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

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Москва - 2025

Работа выполнена в ордена Трудового Красного Знамени федеральном государственном бюджетном образовательном учреждении высшего образования «Московский технический университет связи и информатики» (МТУСИ) на кафедре «Информационная безопасность»

Научный руководитель: Шелухин Олег Иванович - Заслуженный деятель науки РФ, доктор технических наук, профессор, ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики», заведующий кафедрой «Информационная безопасность»

Официальные оппоненты: Павленко Евгений Юрьевич - доктор технических наук, доцент, Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский политехнический университет Петра Великого», Высшая школа кибербезопасности Института компьютерных наук и кибербезопасности, доцент

Израилов Константин Евгеньевич, кандидат технических наук, доцент, Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский университет Государственной противопожарной службы Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий имени Героя Российской Федерации генерала армии Е.Н. Зиничева», кафедра прикладной математики и безопасности информационных технологий, профессор

Ведущая организация Федеральное государственное бюджетное образовательное учреждение высшего образования «Поволжский государственный университет телекоммуникаций и информатики», г. Самара

Защита состоится «18» декабря 2025 г. в 11 часов 00 минут на заседании диссертационного совета 24.2.385.09 созданного на базе федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет промышленных технологий и дизайна» по адресу: 191186, Санкт-Петербург, ул. Большая Морская, д. 18, 437 аудитория

С диссертацией можно ознакомиться на сайте федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет промышленных технологий и дизайна» и в библиотеке по адресу: 190068, Санкт-Петербург, Вознесенский пр., д. 46, https://sutd.ru/nauka/dissertacii/.

Автореферат разослан «___» _____ 2025 г.

Ученый секретарь
диссертационного совета 24.2.385.09
доктор технических наук, доцент Сиротина Лидия Константиновна

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

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., Израилов 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.

Объем и структура диссертационной работы.

Диссертация состоит из введения, четырёх глав, заключения, списка используемых источников (125 наименований) и шести приложений. Основное содержимое диссертации (без списка используемых источников и приложений) изложено на 122 страницах машинописного текста, иллюстрировано 39 рисунками и содержит 19 таблиц.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы, определена цель и научная задача диссертационной работы. Сформулированы частные задачи исследования.

Первый раздел посвящен анализу современных методов и алгоритмов обнаружения КА, оценке фрактальной размерности ФР, включая методы мультифрактального анализа и методы машинного обучения.

Анализ наиболее распространённых методов машинного обучения, касающихся обнаружения КА в компьютерных сетях показал, что несмотря на высокую точность обнаружения, современным классификаторам свойственна относительно большая вероятность ложных срабатываний (ошибок 1-го рода).

Анализ алгоритмов обнаружения и классификации КА, основанных на методах математической статистики, показал, что подобные алгоритмы достаточно точно выявляют аномальные всплески в режиме офлайн, но неудовлетворительны для работы в режиме онлайн.

На основании аналитического обзора уточнены частные задачи исследования.

Второй раздел посвящен разработке методического аппарата по оценке фрактальных свойств КА с использованием вейвлет анализа в режиме онлайн, а также экспериментальной оценке фрактальных свойств компьютерных атак.

Поскольку аномальная активность в сети (включая КА), как правило приводит к значительному изменению текущего значения ФР, это может использоваться для определения момента начала атаки (аномалии). При этом выявление несвойственных (для нормального сетевого трафика) структурных особенностей осуществлялся с помощью кратномасштабного анализа и оценки показателя Херста H, однозначно связанного с фрактальной размерностью Хаусдорфа D_f соотношением $D_f = 2\text{-}H$.

Поскольку D_f и H различаются на постоянную константу для оценки фрактальной размерности в режиме онлайн в работе использована оценка показателя Херста в скользящем окне размером L выборок.

Предложено модифицировать метод оценки ФР компьютерных атак путем дополнительной вторичной фильтрации текущих оценок. Для нейтрализации резких «случайных» выбросов и уменьшения дисперсии используется процедура трешолдинга по отношению к коэффициентам детализации вейвлет разложения. Под трешолдингом понимается очистка сигналов от шумов на основе вейвлет преобразования.

С использованием трешолдинга получено новое соотношение для текущей модели оценки показателя Херста в текущий момент времени t_m, которое легло в основу разработанного алгоритма:

$$\widehat{H}(t_m) = \sum_{l=1}^{L_0} a_{j_0,l}^{(H)} \varphi_l^{(H)}(t_m) + \sum_{j=1}^{J} \sum_{l=1}^{L_j} T\left(d_{j,l}^{(H)}\right) \psi_{j,l}^{(H)}(t_m), \qquad (1)$$

где $a_{j_0,l}^{(H)}, d_{j,l}^{(H)}$ - аппроксимирующие и детализирующие коэффициенты оценки показателя Херста при m-м положении окна фильтрации; $T(d_{j,l}^{(H)})$ – отфильтрованные с помощью трешолдинга детализирующие вейвлет-коэффициенты; $a_{j_0,l}^{(H)} = \left\langle \widehat{H}(t_m), \varphi_l^{(H)} \right\rangle$ – масштабный коэффициент аппроксимации,

равный скалярному произведению оценки показателя Херста $\widehat{H}(t_m)$ и функции «самого грубого» масштаба J, смещенной на l единиц масштаба вправо от начала координат; $d_{j,l}^{(H)} = \left\langle \widehat{H}(t_m), \psi_{J,l}^{(H)} \right\rangle -$ 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 $L_0 = 2^{J_{\max}}, (L_0 \le L)$, $J_{\max} = [\log_2 L]$ - максимальное число масштабов разложения; $[\log_2 L]$ - целая часть числа. Наибольшее распространение во фрактальном анализе получили два вида трешолдинга:

$$\text{жесткий - } T_h = d_{j,l}^{(H)} I\left(\left| d_{j,l}^{(H)} \right| > \tau \right) \tag{2}$$

$$\text{и мягкий - } T_s = sign(d)\left(\left| d_{j,l}^{(H)} \right| - \tau \right) I\left(\left| d_{j,l}^{(H)} \right| \ge \tau \right). \tag{3}$$

При дальнейшем исследовании предпочтение отдано жесткому трешолдингу вследствие выявления более лучшей фильтрации сигнала.

Новизна предложенной модели оценки ФР (1) и (2) заключается в дополнительной фильтрации коэффициентов детализации вейвлет-разложения обрабатываемых данных в скользящем окне.

Оценки эффективности алгоритма, разработанного на основе соотношений (1) и (2), заключались в его тестировании на известных базах данных компьютерных атак DARPA99, UNSW-NB15, Kitsune. На рисунке 1 представлен пример оценки ФР на примере типового трафика IoT и атаки Mirai. Из рисунка 1в виден эффект улучшения качества оценки показателя H от трешолдинга.

При обнаружении атаки в режиме онлайн объем анализируемого трафика ограничивается размером окна анализа L, поэтому число уровней разложения для разных материнских вейвлетов получается разным. Критерием качества оценки ФР был выбран минимум среднего значения *m(H)* и дисперсии *D(H)* оценки показателя Херста до и после вторичной фильтрации (1).

Исследования показали, что разработанный алгоритм текущей оценки за счет вторичной фильтрации позволяет уменьшить дисперсию текущих оценок показателя Херста не менее чем на 50% при использовании наиболее подходящего вейвлета типа Хаар. В гауссовском и асимптотическом приближении доверительный интервал оценки показателя Херста оценивается неравенством:

$$\widehat{H} - \sigma_{\widehat{H}} z_\beta \le H \le \widehat{H} + \sigma_{\widehat{H}} z_\beta, \tag{4}$$

где $z_\beta = 1 - \beta$ квантиль стандартного гауссовского распределения, $P(z \ge z_\beta) = \beta$. Результаты подсчитывались при $\beta = 0.025$ (т.е. доверительной вероятности 0,95), при этом среднее значение оценки *m(H)* оставалось не смещенным и неизменным.

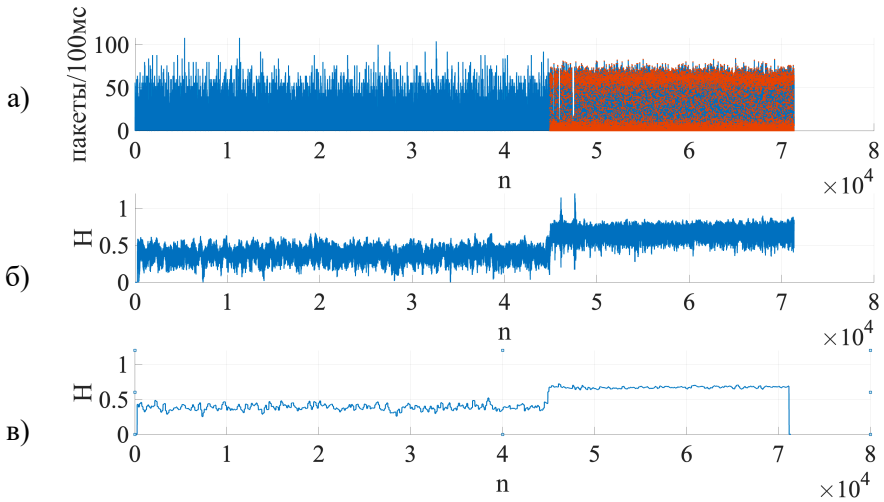

Рисунок 1 – Оценка показателя Херста H трафика IoT при воздействии атаки Mirai в скользящем окне размером Δ= 20 сек: а) фрагмент трафика с атакой Mirai; б) оценка H в скользящем окне без фильтрации; в) оценка H в скользящем окне с фильтрацией (трешолдингом)

На основе разработанной модели исследованы статистические характеристики ФР различных КА на примере сетей IoT. Некоторые результаты представлены на рисунке 2. Видно, что вторичная фильтрация с использованием вейвлета Хаара значительно упрощает и уточняет процедуру оценки H.

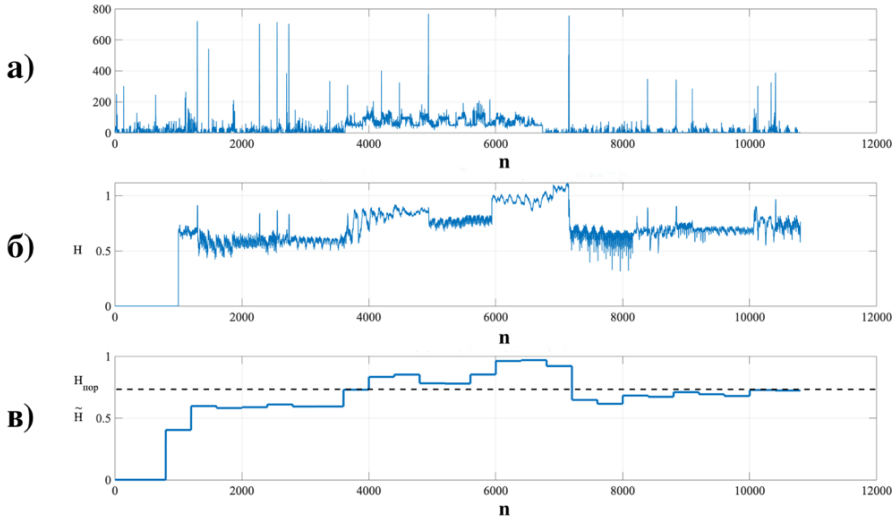

Рисунок 2 – Графики текущих процессов: а) трафик с атакой Neptune; б) оценка показателя Херста в скользящем окне; в) оценка показателя Херста после вторичной фильтрации с использованием вейвлета Хаара

Вычислялись текущие (онлайн) значения в момент t_j, которые характеризуют форму (сигнатуру) плотности распределения вероятностей w(H) параметра Херста: выборочное среднее $M_{H,i}$, выборочная дисперсия$D_{H,i}$; коэффициент асимметрии $\gamma_{H1,i}$, коэффициент эксцесса $\gamma_{H2,i}$. Показано, что они являются информативными и могут быть использованы для повышения эффективности обнаружения/классификации КА.

В третьем разделе представлены результаты исследования процесса обнаружения КА в виде фиксации скачков фрактальной размерности в реальном времени, а также исследованы пути повышения точности обнаружения с помощью модификации известных алгоритмов классификации машинного обучения.

Апробация модели (1) и (2) осуществлялась на реальных данных, включающих в себя как трафик без атак, так и аномалии в виде атаки Neptune (SYN-flood). Алгоритм обнаружения реализует операцию сравнения текущей оценки показателя Херста $\widehat{\mathrm{H}}_{t_m}$ с пороговым уровнем $\mathrm{H}_{\text{пор}}$. Вероятность правильной фиксации (обнаружения) КА оценивалась при помощи известной формулы $P_{\text{ПО}} = P\{(\sum \widehat{H_i} > H_{\text{пор}}; i = \overline{1,n})|\mathrm{A}_1\}$. Выбор порогового уровня $\mathrm{H}_{\text{пор}} > 0.5$ осуществлялся, исходя из заданной величины ошибки 2-го рода $P_{\text{ош.2}} = P\{(\sum \widehat{H_i} < H_{\text{пор}}; i = \overline{1,n})|\mathrm{A}_0\}$. Здесь A_1 и A_0 гипотезы соответственно наличия и отсутствия КА в наблюдаемой последовательности длительностью $\{i = \overline{1,n}\}$.

На рисунке 2 показано, что атака в режиме онлайн обнаруживается путем сравнения получаемой величины текущей оценки параметра H (в скользящем окне) с пороговым уровнем $H_{\text{пор}} = 0{,}75$.

На рисунке 3 представлены зависимости характеристик $P_{\text{ПО}}(H_{\text{пор}})$ и $P_{\text{ОШ2}}(H_{\text{пор}})$ при разной длине окна обнаружения Δ до и после вторичной фильтрации.

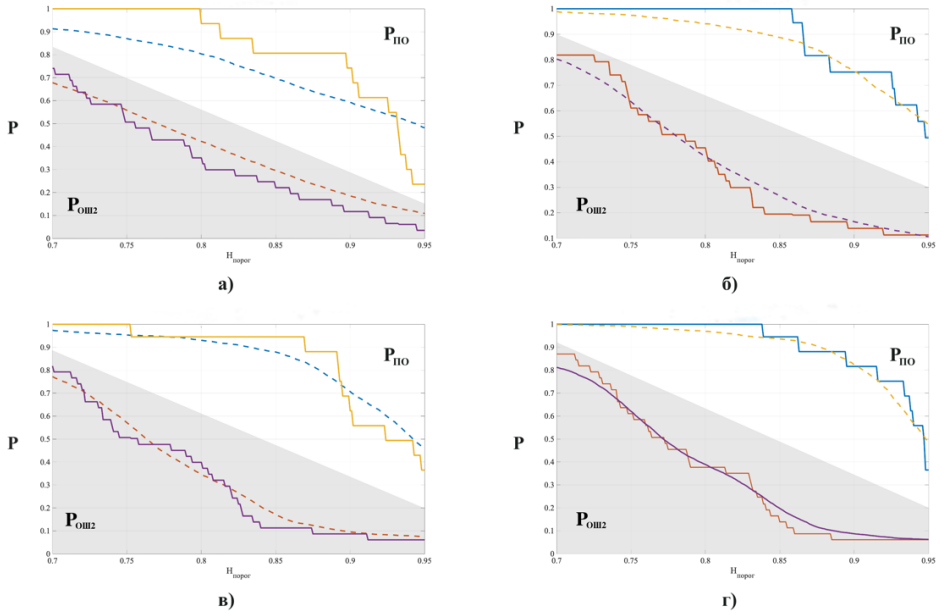

Рисунок 3 – Графики зависимостей $P_{\text{ПО}}(H_{\text{пор}})$ и $P_{\text{ОШ2}}(H_{\text{пор}})$ от величины $P_{\text{ПО}}(H_{\text{пор}})$ при $\Delta = var$ до и после фильтрации: а) Δ = 20 сек; б) Δ = 50 сек; в) Δ = 70 сек; г) Δ = 100 сек

Из рисунка 3 видно, что процедура трешолдинга позволяет повысить $P_{\text{ПО}}$ (приблизительно на 10%), в то время как увеличение размера окна Δ>50 сек. слабо влияет на метрики $P_{\text{ПО}}$ и $P_{\text{ОШ2}}$. Наилучшее соотношение между зависимостями $P_{\text{ПО}}$ и $P_{\text{ОШ2}}$ осуществляется при $\mathrm{H}_{\text{пор}}$ = 0,8…0,9 для максимального Δ = 100 сек.

Исследовались зависимости $P_{\text{ПО}}(H_{\text{пор}})$; $P_{\text{ОШ2}}(H_{\text{пор}})$ при разном количестве уровней разложения J = 2…10 и вторичной фильтрации показателя Херста. Показано, что при увеличении числа уровней разложения во время фильтрации позволяет уменьшить число ложных срабатываний.

Эффективность предложенной модели дополнительно повышается за счет использования известных атрибутов КА и применения алгоритмов машинного

обучения для бинарной/многоклассовой классификации. Так, в одной успешной реализации число используемых атрибутов КА в сетях IoT было 115, а в случае UNSW-NB15 – 49. Тем не менее несмотря на использование значительного числа информативных атрибутов, обеспечить даже 99% качество классификации КА не удается, что обусловлено, прежде всего нестационарным характером реального трафика.

Для повышения эффективности классификации КА предложено использовать в качестве дополнительных информационных атрибутов выявленные различия в устойчивых статистических характеристиках ФР атак и типового трафика без атак. Такими атрибутами, в частности, могут быть среднее значение, дисперсия, коэффициенты асимметрии и эксцесса, характеризующие распределение ФР.

Оценка качества бинарной классификации сетевых атак и нормального трафика осуществлялась при помощи известных баз данных и использования широкого класса алгоритмов машинного обучения: метод k-ближайших соседей (k-Nearest Neighbors, k-NN); множественная логистическая регрессия (Logistic Regression, LR); Мультиномиальный Наивный Байес (Multinomial Naive Bayes, NB); дерево решений (Decision Tree Classifier, DTC); случайный лес (Random Forest, RF); Ada Boost (AB). Для оценки эффективности их работы использовались следующие метрики: точность (precision), полнота (recall), F-мера, ROC-кривые ошибок, AUC – площадь под кривой ошибок.

В качестве дополнительных фрактальных атрибутов выбирались следующие экспериментальные статистические характеристики: M_H; D_H; $\gamma_{H1} = K_{\text{ас}}$; γ_{H2}=$K_{\text{Э}}$ характеризующие плотность распределения вероятности (ПРВ) фрактальной размерности w(H), для следующих типов КА и типового трафика: Normal Analysis; Backdoors; DoS; Exploit; Fuzzers; Generic; Reconnaissance. Некоторые результаты анализа полученных данных (по точности классификации) представлены на рисунке 4.

Из рисунка 4 видно, что использование дополнительных атрибутов в виде статистических параметров ФР для атак herst_stat и нормального трафика дает наибольший выигрыш в точности для алгоритмов классификации *k-NN* и LR (около 20%) и по метрике f1-score меньше (около 7%). Наибольший эффект достигается от использования в качестве дополнительного признака значения M_H. Для алгоритмов классификации DTC и RF выигрыш от дополнительного атрибута M_H составляет около 15–20% практически для всех метрик.

В случае алгоритма DTC использование одного дополнительного параметра M_H позволило уменьшить время на обучение и тестирование более чем в 1,5 раза, а для алгоритма RF – в 2 раза.

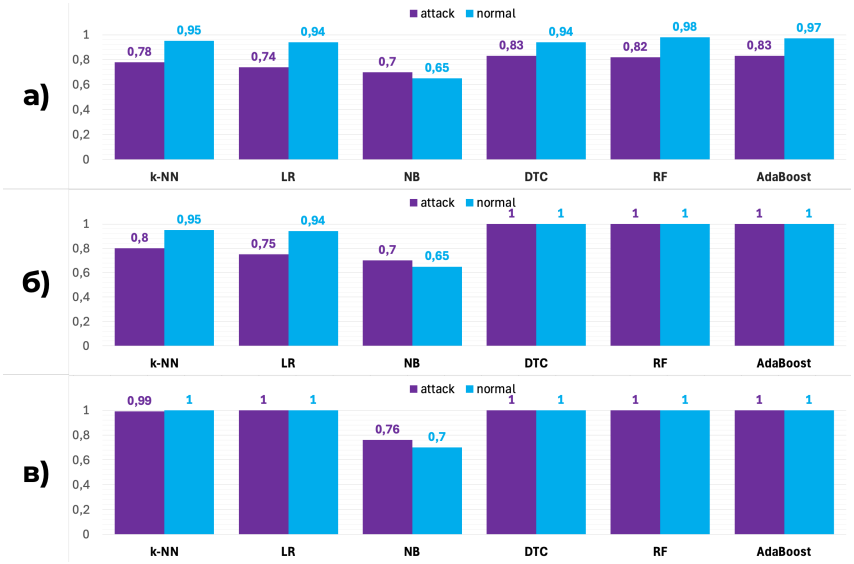

Рисунок 4 – Значения метрики precision для классификаций фрактальной размерности: а) без учета статистических параметров ФР; б) с учетом одного параметра M_H; в) с учетом четырех статистических параметров ФР

Использование всех 4-х дополнительных атрибутов M_H; D_H; $\gamma_{H1} = K_{\text{ac}}$; γ_{H2}=$K_{\text{Э}}$, позволило снизить время на обучение и тестирование в 3,5 раза для алгоритмов DTC и RF. Таким образом, введение дополнительных 4-х статистических параметров фрактальной размерности характеризующих ПРВ w(H), позволяет существенно улучшить качество и быстродействие бинарной классификации атак.

В разделе 4 предложен новый метод повышения точности обнаружения и классификации компьютерных атак, основанный на композиции алгоритмов машинного обучения и мультифрактального анализа трафика.

Поскольку свойство самоподобия наблюдается в широких временных масштабах (на уровне битов, пакетов, потоков), появление в трафике продолжительной атаки или аномальной активности изменяет не только его самоподобную природу, но и приводит к от моно - к мультифрактальной структуре. Поэтому информация об изменении характера ФР обрабатываемого трафика (при различном временном разрешении) может использоваться для улучшения рассмотренных выше алгоритмов обнаружения/классификации КА, и способна привести к улучшению показателей качества классификации методами машинного обучения.

Введено понятие мультифрактального спектра фрактальной размерности, под которым понимается последовательность текущих оценок ФР $\widehat{H}_{t_{Д_i}}$ в i-м окне анализа фиксированной длины Δ=*const* в зависимости от интервала разрешения (времени дискретизации $t_Д$):

$$\widehat{H_i} = \widehat{H}_{t_{Д_i}} = f\left(t_{Д_i}\right);\ i = \overline{1,L};\ t_{Д_i} \in \Delta. \qquad (5)$$

Установлено, что на разных временных шкалах (при разном $t_Д$) величина ФР изменяется, то есть является случайной, так что в общем случае трафик является мультифрактальным. В первом приближении оценка ФР (показатель Херста) является стационарной (квазистационарной) случайной величиной

$\widehat{H_i} \in N(m_{\widehat{H_i}}, \sigma^2_{\widehat{H_i}},)$; $i = \overline{1,L}$ и характеризуется средним значением $m_{\widehat{H_i}}$ и дисперсией $\sigma^2_{\widehat{H_i}}$ (или СКО $\sigma_{\widehat{H_i}}$).

В диссертационном исследования получены параметры МСФР для типичного трафика и разных типов КА в сети IoT. В таблице 1 приведены статистические характеристики оценок основных показателей распределения показателя Херста $\widehat{H}$ в скользящем окне Δ с применением процедуры трешолдинга для $L = 5$ окон оценивания (Δ=100 мс, 500 мс, 1,5 с, 10 с, 1 мин) для атаки типа Mirai.

Таблица 1 - Статистические характеристики оценки параметров МСФР

Δ, с	Параметры фрактальной размерности трафика			
	Атаки нет		Атака есть	
	$m_{\widehat{H_i}}$	$\sigma_{\widehat{H_i}}$ (СКО)	$m_{\widehat{H_i}}$	$\sigma_{\widehat{H_i}}$ (СКО)
0,1	0.39	0.0019	0.67	0.0087
0,5	0.53	0.0098	0.81	0.0804
1,5	0.69	0.0084	1.07	0.0732
10	0.41	0.0522	1.17	0.052
60	0.06	0.0143	0.93	0.007

Полученные значения $\{m_{\widehat{H_i}}, \sigma_{\widehat{H_i}}, i = \overline{1,5}\}$ трафика/КА, (в таблице 1), предложено добавить к уже имеющимся атрибутам значений МСФР. В результате количество атрибутов для классификации, например трафика/КА типа Mirai было увеличено до 120, что способствовало повышению точности классификации КА в сетях IoT на 5-7%.

Сравнительные оценки качества многоклассовой классификации алгоритмом RF для каждой классовой метки и двух наборов экспериментальных данных представлена в виде гистограмм на рисунке 5.

В результате получено, что при добавлении МСФР эффективность многоклассовой классификации атаки *«Mirai botnet»* алгоритмом Random Forest при глубине решающего дерева depth = 2 относительно *«OS scan»* и *«Normal»* заметно возрастает, выигрыш в $AUC_{OVR\ «Mirai»}$ составляет 7,6%. Остаточные ошибки вызваны недостаточной глубиной решающих деревьев.

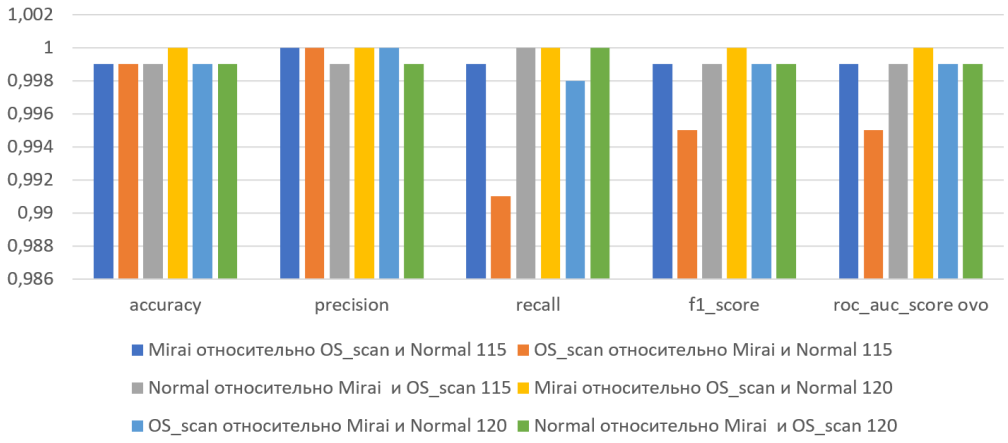

Рисунок 5 - Диаграммы эффективности многоклассовой классификации алгоритмом RF (с глубиной решающего дерева depth 2 OVR) для каждой классовой метки и двух наборов атрибутов экспериментальных данных

Добавление в качестве дополнительного параметра фрактальной размерности для КА *«Mirai botnet»* (при глубине решающего дерева depth=5), повышает эффективность ее классификации относительно *«OS scan»* и *«Normal»* до 0,999. Добавление МСФР при глубине решающего дерева depth = 5 позволяет достичь классификации КА близкой к идеальной ($AUC_{OVR\ «Mirai»} \rightarrow 1$).

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 исследования целесообразно внедрять в корпоративные системы мониторинга в качестве надстройки для раннего обнаружения аномалий. Практический подход заключается в онлайн-оценке показателя Херста с использованием вейвлета Хаара и временных окон от 100 мс до 2 минут, с калибровкой порогов на эталонном трафике. Для повышения точности классификации инцидентов рекомендуется расширять признаковое пространство, включая статистику показателя Херста и параметры мультифрактального спектра, с применением решающих деревьев. Перед развертыванием необходима адаптация на реальном трафике организации и тестирование на эталонных наборах данных.

Перспективы дальнейшей разработки темы связаны с повышением устойчивости и интерпретируемости детектирования в нестационарных условиях за счет разработки адаптивных процедур - динамической настройки параметров. Перспективными задачами являются строгая оценка достоверности мультифрактальных параметров и распространение методики на анализ шифрованного трафика (TLS/QUIC), а также на промышленные и киберфизические системы. Ключевым шагом дальнейших исследований в данном направлении видится в интеграции предложенных алгоритмов в модули предиктивной аналитики для раннего предупреждения о критических состояниях сети, что позволит дополнительно повысить достоверность обнаружения и точность классификации атак.

Список публикаций

В рецензируемых научных изданиях из перечня ВАК

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

2. 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.

3. Рыбаков, С. Ю. 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.

4. Рыбаков, С. Ю. Классификация компьютерных атак с использованием мультифрактального спектра фрактальной размерности / О. И. Шелухин, С. Ю. Рыбаков, Д. И. Раковский // Вопросы кибербезопасности. – 2024. – № 2(60). – С. 103–115.

5. Рыбаков, С. Ю. 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.

6. 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.

7. Рыбаков, С. Ю. 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.

8. Рыбаков, С. Ю. 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.

9. Рыбаков, С. Ю. 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.

В изданиях, индексируемых Scopus и Web of Science

10. Rybakov, S. Y. 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.

11. Rybakov, S. Y. 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.

Свидетельства о регистрации программ для ЭВМ

12. Программа для ЭВМ 2024614545 Российская Федерация. Программа для оценки показателя Херста сетевого трафика в скользящем окне с применением процедуры трешолдинга [текст] / Шелухин, О. И., Рыбаков, С. Ю. – № 2024612747 заявл. 15.02.2024; опубл. 27.02.2024.

Публикации в сборниках трудов научно-технических конференций

13. Рыбаков, С. Ю. Оценка мультифрактального спектра сетевого трафика для обнаружения компьютерных атак / С. Ю. Рыбаков // Фундаментальные и прикладные аспекты компьютерных технологий и информационной безопасности: Сб. ст. X Всерос. науч.-техн. конф. – Таганрог, 2024. – С. 23-26.

14. Рыбаков, С. Ю. Классификация компьютерных атак с использованием мультифрактального спектра фрактальной размерности / О. И. Шелухин, С. Ю. Рыбаков // Методы и технические средства обеспечения безопасности информации: матер. 33-й Всерос. науч.-техн. конф. (СПб, 24-27 июня 2024 г.). – СПб: Изд-во Политех. ун-та, 2024. – С. 38–40.

15. Рыбаков, С. Ю. Анализ алгоритмов машинного обучения для обеспечения безопасности Интернета вещей / С. Ю. Рыбаков, Ф. А. Ташлыков // Технологии информационного общества: Сб. тр. XVIII Межд. отраслевой науч.-техн. конф., Москва, 27–28 февраля 2024 г. – М.: МТУСИ, 2024. – С. 128-131. – EDN LRTDDR.

16. Рыбаков, С. Ю. Обнаружение сетевых атак в сетях интернета вещей методом фиксации скачков фрактальной размерности / С. Ю. Рыбаков, В. В. Спирин // Матер. 9-й Всерос. науч.-практ. конф. (г. Березники, 21 октября 2023 г.). – Пермь: Изд-во Перм. нац. исслед. политехн. ун-та, 2023. – С. 165–167.