A. Machine Learning Approach for Improvement in Kitsune NID / A. Alabdulatif, S. Rizvi // Intelligent Automation & Soft Computing. – 2022. – Vol. 32. – P. 827-840. – DOI: 10.32604/iasc.2022.021879.

95. Aksoy, A. Automated Network Incident Identification through Genetic Algorithm-Driven Feature Selection / A. Aksoy, L. Valle, G. Kar // Electronics. – 2024. – Vol. 13, № 293. – P. 1–25. – DOI: 10.3390/electronics13020293.

96. Atayero, A.A. Integrated Model for Information Communication Systems and Networks. Design and Development / A.A. Atayero, O.I. Sheluhin. – USA : IGI Global, 2013. – 462 p.

97. Self&similar Network Traffic and Performance Evaluation / ed. by K. Park, W. Willinger. – John Wiley & Sons, 2000.

98. Bhuyan, M.H. Network Anomaly Detection: Methods, Systems and Tools / M.H. Bhuyan, D.K. Bhattacharyya, J.K. Kalita // IEEE Communications surveys & tutorials. – 2013. – Vol. 60(1). – P. 303-336.

99. Шелухин, О.И. Статистические характеристики фрактальной размерности трафика IoT на примере набора данных Kitsune / О.И. Шелухин, С.Ю. Рыбаков // Труды учебных заведений связи. – 2023. – Т. 9, № 5. – С. 112-119. – DOI 10.31854/1813-324X-2023-9-5-112-119. – EDN YMSJRF.

100. KDD Cup 1999 Data [Электронный ресурс]. – URL: https://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html (дата обращения: 21.06.2024).

101. NSL&KDD Dataset [Электронный ресурс]. – URL: https://www.unb.ca/cic/datasets/nsl.html (дата обращения: 21.06.2024).

102. Australian Center for Cyber Security (ACCS) [Электронный ресурс]. – 2014. – URL: http://www.accs.unsw.adfa.edu.au/ (дата обращения: 21.06.2024).

103. Moustafa, N. UNSW&NB15: a comprehensive data set for network intrusion detection systems (UNSW&NB15 network data set) / N. Moustafa, J. Slay // Military Communications and Information Systems Conference (MilCIS). – 2015. – DOI: 10.1109/MilCIS.2015.7348942.

104. Рыбаков, С.Ю. Обнаружение сетевых атак в сетях интернета вещей методом фиксации скачков фрактальной размерности / С.Ю. Рыбаков, В.В. Спирин // Решение. – 2023. – Т. 1. – С. 165-167. – EDN WMQFAG.

105. Шелухин, О.И. Оценка характеристик мультифрактального спектра фрактальной размерности сетевого трафика и компьютерных атак в IoT / О.И. Шелухин, С.Ю. Рыбаков, А.В. Ванюшина // Труды учебных заведений связи. – 2024. – Т. 10, № 3. – С. 104–115. – DOI:10.31854/1813-324X-2024-10-3-104-115. – EDN:KIRCNK.

106. Рыбаков, С.Ю. Оценка мультифрактального спектра сетевого трафика для обнаружения компьютерных атак // Фундаментальные и прикладные аспекты компьютерных технологий и информационной безопасности : сборник статей X Всероссийской научно-технической конференции. – Таганрог, 2024. – С. 23-26.

107. Рыбаков, С.Ю. Анализ алгоритмов машинного обучения для обеспечения безопасности Интернета вещей / С.Ю. Рыбаков, Ф.А. Ташлыков // Технологии информационного общества : сборник трудов XVIII Международной отраслевой научно-технической конференции, Москва, 27–28 февраля 2024 года. – Москва : Московский технический университет связи и информатики, 2024. – С. 128-131. – EDN LRTDDR.

108. Шелухин, О.И. Классификация компьютерных атак с использованием мультифрактального спектра фрактальной размерности / О.И. Шелухин, С.Ю. Рыбаков, Д.И. Раковский // Вопросы кибербезопасности. – 2024. – № 2(60). – С. 107-119. – DOI 10.21681/2311-3456-2024-2-107-119. – EDN GKOSBB.

109. Шелухин, О.И. Классификация компьютерных атак с использованием мультифрактального спектра фрактальной размерности / О.И. Шелухин, С.Ю. Рыбаков // Методы и технические средства обеспечения безопасности информации : материалы 33-й всероссийской научно-технической конференции, 24-27 июня 2024 года. – СПб : Изд-во Политехнического университета, 2024. – С. 38-40.

110. Рыбаков, С. Ю. Методы защиты интернета вещей от атак нулевого дня / С. Ю. Рыбаков // Инженерный вестник Дона. – 2025. – № 3. – С. 1–15.

111. Рыбаков, С. Ю. Выбор типа материнского вейвлета при фрактальном анализе в задаче обнаружения компьютерных атак / С. Ю. Рыбаков // Инженерный вестник Дона. – 2024. – № 10(118). – С. 94–104.

112. Шелухин, О.И. Обнаружение кибератак и вредоносного программного обеспечения нулевого дня методами машинного обучения / О. И. Шелухин, С. Ю. Рыбаков, С. С. Звежинский // Радиотехника. 2025. Т. 89. № 8. С. 184–198.

113. Рыбаков, С. Ю. Анализ подходов к обнаружению атак нулевого дня в сетях интернета вещей / С. Ю. Рыбаков, Ф. А. Ташлыков // Инженерный вестник Дона. – 2025. – № 7. – С. 1–17.

114. Sheluhin, O.I. Characteristics Assessment of Multifractal Spectrum of Fractal Dimension IoT-Traffic / O.I. Sheluhin, S.Y. Rybakov // Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO). – 2024. – P. 1–6.

115. Akopov, A. Traffic Improvement in Manhattan Road Networks with the Use of Parallel Hybrid Biobjective Genetic Algorithm / A. Akopov, L. Beklaryan // IEEE Access. – 2024. – Vol. 12. – P. 19532-19552. – DOI: 10.1109/ACCESS.2024.3361399.

116. Spatial linear transformer and temporal convolution network for traffic flow prediction / Z. Xing [et al.] // Scientific Reports. – 2024. – Vol. 14. – P. 1–14. – DOI: 10.1038/s41598-024-54114-9.

117. Sankaranarayanan, M. Traffic Density Estimation for Traffic Management Applications Using Neural Networks / M. Sankaranarayanan, C. Mala, S. Jain // International Journal of Intelligent Information Technologies. – 2024. – Vol. 20. – P. 1–19. – DOI: 10.4018/IJIIT.335494.

118. Short-term electric power load forecasting using random forest and gated recurrent unit / V. Veeramsetty [et al.] // Electrical Engineering. – 2022. – Vol. 104. – P. 307–329. – DOI: 10.1007/s00202-021-01376-5.

119. Израилов, К. Е. Исследование возможностей машинного обучения для автоматического ранжирования уязвимостей по их текстовому описанию / К.Е. Израилов, А.Ю. Ярошенко // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023) : Сборник научных статей. XII Международная научно-техническая и научно-методическая конференция. В 4 т., Санкт-Петербург, 28 февраля – 01 2023 года. Том 1. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2023. – С. 586-590. – EDN ARDWQO.

120. Rao, R.S. Application of word embedding and machine learning in detecting phishing websites / R.S. Rao, A. Umarekar, A.R. Pais // Telecommunication Systems. – 2022. – Vol. 79, № 1. – P. 33–45. – DOI: 10.1007/s11235-021-00850-6.

121. Пахомов, М. А. Раннее обнаружение сетевых атак в беспроводных самоорганизующихся сетях методами машинного обучения / М. А. Пахомов, Е. Ю.

Павленко // Методы и технические средства обеспечения безопасности информации. – 2025. – № 34. – С. 92-93. – EDN PDBGMB.

122. Kotenko, I. Static Analysis of Information Systems for IoT Cyber Security: A Survey of Machine Learning Approaches / I. Kotenko, K. Izrailov, M. Buinevich // Sensors. – 2022. – Vol. 22, No. 4. – DOI 10.3390/s22041335. – EDN XEOLHD.

123. Сергадеева, А. И. Распознавание DDOS-атак с использованием модульной нейронной сети / А. И. Сергадеева, Д. С. Лаврова, Е. Ю. Павленко // Методы и технические средства обеспечения безопасности информации. – 2023. – № 32. – С. 87-89. – EDN GSFMRP.

124. Vijayakumar, D.S. Multistage Ensembled Classifier for Wireless Intrusion Detection System / D.S. Vijayakumar, S. Ganapathy // Wireless Personal Communications. – 2022. – Vol. 122, № 1. – P. 645–668. – DOI: 10.1007/s11277-021-08917-y.

125. Behdani, Z. An Alternative Approach to Rank Efficient DMUs in DEA via Cross-Efficiency Evaluation, Gini Coefficient, and Bonferroni Mean / Z. Behdani, M. Darehmiraki // Journal of the Operations Research Society of China. – 2022. – Vol. 10, № 4. – P. 763–783. – DOI: 10.1007/s40305- 019-00264-x.

Приложение А Сравнительный анализ R/S алгоритма и разработанного алгоритма оценки скачка ФР на примере реальной базы данных КА в сетях интернета вещей

Перед тем как проводить оценку статистических параметров фрактальной размерности сетевого трафика для разных типов атак, необходимо определиться с размером окна оценки фрактальной размерности или же показателя Херста для каждого типа атак, т.к. одни атаки имеют более высокую продолжительность такие как SSDP Flood (54 сек) и Mirai (44 мин), атака типа OS scan напротив имеет более низкую длительность (29 сек) – это проиллюстрировано на рисунке 1, было решено использовать захваченный трафик с интервалом захвата пакетов в 100 мс.

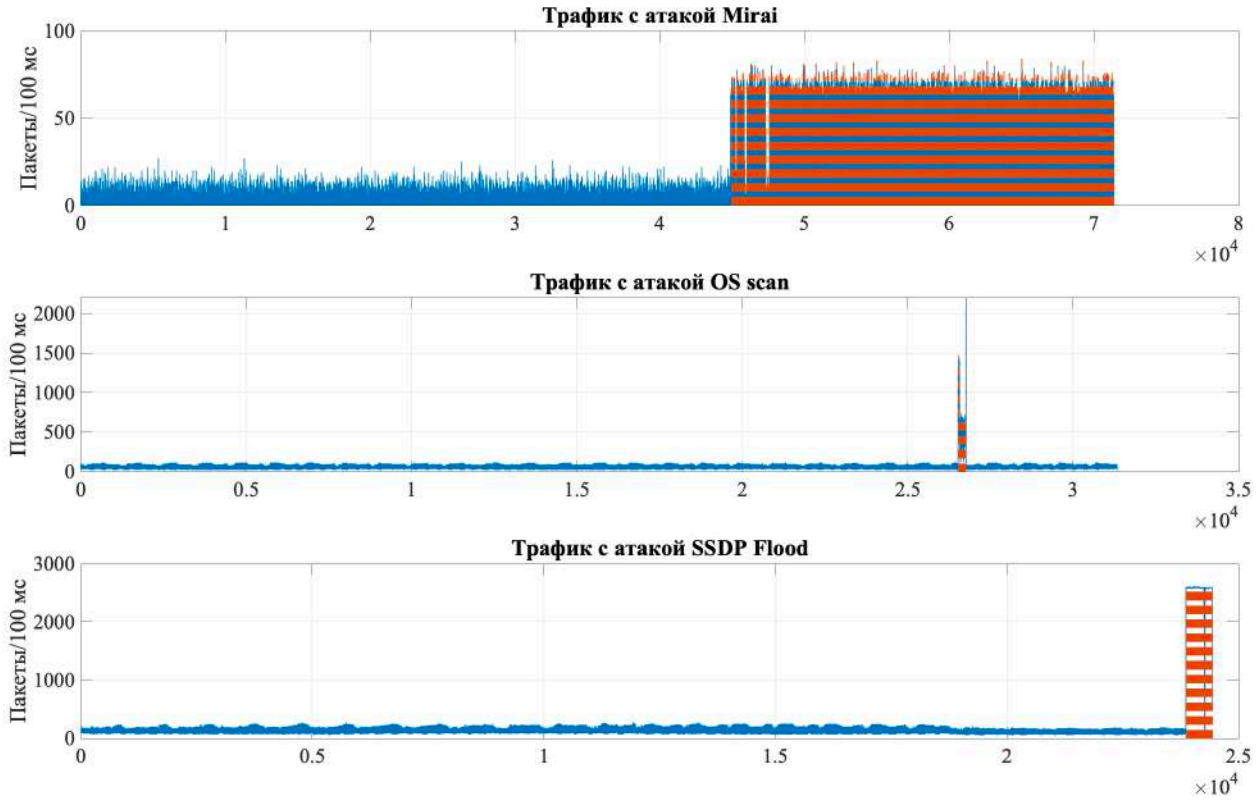


Рисунок 1 - Трафик с помеченными атаками: нормальный трафик (голубой), а трафик атаки(оранжевый)

Далее рассмотрим нормальный трафик по отдельности для каждой из атак и проведем его оценку с помощью алгоритмов RS анализа и скачка фрактальной размерности. Если рассмотреть более детально трафик каждой из атак, то можно заметить, что поведение нормального трафика везде разное, это связано с тем, что трафик снимался на разных участках сети и содержит захваченный трафик для разных типов устройств.

Таблица 1 - Оценка статистических параметров нормального трафика из дампа Mirai

Размер окна анализа	**500**	**1000**	**1500**	**2000**	**2500**	**3000**	**3500**	**4000**	**4500**
Среднее значение показателя H с применением RS анализа	0.7258	0.6048	0.5631	0.5193	0.4933	0.4723	0.4488	0.4623	0.4374
Среднее значение показателя H с применением алгоритма скачка фрактальной размерности	0.5651	0.5828	0.5876	0.5912	0.6000	0.5906	0.5923	0.5918	0.5949
Среднее значение показателя H с трешолдингом	0.5637	0.5815	0.5863	0.5898	0.5986	0.5892	0.5909	0.5904	0.5935
Дисперсия показателя H с применением RS анализа	0.0036	0.0010	0.0005	0.0003	0.0003	0.0003	0.0002	0.0002	0.0002
Дисперсия H с применением алгоритма скачка фрактальной размерности	0.0044	0.0013	0.0007	0.0005	0.0006	0.0003	0.0003	0.0002	0.0002
Дисперсия H с трешолдингом	0.0020	0.0013	0.0011	0.0010	0.0010	0.0009	0.0009	0.0009	0.0009
Асимметрия показателя H с применением RS анализа	-0.010	-0.085	0.1231	0.1118	0.2763	0.1931	0.1247	0.1228	0.3797

Продолжение таблицы 1

Размер окна анализа	**500**	**1000**	**1500**	**2000**	**2500**	**3000**	**3500**	**4000**	**4500**
Асимметрия H с применением алгоритма скачка фрактальной размерности	-1.430	-0.736	-0.472	-0.160	0.754	-0.051	0.028	0.049	0.410
Асимметрия H с трешолдингом	-4.486	-9.346	-11.80	-13.98	-15.46	-15.57	-16.12	-16.56	-17.15
Эксцесс показателя H с применением RS анализа	2.892	3.014	2.977	3.090	3.153	2.778	2.926	3.105	4.278
Эксцесс H с применением алгоритма скачка фрактальной размерности	7.020	4.502	4.201	3.505	5.095	3.274	3.192	3.259	3.867
Эксцесс H с трешолдингом	55.6	150.8	204.7	255.4	290.5	291.9	304.2	313.9	327.4
Нормальный трафик из дампа Mirai									

При детальном рассмотрении полученных статистических показателей, можно отметить, что при длине окна 1000 для RS анализа и 2500 для алгоритма скачка фрактальной размерности показатель среднего значения показателя Херста равны. При увеличении окна анализа среднее значение показателя фрактальной размерности по алгоритму RS уменьшается, тогда как алгоритм основанный на вейвлетах сильно не изменяется при увеличении длительности окна. Проиллюстрируем гистограмму распределения оценки показателя Херста на рисунке 2.

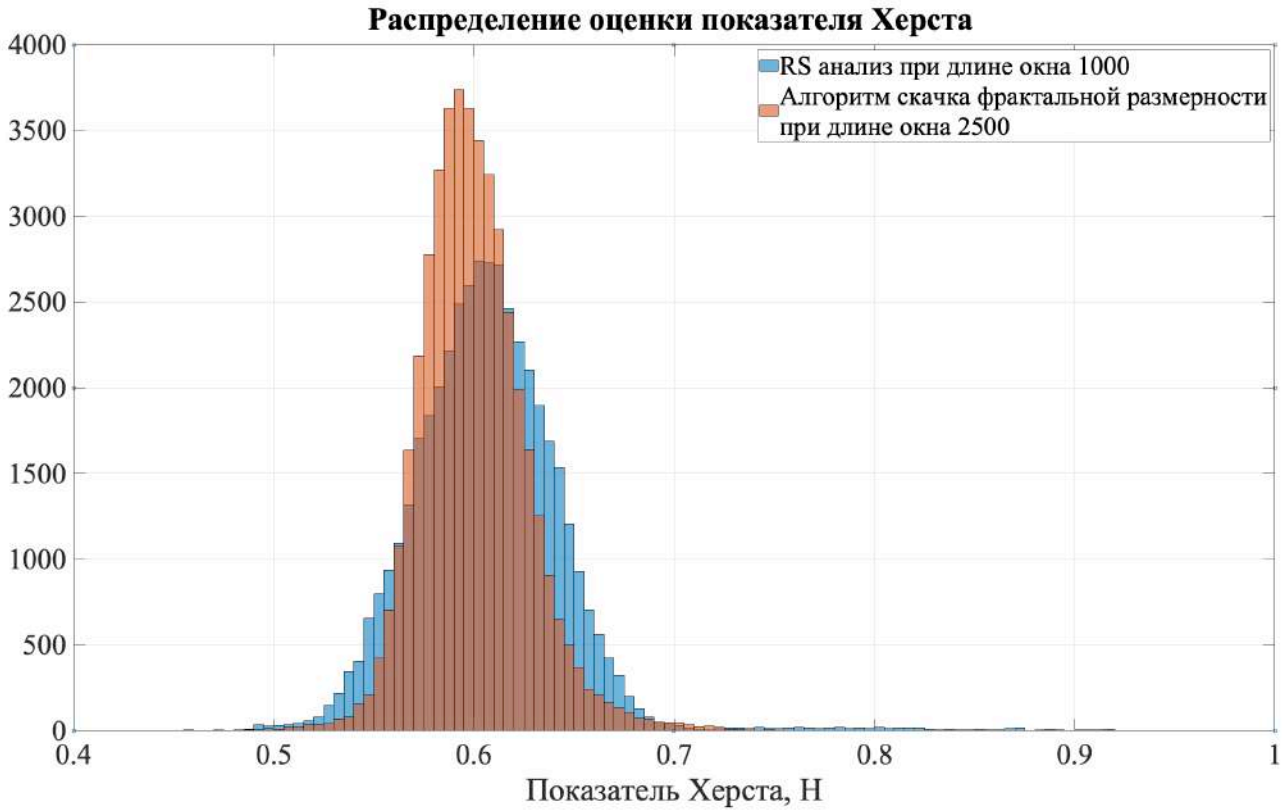


Рисунок 2 - Распределение оценки показателя Херста при использовании алгоритма RS анализа и алгоритма скачка фрактальной размерности

Далее проведем такой же эксперимент с остальным трафиком. В таблице 2 приведены статистические параметры оценки показателя Херста для нормального трафика из дампа OS scan.

Таблица 2 - Оценка статистических параметров нормального трафика из дампа OS scan

Размер окна анализа	**500**	**1000**	**1500**	**2000**	**2500**	**3000**	**3500**	**4000**	**4500**
Среднее значение показателя H с применением RS анализа	0.117	0.095	0.108	0.103	0.095	0.114	0.109	0.109	0.124
Среднее значение показателя H с применением алгоритма скачка фрактальной размерности	0.126	0.086	0.082	0.074	0.203	0.069	0.099	0.0705	0.118

Продолжение таблицы 2

Размер окна анализа	**500**	**1000**	**1500**	**2000**	**2500**	**3000**	**3500**	**4000**	**4500**
Среднее значение показателя H с трешолдингом	0.126	0.085	0.082	0.074	0.202	0.069	0.098	0.070	0.117
Дисперсия показателя H с применением RS анализа	0.0009	0.0006	0.0004	0.0003	0.0003	0.0003	0.0003	0.0002	0.0002
Дисперсия H с применением алгоритма скачка фрактальной размерности	0.0105	0.0044	0.0027	0.0017	0.0141	0.0009	0.0021	0.0006	0.0031
Дисперсия H с трешолдингом	0.0013	0.0002	0.0002	0.0002	0.0009	0.0001	0.0003	0.0001	0.0003
Асимметрия показателя H с применением RS анализа	0.543	0.232	0.243	0.117	-0.230	-0.286	-0.530	-0.808	-0.803
Асимметрия H с применением алгоритма скачка фрактальной размерности	-0.22	-0.07	0.04	0.16	0.04	0.12	0.15	0.12	0.23
Асимметрия H с трешолдингом	-0.07	-0.54	-0.57	-0.49	-1.53	-0.43	-0.79	-1.31	-1.26
Эксцесс показателя H с применением RS анализа	3.52	3.19	3.43	3.15	3.27	3.06	3.08	3.33	3.49
Эксцесс H с применением алгоритма скачка фрактальной размерности	3.35	3.03	2.64	2.98	1.72	3.15	2.20	3.06	2.06
Эксцесс H с трешолдингом	3.12	5.14	5.99	5.12	12.25	7.84	6.30	11.99	9.29
Нормальный трафик из дампа OS scan									

Оценка показала, что данный трафик не обладает фрактальными свойствами так как среднее значение показателя Херста для двух алгоритмов находится в окрестности 0.1. Данное явление можно объяснить спецификой трафика устройств

IoT. Стоит также отметить, что оба алгоритма дают одинаковые результаты независимо от размера окна анализа.

Далее рассмотрим нормальный трафик из дампа SSDP Flood. В таблице 3 представлены результаты оценки.

Таблица 3 - Оценка статистических параметров нормального трафика из дампа SSDP Flood

Размер окна анализа	**500**	**1000**	**1500**	**2000**	**2500**	**3000**	**3500**	**4000**	**4500**
Среднее значение показателя H с применением RS анализа	0.429	0.469	0.510	0.527	0.534	0.564	0.577	0.576	0.597
Среднее значение показателя H с применением алгоритма скачка фрактальной размерности	0.3172	0.3307	0.3367	0.3460	0.3956	0.3530	0.3612	0.3589	0.3702
Среднее значение показателя H с трешолдингом	0.312	0.326	0.333	0.342	0.391	0.349	0.357	0.355	0.366
Дисперсия показателя H с применением RS анализа	0.0215	0.0180	0.0130	0.0115	0.0103	0.0089	0.0086	0.0067	0.0215
Дисперсия H с применением алгоритма скачка фрактальной размерности	0.0153	0.0086	0.0068	0.0056	0.0055	0.0040	0.0032	0.0027	0.0021
Дисперсия H с трешолдингом	0.0102	0.0081	0.0071	0.0062	0.0044	0.0051	0.0043	0.0039	0.0034
Асимметрия показателя H с применением RS анализа	0.804	0.658	0.479	0.388	0.478	0.610	0.754	0.584	0.701
Асимметрия H с применением алгоритма скачка фрактальной размерности	-0.179	0.220	0.193	0.084	-0.291	-0.131	-0.189	-0.208	-0.254

Продолжение таблицы 3

Размер окна анализа	**500**	**1000**	**1500**	**2000**	**2500**	**3000**	**3500**	**4000**	**4500**
Асимметрия H с трешолдингом	0.374	0.024	-0.289	-0.689	-2.199	-1.346	-1.915	-2.218	-3.075
Эксцесс показателя H с применением RS анализа	3.777	3.250	3.112	3.301	3.451	3.106	2.910	2.552	2.633
Эксцесс H с применением алгоритма скачка фрактальной размерности	3.456	3.133	2.811	2.656	2.600	2.385	2.402	2.427	2.493
Эксцесс H с трешолдингом	3.719	4.277	4.650	5.569	14.508	7.989	11.713	13.648	19.986
Нормальный трафик из дампа SSDP Flood									

Построим распределение оценки Херста для RS анализа при длине окна 500 и для скачка фрактальной размерности при 2500.

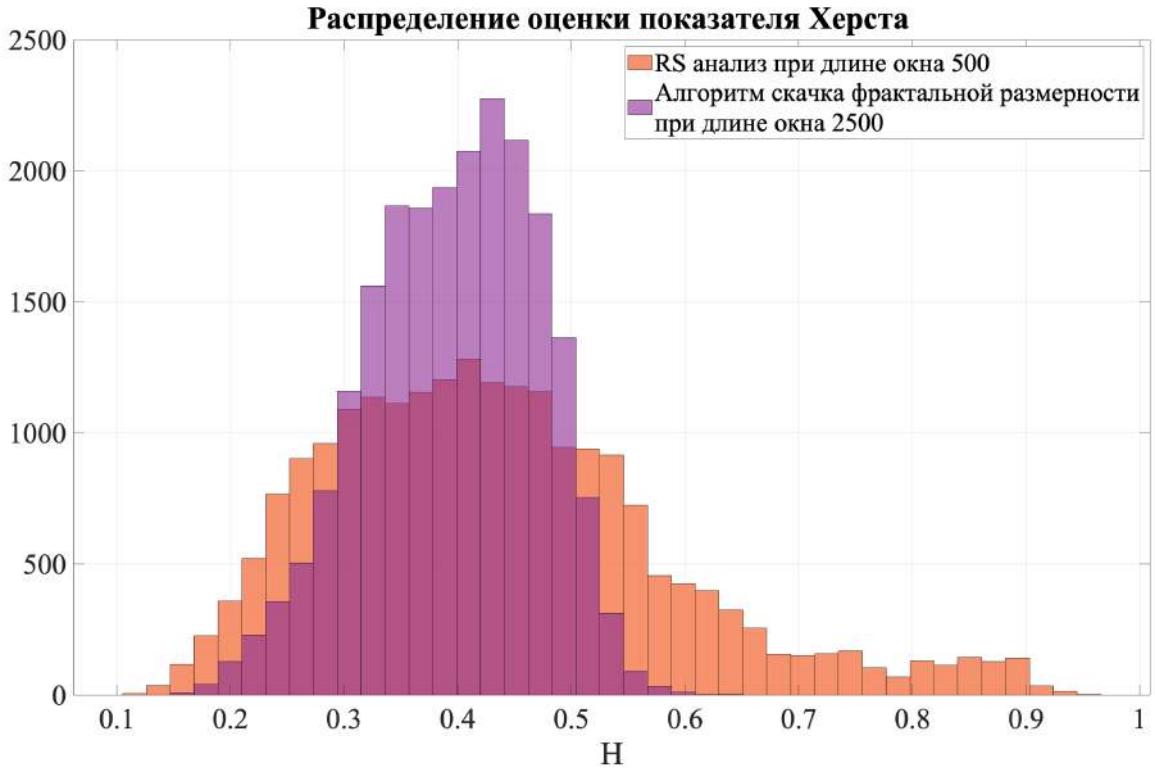


Рисунок 3 - Распределение оценки показателя Херста использовании алгоритма RS анализа и алгоритма скачка фрактальной размерности

Далее вычленим только атаки из перечисленных выше дампов и проведем их оценку. Так как длительность атак намного меньше, чем длительность нормального трафика, было решено уменьшить размер окна до 200.

Таблица 4 - Оценка статистических параметров атаки Mirai

Размер окна анализа	**100**	**150**	**200**
Среднее значение показателя H с применением RS анализа	0.5181	0.2672	0.2795
Среднее значение показателя H с применением алгоритма скачка фрактальной размерности	0.5196	0.6393	0.5766
Среднее значение показателя H с трешолдингом	0.5193	0.6390	0.5763
Дисперсия показателя H с применением RS анализа	0.00040	0.0554	0.0285
Дисперсия H с применением алгоритма скачка фрактальной размерности	0.0134	0.0084	0.0059
Дисперсия H с трешолдингом	0.0013	0.0009	0.0005
Асимметрия показателя H с применением RS анализа	2.481	1.432	2.615
Асимметрия H с применением алгоритма скачка фрактальной размерности	-0.623	-0.356	-0.351
Асимметрия H с трешолдингом	-3.186	-6.374	-9.126
Эксцесс показателя H с применением RS анализа	16.205	9.521	15.752
Эксцесс H с применением алгоритма скачка фрактальной размерности	4.412	3.613	3.097
Эксцесс H с трешолдингом	53.244	127.407	221.583

По полученным данным в таблице 4 видно, что атака Mirai имеет такой же показатель Херста что и нормальный трафик, но если проиллюстровать оценку показателя Херста в скользящем окне по всему трафику то можно заметить, что во время переходного процесса (с нормального трафика на атаку) происходит скачок фрактальной размерности и можно идентифицировать момент начала атаки и в данном случае, так как атака имеет большую длительность здесь имеет смысл подобрать длину окна соразмерную атаке. На рисунке 4 показана оценка показателя Херста в скользящем окне при использовании двух алгоритмов оценки.

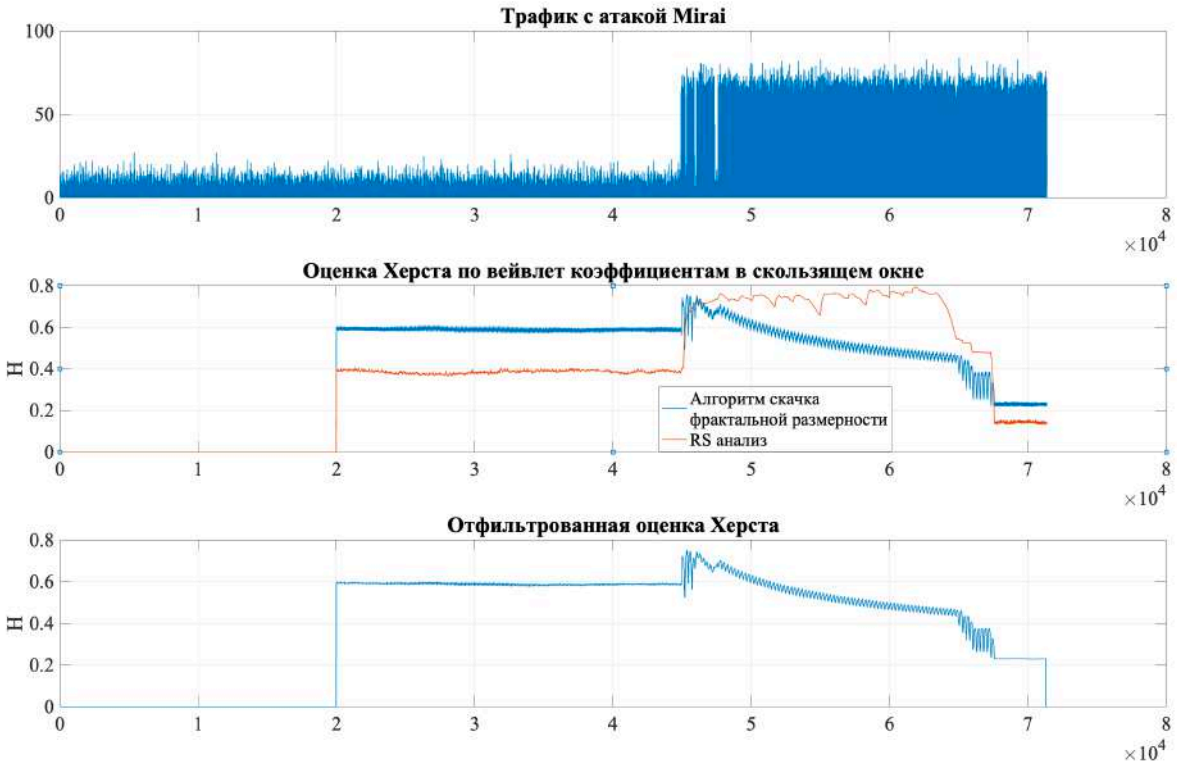


Рисунок 4 - Оценка показателя Херста в скользящем окне размером 2500 (250 сек) при использовании двух алгоритмов оценки

Как видно из рисунка 4 момент начала атаки фиксируется двумя алгоритмами, но оценка при помощи алгоритма скачка фрактальной размерности постепенно убывает и в момент полного наезда всем окном на участок атаки фиксирует значение на уровне 0.3. Если окно будет намного меньше самой атаки будет наблюдаться во время переходного процесса резкий скачок фрактальной размерности до уровня 1 и дальше резкий спад на уровень 0.3 на всем протяжении атаки. Если в ранних исследованиях наблюдался скачок вверх, то здесь наблюдается обратный скачок, что тоже может говорить об аномальном поведении трафика. На рисунке 6 представлена оценка показателя Херста в скользящем окне длительность 100 сек.

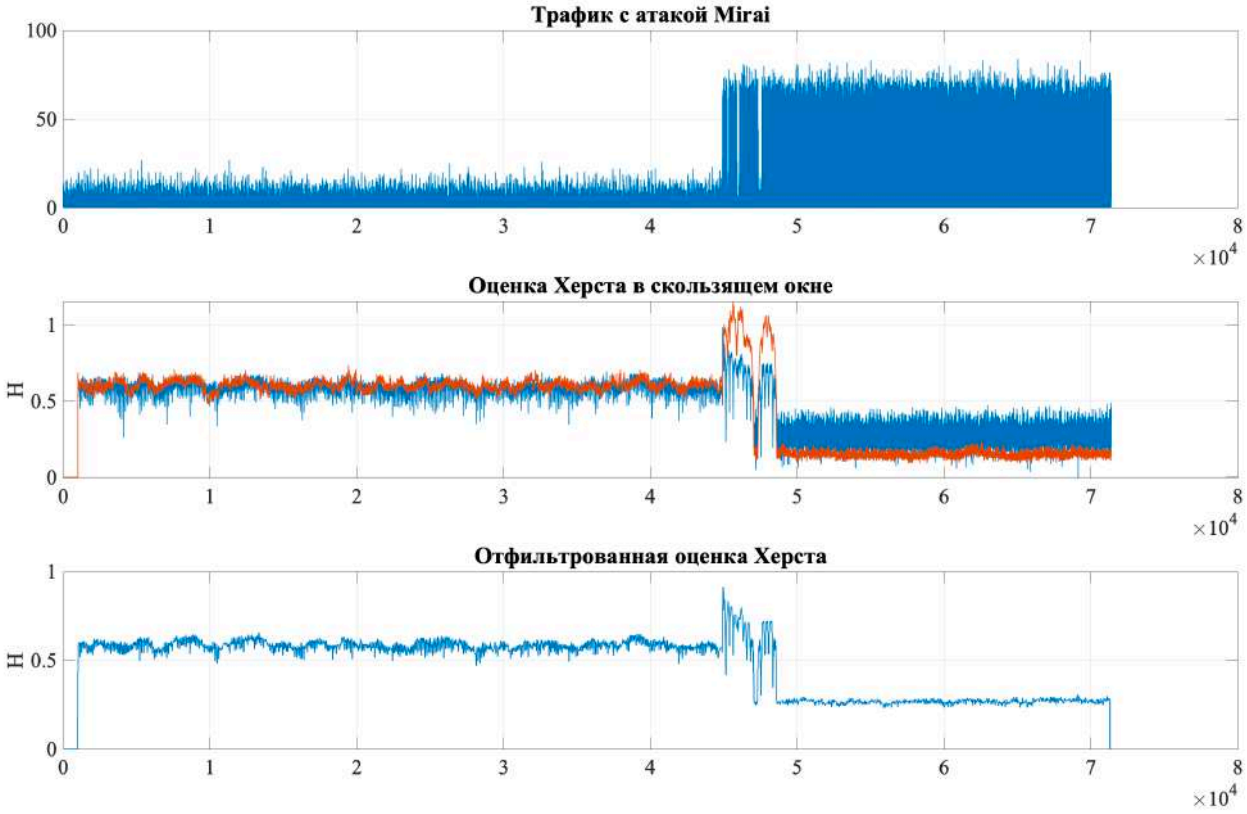


Рисунок 5 - Оценка показателя Херста в скользящем окне размером 1000 (100 сек) при использовании двух алгоритмов оценки

Таблица 5 - Оценка статистических параметров атаки OS scan

Размер окна анализа	**100**	**150**	**200**
Среднее значение показателя H с применением RS анализа	0.6491	0.9331	0.9426
Среднее значение показателя H с применением алгоритма скачка фрактальной размерности	0.8417	0.8714	0.9830
Среднее значение показателя H с трешолдингом	0.8942	-	
Дисперсия показателя H с применением RS анализа	0.0008	0.0706	0.0410
Дисперсия H с применением алгоритма скачка фрактальной размерности	0.0364	0.0254	0.0184
Дисперсия H с трешолдингом	0.0023		
Асимметрия показателя H с применением RS анализа	-0.7038	-0.8917	0.0805
Асимметрия H с применением алгоритма скачка фрактальной размерности	0.2645	0.3213	-1.8432
Асимметрия H с трешолдингом	-0.5042		
Эксцесс показателя H с применением RS анализа	2.7043	5.3770	1.8917
Эксцесс H с применением алгоритма скачка фрактальной размерности	2.0515	1.4654	5.5716
Эксцесс H с трешолдингом	1.2542		

Атака OS scan имеет отличный от нормального трафика высокий показатель Херста и идентифицировать атаку несложно. Проиллюстрируем на рисунке 6 обнаружение атаки OS scan алгоритмами при длине окна 30 сек (300 отсчетов).

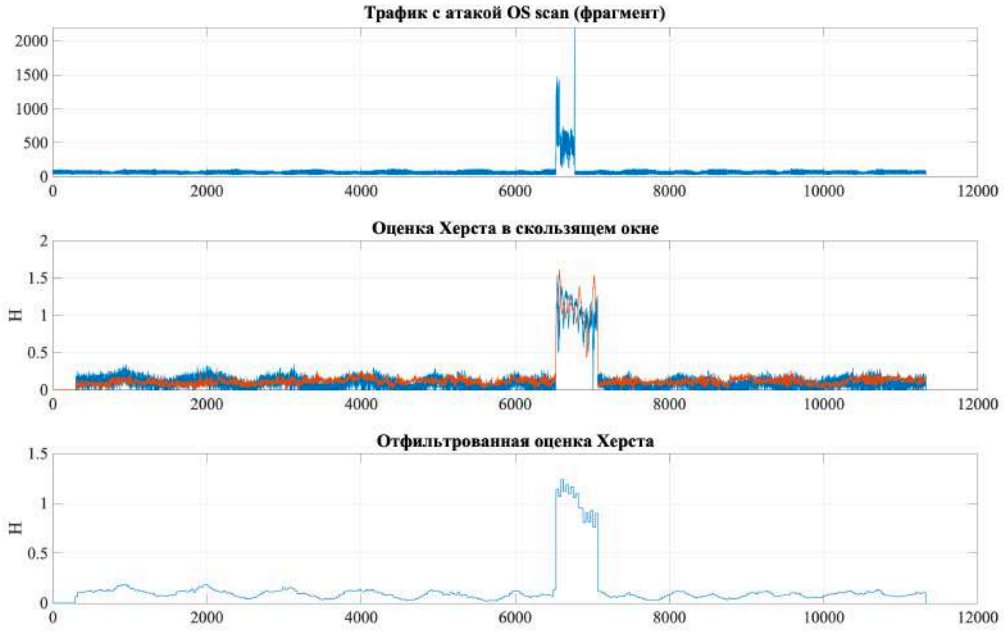


Рисунок 6. обнаружение атаки OS scan алгоритмами при длине окна 30 сек (300 отсчетов)

Таблица 6 - Оценка статистических параметров атаки SSDP Flood

Размер окна анализа	**100**	**150**	**200**
Среднее значение показателя H с применением RS анализа	0.6273	0.7700	0.8011
Среднее значение показателя H с применением алгоритма скачка фрактальной размерности	0.7604	0.7644	0.8372
Среднее значение показателя H с трешолдингом	0.7393	0.5549	0.6027
Дисперсия показателя H с применением RS анализа	0.0022	0.0849	0.0265
Дисперсия H с применением алгоритма скачка фрактальной размерности	0.0831	0.1285	0.1271
Дисперсия H с трешолдингом	0.0458	0.0305	0.0036
Асимметрия показателя H с применением RS анализа	0.6740	-0.8349	0.4747
Асимметрия H с применением алгоритма скачка фрактальной размерности	1.3010	0.3072	-0.1303
Асимметрия H с трешолдингом	1.2412	-0.6961	-1.7489
Эксцесс показателя H с применением RS анализа	2.5742	4.0648	2.9383
Эксцесс H с применением алгоритма скачка фрактальной размерности	4.4133	3.5777	2.6963
Эксцесс H с трешолдингом	3.1654	4.9049	4.5487

По полученным данным можно сделать вывод, что атака будет определяться скачком фрактальной размерности и это хорошо видно на рисунке 7.

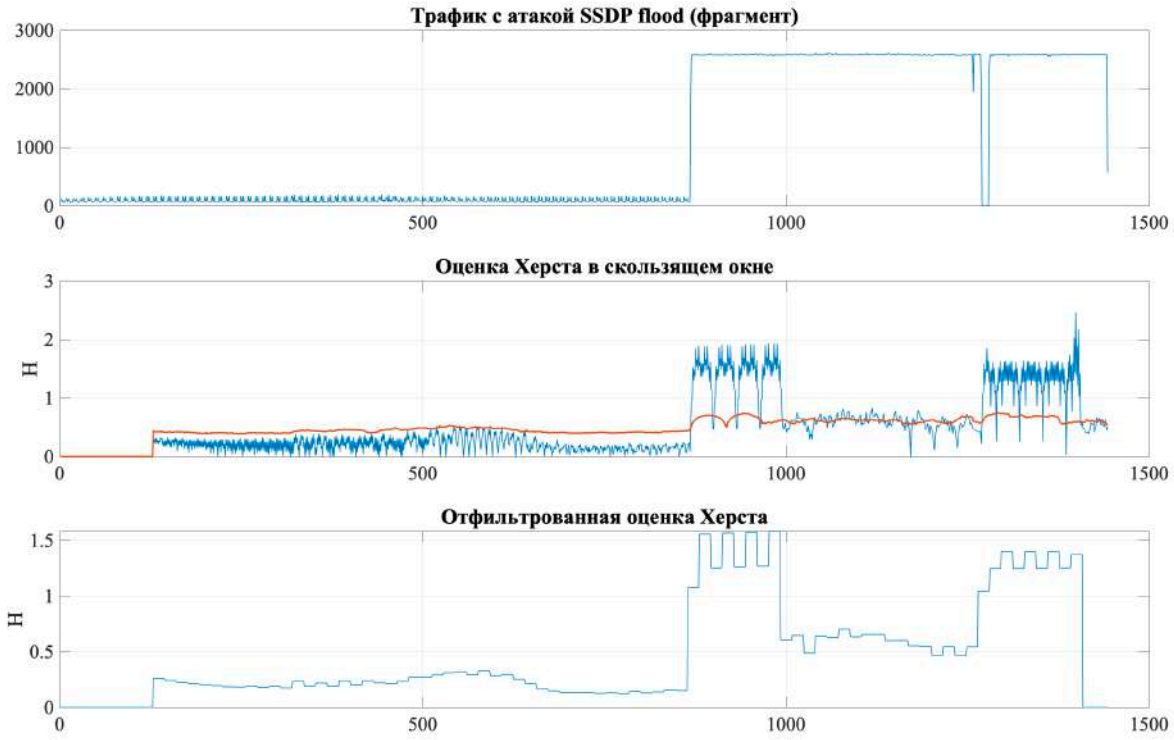


Рисунок 7 - Оценка показателя Херста в скользящем окне фрагмента трафика с атакой SSDP Flood

В момент наезда окна на атаку виден аномальный скачок показателя Херста, что можно обосновать нестационарностью процесса при переходе от нормального трафика к атаке. При детальном рассмотрении графика видно, что оба алгоритма позволяют оценить момент начала атаки и на самой атаке показатель Херста выше.

Приложение Б Алгоритм моделирования последовательности ФГШ

Проведем моделирование ФГШ, используя математическую среду R-Environment [1]. Для моделирования последовательности ФГШ воспользуемся методом $fgnSim()$, принимающим на вход такие параметры, как n – число элементов последовательности, H – значение параметра Херста в моделируемой последовательности. Среднее значение моделируемой выборки и среднеквадратическое отклонение по умолчанию задаются в 0 и 1 соответственно. Метод реализует алгоритм:

```
z = rnorm(2*n)
zr = z[c(1:n)]
zi = z[c((n+1):(2*n))]
zic = -zi
zi[1] = 0
zr[1] = zr[1]*sqrt(2)
zi[n] = 0
zr[n] = zr[n]*sqrt(2)
zr = c(zr[c(1:n)], zr[c((n-1):2)])
zi = c(zi[c(1:n)], zic[c((n-1):2)])
z = complex(real = zr,imaginary = zi)
# .gkFGN0:
k = 0:(n-1)
gammak = (abs(k-1)**(2*H)-2*abs(k)**(2*H)+abs(k+1)**(2*H))/2
ind = c(0:(n - 2), (n - 1), (n - 2):1)
.gkFGN0 = fft(c(gammak[ind+1]), inverse = TRUE)
gksqrt = Re(.gkFGN0)
if (all(gksqrt > 0)) {
gksqrt = sqrt(gksqrt)
z = z*gksqrt
z = fft(z, inverse = TRUE)
```

```
z = 0.5*(n-1)**(-0.5)*z
z = Re(z[c(1:n)])
} else {
gksqrt = 0*gksqrt
stop("Re(gk)-vector not positive")
}
# Standardize:
# (z-mean(z))/sqrt(var(z))
ans = std*drop(z) + mean
```

Приложение В Признаки набора данных UNSW-NB15

Таблица 1 - Признаки набора данных UNSW-NB15

№	Признак	Описание
Потоковые признаки		
1	Scrip	IP адреса отправителя
2	Sport	Номер порта отправителя
3	Dstip	IP адреса получателя
4	Dsport	Номер порта получателя
5	Proto	Протокол связи
Базовые признаки		
6	State	Состояние и его соответствующий протокол, например, ACC, CLO, еще (-)
7	Dur	Общая продолжительность записи
8	Sbyte	Число байтов от отправителя к получателю
9	Dbyte	Число байтов от получателя к отправителю
10	Sttl	Время существования от отправителя к получателю
11	Dttl	Время существования от получателя к отправителю
12	Sloss	Пакеты отправителя ретранслированы или потеряны
13	Dloss	Пакеты получателя ретранслированы или потеряны
14	Service	http, ftp, ssh, dns...,else
15	Sload	Биты отправителя в секунду
16	Dload	Биты получателя в секунду
17	Spkts	Количество пакетов от отправителя к получателю
18	dpkts	Количество пакетов от получателя к отправителю
Содержательные признаки		
19	Swin	Окно подтверждения TCP отправителя
20	Dwin	Окно подтверждения TCP получателя
21	Stcpb	Номер очереди TCP отправителя
22	Dtcpb	Номер очереди TCP получателя
23	Smeansz	Среднее значение размера пакета, переданного с помощью src
24	Dmeansz	Среднее значение пакета, переданного с помощью dst
25	Trans_depth	Глубина подключения http транзакции запроса/ ответа
26	Res_bdy_len	Размер данных, переданных от http службы сервера

Продолжение таблицы 1

№	Признак	Описание
Временные признаки		
27	Sjit	Джиттер отправителя (мс)
28	Djit	Джиттер получателя (мс)
29	Stime	Начало времени записи
30	Ltime	Конец времени записи
31	Sintpkt	Время поступления inter-packet отпр отправителя
32	Dinpkt	Время поступления inter-packet получателя (мс)
33	Tcprtt	Сумма ‘synack’ и ‘ackdat’ TCP
34	Synack	Время между SYN и SYN и SYN_ACK пакетами TCP
35	Ackdat	Время между SYN_ACK и ACK пакетами TCP
Дополнительные признаки		
36	Is_sm_ips_port	Если отправитель (1) и получатель (3) имеют одинаковые IPадреса и номера портов (2) (4) равны, тогда эта переменная принимает значение 1, в противном случае 0
37	Ct_state_ ttl	Число для каждого состояния (6), соответствующее определенному диапазону значений времени жизни отправителя/получате ля (10) (11).
38	Ct_flw_http_mthd	Число потоков, у которых есть такие методы, как Get и Post в http службе
39	Is_ftp_login	Если сеанс ftp инициирован пользователем и пароль правильный, тогда 1, в противном случае 0.
40	Ct_ftp_cmd	Число потоков, у которых есть команда в ftp сессии.
Признаки соединений		
41	Ct_srv_src	Число соединений, которые содержат одинаковые службы (14) и адреса отправителя в 100 соединениях, согласно последнему времени (26).
42	Ct_srv_dst	Число соединений, которые содержат одинаковые службы (14) и адреса получателя в 100 соединениях согласно последнему времени (26).
43	Ct_dst_ltm	Число соединений одного и того же адреса получателя (3) в каждых 100 соединениях согласно последнему времени (26)
44	Ct_src_ltm	Число соединений одного и того же адреса отправителя (1) в каждых 100 соединениях согласно последнему времени (26).
45	Ct_src_dport_ltm	Число соединений одного и того же адреса отправителя (1) и порта получателя (4) в 100 соединениях согласно последнему времени (26).
46	Ct_dst_sport_ltm	Число соединений одного и того же адреса получателя (1) и порта отправителя (4) в 100 соединениях согласно последнему времени (26).
47	Ct_dst_src_ltm	Число соединений одного и того же адреса отправителя (1) и адреса получателя (3) в 100 соединениях согласно последнему времени (26).

Продолжение таблицы 1

№	Признак	Описание
Признаки метки классов		
48	Attack_cat	Название каждого типа атаки. В этом наборе данных содержится 9 типов атак (Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode and Worms)
49	Label	0 для нормальной записи и 1 для записи атаки

Основные категориями записей набора данных UNSW-NB15 являются нормальные и атаки. Атаки классифицируются на девять типов в зависимости от характера атак.

В анализируемой базе данных UNSW-NB15 в наборе тестовых и обучающих выборок отсутствуют признаки 29-30, а также признаки 1-4. Всего выборки содержат **175341** и **82332** обучающих и тестовых записей соответственно. Распределение записей по категориям показано на *рисунках 1 и 2.*

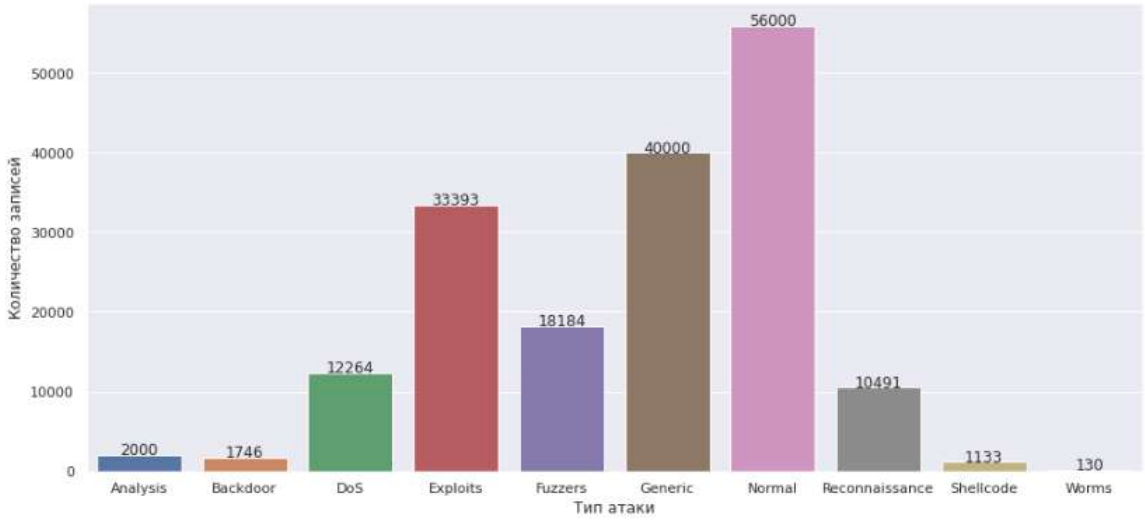


Рисунок 1 - Распределение записей в обучающей выборке для всех классов

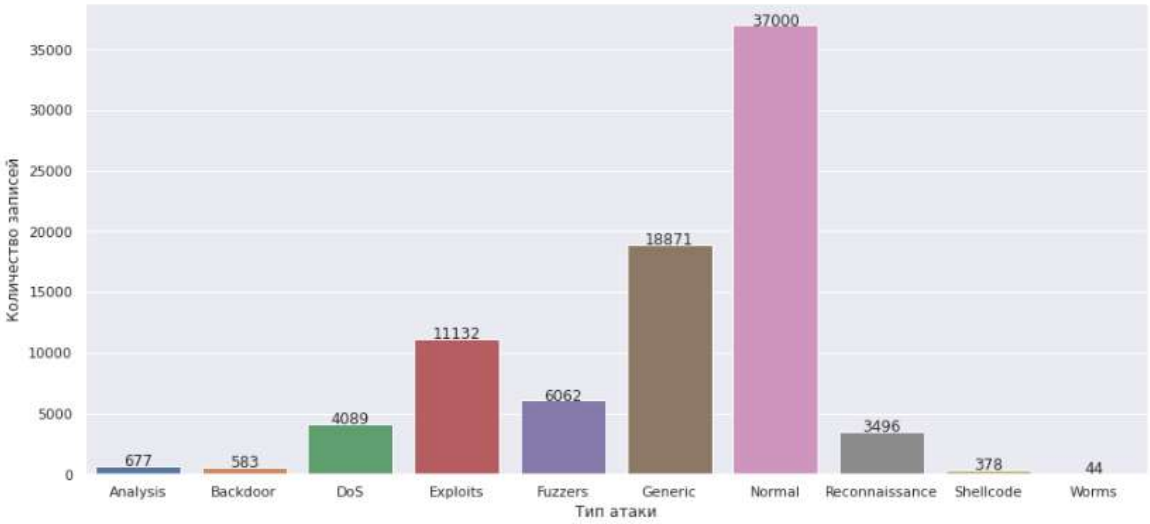


Рисунок 2 - Распределение записей в тестовой выборке для всех классов

Приложение Г Свидетельство о регистрации ПО

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2024614545

Программа для оценки показателя Хёрста сетевого трафика в скользящем окне с применением процедуры трешолдинга

Правообладатель: ***Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики» (RU)***

Авторы: ***Шелухин Олег Иванович (RU), Рыбаков Сергей Юрьевич (RU)***

Заявка № **2024612747**
Дата поступления **15 февраля 2024 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***27 февраля 2024 г.***

Руководитель Федеральной службы по интеллектуальной собственности

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат 429b6a0fe38b3164baf96f83b73b4aa7
Владелец Зубов Юрий Сергеевич
Действителен с 10.05.2023 по 02.08.2024

Ю.С. Зубов

Приложение Д Акт о внедрении в учебный процесс

«УТВЕРЖДАЮ»
Ректор ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»

_____ С.Д. Ерохин

«10» ____12____ 2024 г.

Акт об использовании в учебном процессе научных результатов диссертационной работы Рыбакова С.Ю. «Обнаружение и классификация компьютерных атак методами мультифрактального анализа и машинного обучения»

Комиссия в составе:

– руководителя Департамента организации и управления учебным процессом МТУСИ Вандиной О.Г.;

– декана факультета «Кибернетика и информационная безопасность» Иевлева О.П.;

– заведующего кафедрой ИБ Шелухина О.И. удостоверяет, что в учебном процессе кафедры ИБ при чтении курса лекций по дисциплине «Искусственный интеллект и машинное обучение в кибербезопасности» для бакалавров направления 10.03.01 и по дисциплине «Обнаружение вторжений в компьютерные сети» для магистров направления 10.04.01 «Информационная безопасность» используются результаты диссертационного исследования Рыбакова С.Ю., а именно: проведенный диссертантом анализ алгоритмов и методов мультифрактального анализа при обнаружения компьютерных атак.

Руководитель Департамента организации и управления учебным процессом МТУСИ	О.Г. Вандина
Декан факультета «Кибернетика и информационная безопасность»	О.П. Иевлев
Заведующий кафедрой «Информационная безопасность», д.т.н., профессор	О.И. Шелухин

Приложение Е Акт о внедрении результатов диссертационного исследования в научно-производственную деятельность ФГУП «НИИ «Квант»

Экз. № 1

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ
УНИТАРНОЕ ПРЕДПРИЯТИЕ
«НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ
ИНСТИТУТ «КВАНТ»

4-й Лихачевский пер., д.15, Москва, 125438
тел.: (499)154-80-21, факс: (499)154-14-18
www.rdi-kvant.ru, e-mail: info@rdi-kvant.ru
ОКПО 11496748, ОГРН 1027739824254
ИНН 7711000890, КПП 774301001

На № 6/22 от 24.01.2025

УТВЕРЖДАЮ
Главный инженер – первый заместитель директора
ФГУП «НИИ «Квант», к.т.н.
Г.Б. Кульков
«24» 01 2025 г.

АКТ

о внедрении (использовании) результатов диссертационной работы
Рыбакова Сергея Юрьевича
«ОБНАРУЖЕНИЕ И КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ АТАК МЕТОДАМИ МУЛЬТИФРАКТАЛЬНОГО АНАЛИЗА И МАШИННОГО ОБУЧЕНИЯ»

Комиссия в составе:		
председателя комиссии:	Начальника НИО-6, к.т.н.	Самарина Н.Н.
членов комиссии:	Главного инженера НИО-1, к.ф-м.н.	Игнатьева А.Н.
	Начальника отдела 62, к.т.н.	Рыбина М.А.

составила настоящий акт о том, что результаты диссертационной работы Рыбакова С.Ю. «Обнаружение и классификация компьютерных атак методами мультифрактального анализа и машинного обучения» используются в научно-производственной деятельности в ФГУП НИИ «Квант» (г. Москва) при проектировании и создании автоматизированных систем в защищенном исполнении, моделировании вторжений в действующие корпоративные сети и выполнении НИР «Доверие», а именно:

- новая методика оценки фрактальной размерности компьютерных атак в реальном времени, позволяющая существенно повысить достоверность их обнаружения в сетевом трафике;
- новый исследовательский фреймворк для выполнения экспериментов, связанных с решениями задач обнаружения и классификации сетевых атак, основанный на композиции приемов (механизмов) машинного обучения и характеристик мультифрактального спектра фрактальной

Продолжение приложения Е

размерности сетевого трафика и компьютерных атак.

Применение разработанного алгоритма и реализующего его программного обеспечения позволяет повысить эффективность обнаружения и классификации компьютерных атак в компьютерных сетях посредством применения мультифрактального анализа и методов машинного обучения.

Председатель комиссии: Н.Н. Самарин

Члены комиссии: А.Н. Игнатьев

М.А. Рыбин