Министерство цифрового развития, связи и массовых коммуникаций РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Поволжский государственный университет
телекоммуникаций и информатики»

На правах рукописи

ПЛАВАН Алексей Игоревич

МЕТОДЫ ОБНАРУЖЕНИЯ АНОМАЛИЙ В СЕТЕВОМ ТРАФИКЕ НА ОСНОВЕ ОПТИМАЛЬНОЙ ЛИНЕЙНОЙ ФИЛЬТРАЦИИ

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
Карташевский Вячеслав Григорьевич

Самара – 2026

ОГЛАВЛЕНИЕ

Введение 5
1. Анализ статистических характеристик сетевого трафика для выявления его характерных особенностей 13
1.1. Предназначение и методы анализа трафика 13
1.1.1. Сетевой трафик 13
1.1.2. Методы анализа трафика 13
1.2. Различные представления трафика 16
1.2.1. Случайный временной ряд 16
1.2.2. Случайный поток событий 17
1.3. Самоподобие трафика 19
1.3.1. Свойство самоподобия и его причины 19
1.3.2. Показатель Херста 20
1.3.3. АКФ самоподобного трафика 21
1.4. Анализ характеристик реального сетевого трафика 22
1.4.1. Исследование АКФ магистрального трафика 22
1.4.2. Влияние DoS-атак на АКФ и плотность распределения трафика 23
1.4.3. Исследование агрегированных статистических характеристик 25
1.4.4. Применение методов машинного обучения для анализа трафика 31
1.4.5. Влияние различных видов атак на характеристики трафика 36
1.5. Выводы по главе 1 41
2. Моделирование сетевого трафика с заданными характеристиками 42
2.1. Задачи моделирования трафика 42
2.1.1. Моделирование в телекоммуникационных сетях 42
2.1.2. Моделирование в задачах обеспечения ИБ 43
2.2. Методы моделирования интернет-трафика 44
2.2.1. Методы моделирования самоподобного трафика 44
2.2.2. Модель процесса всплесков Пуассона-Парето в симуляторе ns-3 46
2.2.3. Моделирование и обнаружение DoS-атак 47
2.2.4. Объединение трафика от нескольких источников 50

2.3. Методы моделирования случайных процессов 54
2.3.1. Классические методы моделирования случайных процессов 54
2.3.2. Способ выражения взаимосвязи АКФ на основе копулы 56
2.3.3. Результаты вычислительного эксперимента 61
2.4. Выводы по главе 2 68
3. Алгоритмы обнаружения аномалий на основе применения оптимальной линейной фильтрации 70
3.1. Обнаружение аномалий в компьютерных сетях 70
3.1.1. Сетевые аномалии 70
3.1.2. Системы обнаружения вторжений 71
3.1.3. Обзор существующих методов обнаружения аномалий 72
3.2. Оптимальная линейная фильтрация 74
3.2.1. Фильтр Винера 74
3.2.2. Фильтр Калмана 79
3.3. Ошибка фильтрации как критерий обнаружения аномалий 81
3.3.1. Метод на основе отклонения ошибки фильтрации 81
3.3.2. Метод на основе значения ошибки фильтрации 85
3.3.3. Пороговые значения 87
3.3.4. Бинарная классификация 89
3.3.5. Основные этапы алгоритма обнаружения аномалий 90
3.4. Выводы по главе 3 96
4. Оценка эффективности разработанных алгоритмов обнаружения аномалий в трафике 98
4.1. Обнаружение аномалий в смоделированном трафике 98
4.1.1. Моделирование смеси трафика с различной формой АКФ 98
4.1.2. Зависимость ошибки от отношения сигнал/шум 101
4.2. Обнаружение аномалий в реальном сетевом трафике 104
4.2.1. Обнаружение аномалий в трафике MAWI 104
4.2.2. Обнаружение аномалий в трафике CIC-IDS2017 106

4.2.3. Ошибка фильтрации как дополнительный признак в алгоритмах машинного обучения 112
4.3. Выводы по главе 4 116
Заключение 117
Список сокращений 122
Список литературы 124
Приложение А. Акты внедрения результатов работы 142
Приложение Б. Свидетельства о государственной регистрации программ для ЭВМ и электронных ресурсов 145

Введение

Актуальность темы исследования. С ростом объемов глобального сетевого трафика и развитием инструментов искусственного интеллекта количество и масштаб кибератак неуклонно увеличивается, что актуализирует проблему их своевременного и точного обнаружения. Среди каналов распространения вредоносного программного обеспечения (ВПО) компьютерные сети по частоте использования уступают лишь электронной почте, а число зондирующих и DDoS-атак, в том числе с использованием ботнетов, стабильно растет [1, 2].

Злоумышленник не может получить доступ к трафику, не воздействуя на него, то есть не установив соединение с некоторым сервером и не отправив пакеты данных. Появление нового источника трафика может влиять на состояние сети и значения её статистических характеристик. В отличие от систем обнаружения вторжений (СОВ) на основе злоупотреблений, такие изменения могут быть обнаружены СОВ на основе выявления аномалий, даже при отсутствии известных сигнатур для реализуемой атаки.

Большинство современных систем Network Traffic Analysis (NTA) реализуют обнаружение на основе сигнатур, некоторые применяют простые статистические методы, но чаще сразу переходят к более сложным алгоритмам машинного обучения и нейросетям. Тем не менее, статистические методы, основанные на анализе характеристик временных рядов, остаются актуальными и представляют значительный интерес благодаря высокой точности выявления аномалий при сравнительно более низких вычислительных затратах и лучшей интерпретируемости результатов [3].

Данные факторы обусловили актуальность исследования, которое посвящено разработке алгоритмов обнаружения аномалий в сетевом трафике на основе оптимальной линейной фильтрации с применением фильтра Колмогорова-Винера и анализа статистических характеристик трафика. Описание разработанных методов и результаты их экспериментального

исследования могут быть использованы для повышения безопасности сетей и защиты от кибератак.

Степень разработанности темы исследования. Проблема обеспечения информационной безопасности компьютерных сетей и обнаружения сетевых атак является предметом пристального внимания мирового научного сообщества на протяжении последних десятилетий. Основы построения СОВ были заложены в трудах таких ученых как Anderson J.P., Neumann P.G. и Denning D.E., в работе которой впервые вводится понятие профилей нормального поведения пользователя [4]. Становление и развитие научного направления защиты информации в отечественной науке связано с именами таких ученых как Котенко И.В., Зегжда П.Д., Герасименко В.А., Кульба В.В., Шелупанов А.А.

Самоподобная природа сетевого трафика, впервые отмеченная в работах Leland W.E., Taqqu M.S., Willinger W., Wilson D.V., поставила под сомнение эффективность классических пуассоновских моделей при анализе телекоммуникационных сетей. Значительный вклад в изучение свойств фрактального сетевого трафика и моделирование его параметров внесли Шелухин О.И., Осин А.В., Потапов А.А., Карташевский И.В., Треногин Н.Г., Соколов Д.Е., Лихтциндер Б.Я., Чабдаров Ш.М., Благов А.В., Привалов А.Ю., Багманов В.Х., Султанов А. Х., Nason G.P., Veitch D., Zukerman M.

Разработке методов обнаружения аномалий на основе интеллектуального анализа данных и машинного обучения посвящены, например, работы Васильева В.И., Вульфина А.М., Картака В.М., Гвоздева В.Е., Гетьмана А.И., Соколова А.Н., Cristophe D. Однако большинство методов на основе нейронных сетей, несмотря на высокую точность, требуют существенных вычислительных затрат, особенно при обучении, что затрудняет их применение в режиме реального времени на магистральных каналах связи.

Формирование основ теории оптимального оценивания и фильтрации случайных процессов, а также создание соответствующего математического

аппарата связаны с именами таких выдающихся ученых, как Wiener N., Kalman R.E., Bucy R.S., Haykin S., Колмогоров А.Н., Левин Б.Р., Смирнов Н.В., Стратонович Р.Л. Попытки применения статистических методов для обнаружения сетевых атак предпринимались в работах ряда современных исследователей, например Фаткиевой Р.Р., Рыбакова С.Ю., Ngong S., Lakhina A., Crovella M., Barford P. В большинстве работ фильтрация применяется для сглаживания временных рядов трафика, на основе прогнозирования которых строятся предположения о наличии аномалий в трафике, однако упрощенные линейные модели не всегда корректно описывают самоподобный характер трафика и не всегда позволяют обнаруживать распределенные по времени аномалии. Таким образом, актуальной научной задачей является разработка методов обнаружения аномалий, сочетающих в себе вычислительную эффективность линейной фильтрации с высокой точностью детектирования для минимизации ошибок первого и второго рода.

Объектом исследования является сетевой трафик в виде последовательности пакетов, порождаемых различными сетевыми устройствами.

Предметом исследования являются аномалии в сетевом трафике, выражающиеся в изменении его статистических характеристик.

Целью диссертационной работы является повышение защищенности телекоммуникационных систем за счет повышения эффективности алгоритмов обнаружения аномалий в сетевом трафике на основе его статистических характеристик.

Для достижения цели исследования поставлены и решены следующие задачи:

1. Провести анализ статистических характеристик реального сетевого трафика, таких как автокорреляционная функция (АКФ) и вероятностное распределение интервалов времени между пакетами, размеров пакетов и других параметров, и установить влияние различных видов атак на статистические характеристики трафика.

2. Провести моделирование реалистичного сетевого трафика, соответствующего нормальной активности пользователей и проведению атаки, изучить свойства объединенного трафика.

3. Разработать методы обнаружения аномалий в сетевом трафике на основе оптимальной линейной фильтрации.

4. Исследовать возможность применения признаков на основе статистических характеристик трафика в методах машинного обучения для повышения точности обнаружения аномалий.

5. Оценить эффективность разработанных методов на смоделированном и реальном трафике по различным метрикам.

Методы исследования включают в себя методы теории вероятностей и математической статистики, анализ временных рядов, в том числе методы корреляционного анализа, проверки статистических гипотез, моделирования случайных процессов, машинного обучения, и различные метрики оценки алгоритмов классификации.

Научная новизна полученных результатов:

1. Разработан алгоритм определения численных индикаторов сетевых атак по статистическим характеристикам трафика, *основанный* на методе «случайного леса», *отличающийся* возможностью определения не только важности признаков, но и их пороговых значений, и *позволяющий* оценивать их статистическую значимость.

2. Разработан метод моделирования случайных процессов, представляющих самоподобный Интернет-трафик, *основанный* на преобразовании распределения Рэлея, *отличающийся* применением копулы Фарли-Гумбеля-Моргенштерна для выражения аналитической связи между АКФ исходного и преобразованного процессов, и *позволяющий* повысить точность воспроизведения заданных статистических характеристик при моделировании легитимного трафика.

3. Разработаны методы обнаружения аномалий в сетевом трафике и реализующий их алгоритм, *основанные* на вычислении минимальной

среднеквадратической ошибки фильтрации и сравнении её с эталонным значением для легитимного трафика, *отличающиеся* возможностью учитывать шум наблюдений, и *позволяющие* выявлять сетевые атаки, связанные с изменением статистических характеристик трафика.

4. Предложен механизм формирования признаков для моделей машинного обучения, *основанный* на вычислении минимальной среднеквадратической ошибки фильтрации для различных представлений трафика, *отличающийся* объединением множества отсчетов АКФ в единый скалярный признак ошибки, и *позволяющий* повысить эффективность обнаружения сетевых атак алгоритмами обучения без учителя.

Положения, выносимые на защиту:

1. Алгоритм определения численных индикаторов сетевых атак по статистическим характеристикам трафика, основанный на методе «случайного леса».

2. Метод моделирования случайных процессов, представляющих самоподобный Интернет-трафик, основанный на преобразовании распределения Рэлея и применении копулы Фарли-Гумбеля-Моргенштерна.

3. Методы обнаружения аномалий в сетевом трафике и реализующий их алгоритм, основанные на вычислении минимальной среднеквадратической ошибки фильтрации и сравнении её с эталонным значением для легитимного трафика.

4. Механизм формирования признаков для моделей машинного обучения, предназначенных для обнаружения сетевых атак, основанный на вычислении минимальной среднеквадратической ошибки фильтрации для различных представлений трафика.

Теоретическая значимость исследования заключается в разработке алгоритма определения значимых статистических признаков различных видов сетевых атак, способа моделирования случайных процессов с заданными характеристиками на основе копул, методов обнаружения аномалий в сетевом трафике на основе минимальной среднеквадратической

ошибки оптимального фильтра Колмогорова-Винера, которые позволяют эффективно выявлять аномальные последовательности в трафике. Данные результаты вносят важный вклад в совершенствование моделей и методов обеспечения безопасности сетевого взаимодействия, так как их применение может позволить оперативно выявлять потенциальные угрозы и снизить риск инцидентов безопасности.

Практическая значимость исследования заключается в возможности применения полученных результатов для разработки перспективных средств защиты информации и мониторинга сетевого трафика. Внедрение разработанных алгоритмов в существующие корпоративные системы безопасности позволяет повысить число выявленных аномалий, обеспечив своевременное обнаружение и предупреждение атак и снижение количества инцидентов информационной безопасности.

Достоверность результатов работы обеспечивается корректным и обоснованным применением методов исследования, проведением вычислительных экспериментов на открытых наборах данных, проверкой статистической значимости полученных результатов, а также апробацией результатов исследований на международных и всероссийских конференциях и публикацией результатов в рецензируемых научных изданиях.

Связь исследований с научными программами. Часть исследования выполнена в рамках гранта Фонда содействия инновациям УМНИК «Разработка программного комплекса для выявления нарушений информационной безопасности на основе анализа статистических зависимостей в сетевом трафике» и гранта МТУСИ на реализацию научного проекта «Обнаружение аномалий сетевого трафика на основе линейного преобразования трафика по критерию минимума среднеквадратической ошибки» №37/21-к.

Соответствие паспорту специальности. Результаты диссертационной работы соответствуют следующим пунктам паспорта специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность»: **п.**

5 «Методы, модели и средства (комплексы средств) противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет» (положения 2, 3), **п. 6** «Методы, модели и средства мониторинга, предупреждения, обнаружения и противодействия нарушениям и компьютерным атакам в компьютерных сетях» (положения 1, 3, 4), **п. 15** «Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности» (положения 1, 3, 4).

Апробация работы. Основные результаты и положения диссертационного исследования докладывались и обсуждались на международных и всероссийских научных и научно-технических конференциях. Результаты работы внедрены в ООО «Идентификация» и в учебный процесс кафедры информационной безопасности ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики».

Публикации. По теме диссертационного исследования всего опубликовано 22 работы, отражающих основные полученные результаты, из них: 5 статей в ведущих научных журналах из Перечня рецензируемых научных изданий ВАК при Министерстве науки и высшего образования РФ, 1 научная работа в изданиях, индексируемых ведущими международными реферативными базами Web of Science и Scopus, 6 тезисов международных и 10 всероссийских научных и научно-технических конференций. Во время выполнения научного исследования разработаны 3 программы для ЭВМ, свидетельства о государственной регистрации: №2022614836, №2023664160, №2024611818.

Сведения о личном вкладе автора. Основные результаты диссертационной работы, представляющие научную новизну, а также анализ с соответствующими выводами, выполнены автором самостоятельно.

Некоторые из этих результатов подготовлены к публикации в сотрудничестве с соавторами, при этом определяющий вклад вносил автор данной работы.

Структура и объем работы. Работа состоит из введения, четырех глав, заключения, списка сокращений, списка литературы и приложений, содержит 52 рисунка, 11 таблиц, 107 формул, 2 приложения, выполнена на 147 страницах. Список использованной литературы включает 139 источников.

1. Анализ статистических характеристик сетевого трафика для выявления его характерных особенностей

1.1. Предназначение и методы анализа трафика

1.1.1. Сетевой трафик

Сегодня сетевые технологии стали неотъемлемой частью повседневной деятельности, обеспечивая передачу данных и обмен информацией в глобальных масштабах. Однако расширение масштабов цифровизации сопряжено с ростом риска кибератак, направленных на нарушение конфиденциальности, целостности и доступности данных. В связи с этим обеспечение сетевой безопасности и обнаружение вторжений приобретают первостепенное значение. Одним из ключевых методов обнаружения вторжений является анализ сетевого трафика с использованием различных подходов и алгоритмов.

Трафик – это последовательность пакетов данных, формируемая различными источниками и передаваемая через компьютерную сеть в течение определенного промежутка времени [5]. Трафик можно разделить на входящий, исходящий, внутренний (обмен информацией внутри локальной сети) и внешний (Интернет-трафик).

Анализ трафика играет важнейшую роль на этапе тестирования на проникновение [6]: он позволяет выявить проблемы в работе сети (в том числе вызванные активностью злоумышленников), обнаружить несанкционированную деятельность, восстановить последовательность событий перед инцидентом безопасности и определить паттерны использования сети клиентами. Кроме того, анализ трафика используется для сбора статистики с целью модернизации системы.

1.1.2. Методы анализа трафика

Из последовательности пакетов полезную информацию можно извлечь различными способами в зависимости от целей анализа и уровня доступа к данным. Один из основных методов анализа сетевого трафика – анализ

заголовков отдельных пакетов [7]. Атаки обнаруживаются преимущественно посредством поиска специфических сигнатур и сравнения с шаблонами поведения вредоносных программ [8], например, сочетанием TCP-флагов. Сигнатурный анализ трафика также может искать специфические шаблоны в содержимом пакетов для обнаружения известных атак.

Глубокий анализ пакетов (Deep Packet Inspection, DPI) включает в себя детальное исследование содержимого пакетов (полезной нагрузки), в том числе декодирование протоколов и дешифрование данных. Данный метод позволяет обнаруживать атаки, эксплуатирующие уязвимости протоколов прикладного уровня, выполнять фильтрацию пакетов по содержимому и выявлять обход запретов через скрытые каналы передачи данных [9, 10].

На более высоком уровне абстракции находится анализ потоков трафика. Поток состоит из пакетов, сгруппированных по заданному набору признаков, чаще всего используется кортеж из пяти полей (5-tuple): IP-адрес источника, порт источника, IP-адрес назначения, порт назначения, тип протокола из заголовка IP-пакета [11, 12], также может включаться тип сервиса и индекс интерфейса. Выделение данных атрибутов требует разбора заголовков как минимум до сетевого уровня для каждого пакета, что может привести к проблемам с производительностью. Это актуально и для методов на основе сигнатур, особенно извлекаемых из содержимого пакета [12].

При мониторинге сетевой активности трафик является по сути случайным процессом, поэтому для его анализа широко используются стандартные методы теории вероятностей и математической статистики. Распределение этого процесса в реальной сети заранее неизвестно, и его можно лишь примерно определить после некоторого количества наблюдений. Объектом исследования в прикладной статистике как раз и являются статистические данные, полученные в результате серии из нескольких наблюдений или экспериментов. Статистический анализ может применяться к отдельным пакетам или потокам, всем потокам отдельного узла, или подсети, для анализа взаимодействий между узлами в виде графов потоков.

Выбор того или иного уровня агрегации представляет собой компромисс между скоростью обнаружения и пропускной способностью, а также зависит от доступных точек подключения средств мониторинга к сети [7].

Случайным процессом называется случайная функция времени. Функция называется случайной, если в результате эксперимента она принимает тот или иной вид, причем заранее не известно, какой именно. Для описания экспериментально наблюдаемых случайных величин (СВ) используются числовые характеристики или *моменты* случайной величины m_k – математическое ожидание (среднее значение), дисперсия, коэффициенты асимметрии и эксцесса.

Степень линейной зависимости между двумя случайными величинами ξ и η определяется через *коэффициент корреляции*:

$$R(\xi,\eta) = \frac{E([\xi - m_1(\xi)][\eta - m_1(\eta)])}{\sqrt{D_\xi D_\eta}}, \qquad (1.1)$$

где $E(\cdot)$ – символ усреднения.

Выражение в числителе данной формулы называется *ковариацией* двух случайный величин. Нормирование на корень из дисперсии производится для приведения случайных величин к общей размерности. В случае, если число переменных больше двух, используются матрицы ковариации или матрицы корреляции [13]. Если случайные величины независимы, то их коэффициент корреляции равен 0, однако обратное утверждение несправедливо. Выборочный коэффициент корреляции определяется аналогично, но вместо истинных значений моментов используются их выборочные оценки.

Зависимость между значениями реализации случайного процесса в разные моменты времени можно оценить через *автокорреляционную функцию* (АКФ), которая определяется через коэффициент корреляции для отсчетов, взятых в различные моменты времени: $R_x(t_1, t_2)$. *Взаимокорреляционная функция* (ВКФ) $R_{xy}(t_1, t_2)$ позволяет оценить степень зависимости между значениями двух случайных процессов.

Анализ заголовков отдельных пакетов и DPI не всегда применимы, поскольку они могут раскрывать внутреннюю структуру сети или требовать расшифровки передаваемых данных. Из-за требований конфиденциальности, юридических ограничений или высоких затрат сбор данных с конечных узлов может быть невозможен. В таких условиях приемлемым решением остается статистический анализ трафика, в чем и заключается его преимущество [14].

Данные методы находят применение в системах обнаружения вторжений, системах управления качеством обслуживания (QoS), а также при расследовании инцидентов информационной безопасности в SIEM-системах.

1.2. Различные представления трафика

1.2.1. Случайный временной ряд

Существуют различные способы представления сетевого трафика как последовательности пакетов в пригодной для дальнейшего анализа форме. Наиболее простой способ заключается в оценке количества пакетов, поступивших на вход обрабатывающего устройства в последовательные фиксированные интервалы времени. Если отобразить результаты этих измерений на графике, где по оси абсцисс отложены временные интервалы, а по оси ординат объем трафика, то полученная зависимость образует случайный *временной ряд* – последовательность упорядоченных во времени числовых показателей, характеризующих состояние наблюдаемого явления [5, 15]. Временной ряд может представлять не только объем, но и другие параметры трафика или обрабатывающих устройств, например, количество активных сеансов или текущую загрузку памяти и процессора [16, 17].

На Рисунке 1.1 представлен пример временного ряда, построенного по записи сетевого трафика из датасета CIC-IDS2017.

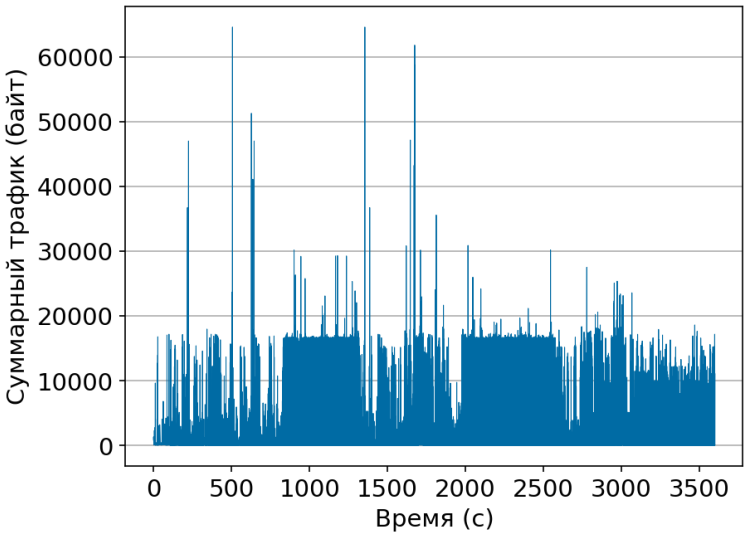


Рисунок 1.1 – Случайный временной ряд

К основным характеристикам временных рядов относятся *сезонность* (периодические колебания значений), *тренд* (долгосрочная составляющая, отражающая общую направленность изменения данных) и стационарность. Остаточные изменения не имеют устойчивых тенденций и обусловлены случайной компонентой ряда.

При рассмотрении трафика в виде случайного временного ряда позволяет выделить следующие представления трафика:

Количество пакетов, поступивших на вход обрабатывающего устройства за интервал времени t:

$$N = \{N_1, N_2, N_3, \dots, N_T\} = \{N_t\}_{t \le T}, \quad N_t \ge 0. \tag{1.2}$$

Объем трафика (суммарный размер пакетов) за интервал времени t:

$$V = \{V_1, V_2, V_3, \dots, V_T\} = \{V_t\}_{t \le T}, \quad V_t \ge 0. \tag{1.3}$$

1.2.2. Случайный поток событий

Сетевой трафик, как правило, описывается целочисленным случайным процессом, представляющим собой число событий, таких как поступление пакетов, кадров или байтов. В то же время, ключевые результаты теории массового обслуживания, широко применяемой для анализа телетрафика и проектирования сетей связи, получены на основе анализа последовательностей интервалов времени между событиями [18]. Это делает

принципиально важным рассмотрение трафика в виде потока событий, так как именно статистика интервалов между ними определяет ключевые характеристики производительности сети.

На Рисунке 1.2 представлен пример случайного потока событий, где моменты поступления заявок (пакетов на вход обрабатывающего устройства) обозначены как t, а интервалы между поступлением пакетов как X.

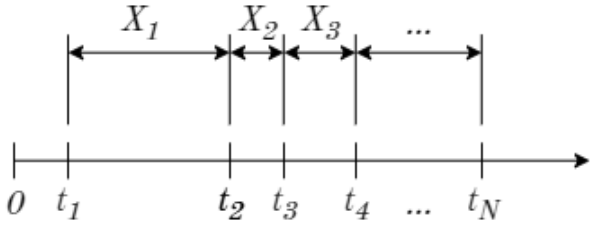


Рисунок 1.2 – Случайный поток событий

Свойства потока событий, соответствующего сетевому трафику [5]:

1. *Нерегулярность* – события на временной оси расположены через нерегулярные (случайные) промежутки времени;

2. *Ординарность* – вероятность появления более одного события в бесконечно малый промежуток времени пренебрежимо мала (в зависимости от разрешения временной шкалы, поток может быть и *неординарным*);

3. *Однородность* – все события считаются одинаковыми и не различаются по своим свойствам (если различать пакеты, например, по приоритетам или по размерам, то такой поток считается *неоднородным*);

4. Если вероятностные свойства потока постоянны во времени, то такой поток называется *стационарным*.

Рассмотрение трафика в виде случайного потока событий позволяет выделить следующие представления трафика:

Последовательность интервалов между событиями:

$$X = \{X_1, X_2, X_3, \dots, X_{N-1}\} = \{X_n\}_{n<N}, \quad X_n > 0. \tag{1.4}$$

Длительность обработки пакетов (или размеры пакетов):

$$Y = \{Y_1, Y_2, Y_3, \dots, Y_N\} = \{Y_n\}_{n\leq N}, \quad Y_n > 0, \tag{1.5}$$

причем $Y_n \leq X_n$.

В реальных сетях получить длительность обработки отдельного пакета обычно не представляются возможным, поскольку стандартные сетевые карты регистрируют только время поступления пакета на сетевой интерфейс, но не время окончания его обработки. Для этого могут применяться специализированные сетевые платы, например производителя *Endace*, но на практике чаще используется значение размера пакета в байтах, поскольку время обслуживания одного пакета обычно прямо пропорционально ему [19].

Последовательность интервалов между моментами поступления пакетов (inter-arrival times, IAT) X и длительностей обработки пакетов (service times) или их размеров Y представляют собой выборки случайных величин ξ и η, для анализа которых применяются стандартные методы теории вероятностей и математической статистики.

Типичные последовательности этих величин для трафика, сгенерированного в результате запроса к поисковой системе и в результате активности ВПО, отличаются, что указывает на их потенциал использования для обнаружения аномалий [14].

Интенсивность реального сетевого трафика может достигать крайне высоких значений, что делает непосредственный анализ трафика в виде потока событий затруднительным. Это связано с необходимостью анализа характеристик отдельных пакетов, что приводит к увеличению объема обрабатываемых данных и, как следствие, к снижению производительности, о чем упоминалось в разделе про анализ потоков трафика.

1.3. Самоподобие трафика

1.3.1. Свойство самоподобия и его причины

В ходе развития сетевых технологий выяснилось, что сетевому трафику присуще свойство *самоподобия* или *фрактальности*, которое заключается в сохранении значений статистических характеристик при рассмотрении процесса в разных временных масштабах [20]. Самоподобный трафик характеризуется наличием долговременных зависимостей (ДВЗ) или

долговременной памяти, что выражается в медленном затухании АКФ при увеличении расстояния (лага) между двумя отсчетами. [21–23]. Поток событий с фрактальным законом поступления сохраняет свои свойства при прохождении системы массового обслуживания (СМО) [24].

Самоподобные процессы, обладающие ДВЗ, характеризуются распределениями вероятности с *тяжелыми хвостами*, что означает, что в выборке могут появляться экстремально большие значения, а математическое ожидание и дисперсия становятся *несуммируемыми*, то есть их выборочные значения очень медленно сходятся к действительному значению или не сходятся вообще. Среди распределений с тяжелыми хвостами наиболее точное описание Интернет-трафика дают законы распределения Парето, Коши, Вейбулла [25, 26].

К числу причин, объясняющих данное явление, обычно относят зависимость интервалов передачи данных от размеров файлов, и пауз от ожиданий действий пользователя, а также наложением трафика от множества источников [27]. И передачи, и паузы, имеют тяжелохвостое распределение, причем для размеров файлов (веб-страниц) характерны более тяжелые хвосты [28].

1.3.2. Показатель Херста

В качестве меры ДВЗ используется *показатель Хёрста* H. Он связан со скоростью затухания АКФ по мере увеличения расстояния между парами значений, а также с фрактальной размерностью D:

$$D = 2 - H. \tag{1.6}$$

Коэффициент Херста может принимать значения от 0 до 1 [5]:

- $H > 0{,}5$ – ряд персистентный с фрактальными свойствами, значения коррелированы и имеют распределение с тяжелыми хвостами;
- $H = 0{,}5$ – значения ряда считаются независимыми величинами без явно выраженной корреляции:

- $H < 0{,}5$ – ряд считается антиперсистентным, то есть любая тенденция к изменению значений стремится смениться противоположной.

Стационарный случайный процесс $X(t)$ с показателем Херста $0{,}5 < H < 1$ считается строго самоподобным второго порядка, если математическое ожидание, дисперсия и АКФ исходного и перемасштабированного с коэффициентом c процесса $c^{-H}X(ct)$ совпадают, и его АКФ имеет вид:

$$R(k) = \frac{\sigma^2}{2}[(k+1)^{2H} - 2k^{2H} + (k+1)^{2H}]. \quad (1.7)$$

Исследуемые на практике реализации случайного процесса обладают конечной длиной, поэтому они могут не обладать в точности требуемой АКФ, и используется следующая аппроксимация:

$$R(k) = k^{(2H-2)}L(t), \quad (1.8)$$

где $L(t)$ – медленно убывающая функция.

АКФ такого типа является несуммируемой, то есть $\sum_k R(k) = \infty$ [5].

Для оценки показателя Херста самоподобного случайного процесса по его реализации применяются различные методы: R/S-анализ (метод нормированного размаха), анализ графика изменения дисперсии, периодограммный метод, метод Виттла, вейвлет-анализ и другие [27, 29]. Для Интернет-трафика типичное значение показателя Херста составляет от 0,65 до 0,8 [20, 30]. Отклонения показателя Херста и фрактальной размерности от ожидаемых значений могут сигнализировать о возникновении аномалии. [31, 32].

1.3.3. АКФ самоподобного трафика

В наблюдаемом трафике корреляция может наблюдаться как между отдельными значениями одной последовательности, так и между значениями разных последовательностей. Между количеством пакетов и общим объемом трафика существует прямая корреляционная зависимость, поскольку суммарный трафик является функцией от числа и размеров пакетов.

Отклонения от этой тенденции указывают на изменение типа передаваемого трафика. Некоторые исследования показывают, что размеры пакетов и интервалы между поступлениями являются статистически независимыми величинами [33].

Несмотря на теоретическую несуммируемость математического ожидания и дисперсии для самоподобного процесса, АКФ реального трафика сходится к конечному значению в некоторых случаях, например для трафика IPTV, IoT и потокового видео [18]. Трафик **BC-pOct89**, который использовался в одном из первых исследований самоподобия Интернет-трафика [20], также обладает конечной АКФ [34].

Таким образом, при анализе самоподобного трафика целесообразно использовать модели, которые воспроизводят не строгое самоподобие, а именно характерное поведение АКФ, то есть её медленное изменение вследствие ДВЗ. При этом важно помнить, что не всякий коррелированный трафик является строго самоподобным.

1.4. Анализ характеристик реального сетевого трафика

1.4.1. Исследование АКФ магистрального трафика

Исследование магистрального трафика транзитного канала связи, записанного в архиве Measurement and Analysis on the WIDE Internet (MAWI) [35] на протяжении 12 лет, показало, что АКФ ежедневного трафика обладает устойчивой формой, сходной с формой АКФ обобщенного процесса Коши [26]. Если АКФ трафика в определенной сети достаточно стабильна, то ее изменение может говорить об изменении параметров сети, возникновении аномалии, вторжении или атаке.

На Рисунке 1.3 представлены графики АКФ для различных представлений трафика из архива MAWI, собранного в течение недели 11-17 октября 2021 года. По оси абсцисс отмечены значения интервалов между отсчетами (лагов) τ, по оси ординат усредненный коэффициент корреляции, полупрозрачные области показывают разброс его значений (СКО).

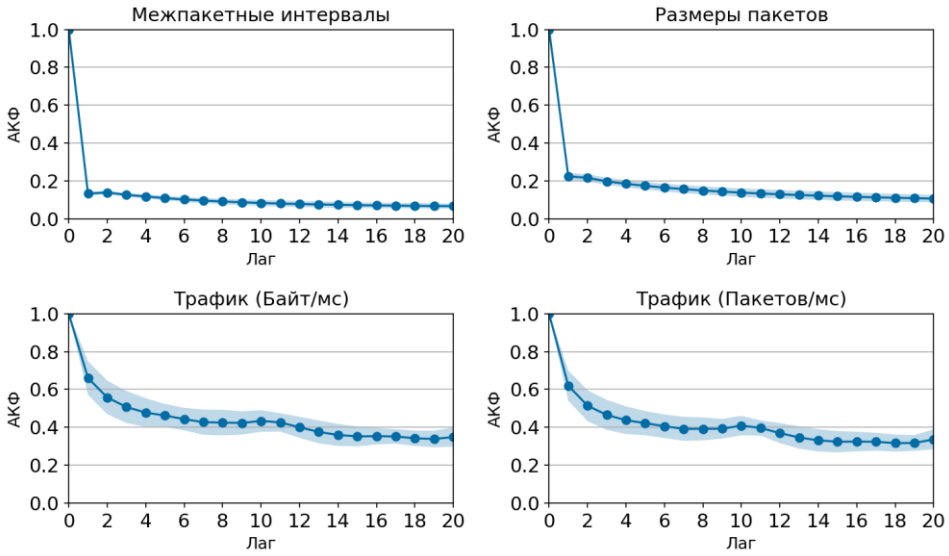


Рисунок 1.3 – Стабильность АКФ в течение недели

По графикам можно видеть, что АКФ трафика действительно сохраняет устойчивую форму, при этом более стабильную АКФ имеют последовательности межпакетных интервалов времени и размеров пакетов, а большие значения АКФ наблюдаются у временных рядов.

1.4.2. Влияние DoS-атак на АКФ и плотность распределения трафика

В работе [8] было проведено моделирование DoS-атак (ICMP-, SYN-, FIN-, RST-flood) в локальной сети, состоящей из двух узлов и маршрутизатора. На одном узле исследовалась интенсивность сетевого трафика, характерного для нормальной активности (просмотр веб-страниц и потокового видео), на другом имитировались действия злоумышленника, направленные на маршрутизатор с целью блокировки доступа во внешнюю сеть. Установлено, что значения среднего, СКО и коэффициентов корреляции интервалов между пакетами снижаются при наличии трафика атаки в окне наблюдения. Аналогичный результат был получен в работе [36]. Это свидетельствует о том, что изменение данных характеристик последовательности интервалов между поступлением пакетов может служить индикатором атаки.

В работе [37] проведено сравнение распределений интервалов между поступлениями пакетов при нормальном режиме работы и при воздействии

DoS-атаки. Гистограмма и подобранная в программе EasyFit плотность вероятности для нормального трафика отображена на Рисунке 1.4.

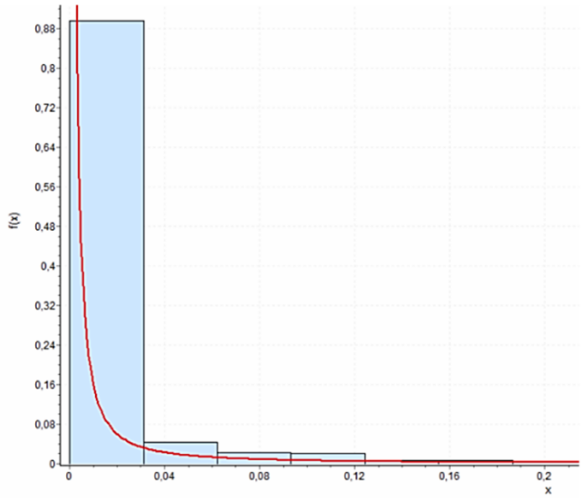


Рисунок 1.4 – Гистограмма и плотность вероятности нормального трафика

По результатам анализа в программе EasyFit, наиболее подходящее по критерию согласия хи-квадрат распределение для данной последовательности – распределение Парето типа II (распределение Ломакса) с плотностью вероятности:

$$f(x) = \frac{\alpha\beta^{\alpha}}{(x+\beta)^{\alpha+1}}, \tag{1.9}$$

где $\alpha = 0{,}436$ – параметр формы, $\beta = 7{,}6 \cdot 10^{-5}$ – параметр масштаба, $\sigma^2 = 0{,}001$ – значение дисперсии.

Плотность вероятности последовательности интервалов между поступлениями пакетов DoS-атаки типа ICMP Flood представлена на Рисунке 1.5.

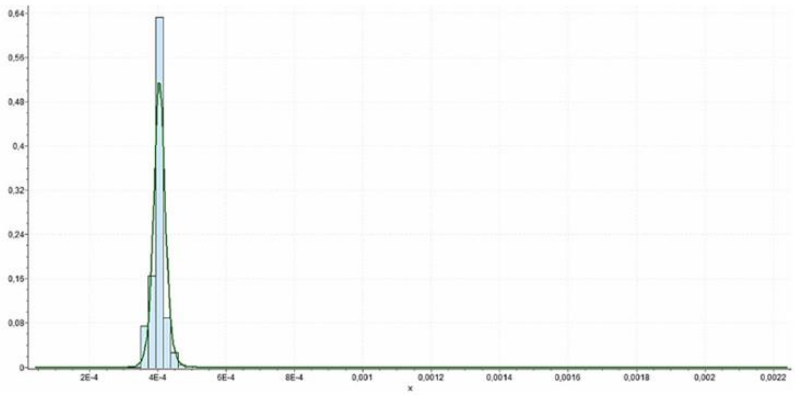


Рисунок 1.5 – Гистограмма и плотность вероятности трафика атаки

Для последовательности интервалов между поступлениями пакетов для атаки ICMP-flood, наиболее подходящим распределением оказывается лог-логистическое с плотностью вероятности:

$$f(x) = \frac{\alpha}{\beta}\left(\frac{x}{\beta}\right)^{\alpha-1}\left(1+\left(\frac{x}{\beta}\right)^{\alpha}\right)^{-2}, \quad (1.10)$$

где $\alpha = 66{,}347$ – параметр формы, $\beta = 7{,}02 \cdot 10^{-4}$ – параметр масштаба, $\sigma^2 = 0{,}0015 \cdot 10^{-6}$ – значение дисперсии.

В работе [19] проведен аналогичный анализ MPEG-4 трафика с IP-камеры на видеосервер, при этом исследовались последовательности интервалов времени между поступлением пакетов и длин пакетов. Для них наиболее подходящими по критерию согласия Колмогорова-Смирнова оказались распределение Парето и Бета-распределение соответственно. В [38] распределение межпакетных интервалов оказалось близко к распределению Вейбулла [25, 26].

Таким образом, сетевой трафик, генерируемый нормальной (легитимной) активностью пользователей, действительно может характеризоваться распределениями с тяжелыми хвостами, а для трафика атаки закон распределения изменяется.

1.4.3. Исследование агрегированных статистических характеристик

Для того, чтобы проверить, как атаки влияют на статистические характеристики трафика, а также чтобы выделить наиболее характерные признаки различных видов атак, необходимы данные реального сетевого трафика. В большинстве исследовательских работ используются разные трассы, полученные в разных точках разных сетей, на разных сценариях, в разные по длительности промежутки времени [7]. Для обеспечения воспроизводимости и достоверности результатов исследования предпочтительнее использовать общедоступные датасеты (наборы данных). При этом для статистических методов анализа не требуется доступ к содержимому пакета, в котором может содержаться конфиденциальная

информация, в чем заключается их преимущество. Одними из наиболее часто используемых наборов данных в научных исследованиях по обнаружению аномалий в сетевом трафике являются: **MAWI** [35, 39, 40], который упоминался ранее, **NSL-KDD** [41–45], **UNSW-NB15** [45–50] и **CIC-IDS2017** [39, 44, 51].

В данной работе используется последний, поскольку он включает в себя не только обработанные данные сетевых потоков с извлеченными признаками, но и «сырые» записи трафика, которые могут использоваться для получения необходимых последовательностей и временных рядов, а также несколько типов различных видов атак, и отдельные записи легитимного трафика, сгенерированного нормальной активностью пользователей (без аномалий) при использовании протоколов HTTP, HTTPS, FTP, SSH и электронной почты [52]. Полный набор данных состоит из пяти записей около 8 часов трафика, собранных в течение одной недели в тестовой сети, где в каждый день кроме понедельника осуществлялась реализация различных видов атак.

В записи нормального трафика, собранного в понедельник, содержится 497 056 сетевых потоков (сгруппированных по 5-tuple), статистические характеристики которых представлены в Таблице 1.1:

Таблица 1.1 – Статистические характеристики потоков трафика

Характеристика	Длина потока	Длительность потока	Суммарный размер пакетов (байт)
Среднее	23,559	0:25:23.017568	20989,779
СКО	3144,393	1:23:38.486465	5741762,270
Минимум	1	0:00:00	60
50 процентиль	6	0:00:00.525376	766
95 процентиль	34	4:02:48.368673	11062
99 процентиль	111	7:15:30.255112	93056
Максимум	1389757	8:05:28.825126	3142960152

Средняя длина потока составляет чуть больше 23 пакетов, 99% всех потоков не превышают 111 пакетов. В работе [53] было проведено исследование потоков трафика университетской сети с использованием протокола NetFlow. Было установлено, что типичный трафик

преимущественно состоит из пакетов TCP и UDP, при этом средняя длина потока составила 122, 29 и 79 пакетов, а средний размер – 923, 631 и 871 байт соответственно для TCP, UDP и для всего трафика в целом.

Эти результаты достаточно близки к полученным при анализе данных CIC-IDS2017. Большинство сетевых потоков имеют слишком малую длину для выделения достоверных статистических характеристик. Состав трафика также близок к полученным в работе данным. В Таблице 1.2 представлено его распределение по сетевым протоколам:

Таблица 1.2 – Распределение сетевых потоков по протоколам

Протокол	Всего пакетов	Всего пакетов (%)
TCP	10718469	91,53
UDP	934702	7,98
ICMP6	1651	0,01
ICMP	671	0,01
IGMP	53	<0,01
Другие	54425	0,46

Другим вариантом агрегации сетевого трафика является разбиение общего потока данных на временные окна фиксированной длины. В Таблице 1.3 представлены статистические характеристики интервалов, полученных при разбиении трафика на неперекрывающиеся окна длительностью 1 с, всего было получено 28 940 таких окон (≈8,04 ч.):

Таблица 1.3 – Статистические характеристики интервалов трафика

Характеристика	Число пакетов	Суммарный размер пакетов (байт)
Среднее	404,629	360507,795
СКО	975,820	1270346,659
Минимум	1	60
50 процентиль	93	14972
95 процентиль	1975	1821905
99 процентиль	4850	6263946
Максимум	9773	12306737

В данном варианте разбиения трафика среднее число пакетов в 20 раз выше, 95% окон включают 1975 или более пакетов, что позволяет получить более достоверные оценки статистических характеристик.

На Рисунке 1.6 показаны средние значения различных представлений трафика в течение каждого дня. Для получения значений временного ряда

трафик агрегировался с интервалом 1 мс. Разброс значений вокруг среднего обозначен полупрозрачной заливкой. Пунктирной линией обозначено значение той же последовательности в понедельник. Временные интервалы, в которые осуществлялись атаки, выделены соответствующими цветами.

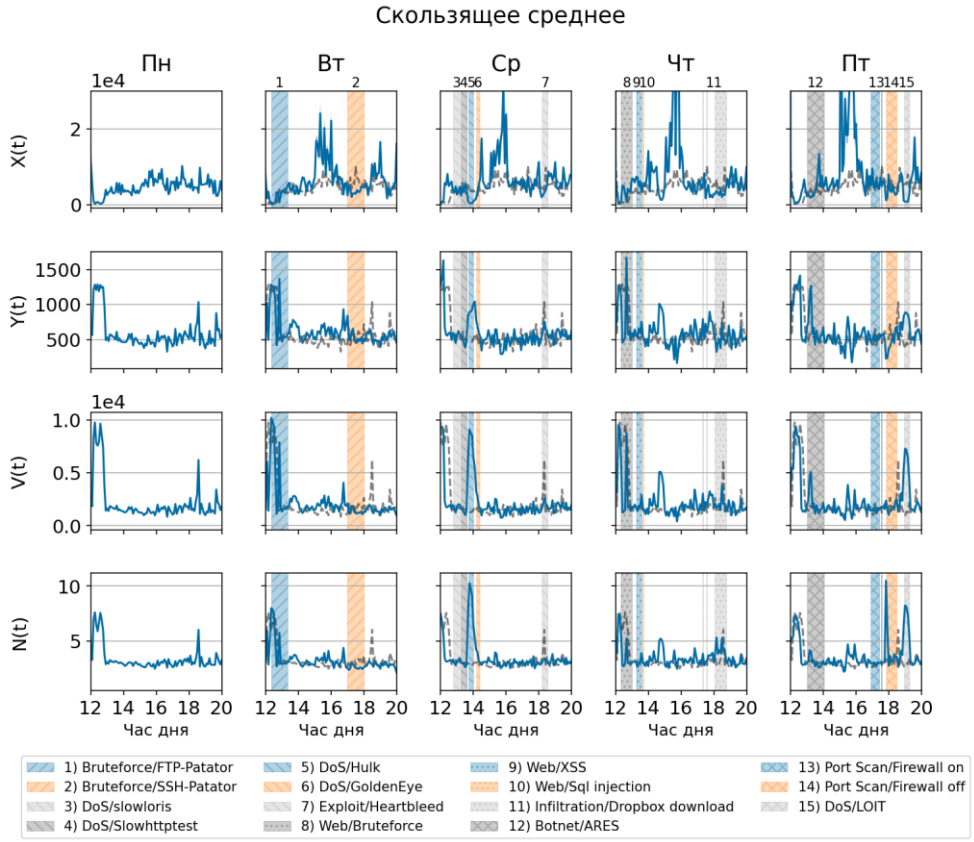


Рисунок 1.6 – Среднее и СКО последовательностей трафика

По графикам можно видеть, что в середине дня значения интервалов между пакетами увеличиваются, что служит косвенным индикатором снижения пользовательской активности. Пик в течение первого часа вероятно связан с инициализацией сети.

Наиболее существенное влияние на значения последовательностей оказывают DoS-атаки *HULK* (HTTP Unbearable Load King) и *LOIC* (Low Orbit Ion Cannon). Средний интервал между пакетами снижается, а средние размер и количество пакетов – увеличиваются. Атаки типа *slowloris* и *Slowhttptest* нацелены на логическое, а не на физическое исчерпание ресурсов сервера, поэтому при их реализации на графиках не видно заметных изменений. То же относится и к атаке *Heartbleed*, нацеленной на библиотеку OpenSSL,

реализующую шифрование TLS трафика и к атакам на уровень приложений. Атаки методом «грубой силы» на FTP и SSH сервер не отражаются на графиках, что может означать, что при использовании утилиты *Patator*, реализующей атаки, были заданы настройки, маскирующие трафик под действия легитимного пользователя. Активность зараженных устройств, входящих в Python-ботнет *ARES*, отражается на графиках в виде увеличения среднего размера и количества пакетов спустя некоторое время после начала атаки, вероятно, после заражения основной части узлов. При сканировании портов средний размер пакетов значительно уменьшается, а количество увеличивается, что соответствует отправке множества пустых TCP пакетов с разными целевыми портами.

На Рисунке 1.7 показано рассчитанное значение показателя Херста для всех представлений трафика в течение каждого дня. Предварительная проверка показала, что последовательности на большинстве интервалов являются стационарными.

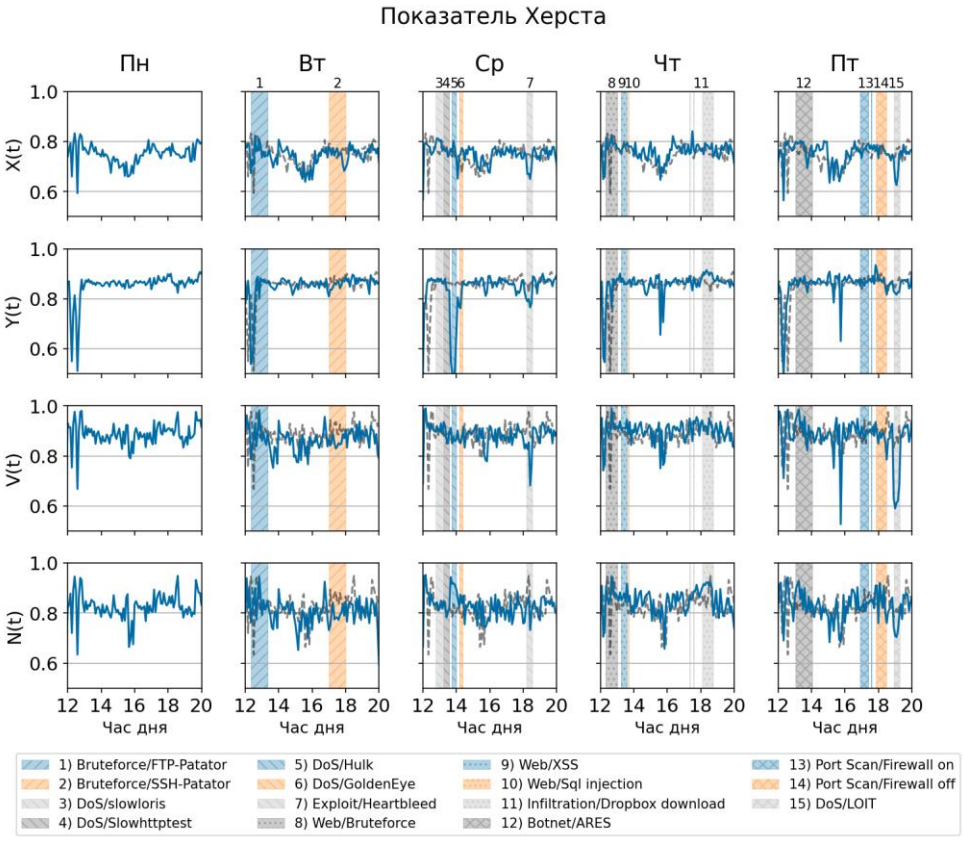


Рисунок 1.7 – Показатель Херста последовательностей трафика

Среднее значение показателя Херста составляет 0,7-0,8 для последовательности интервалов между пакетами и 0,8-0,9 для других представлений, что совпадает с оценками, полученными в работе [19]. В отличие от среднего, для временных рядов показатель Херста возрастает в момент атаки внедрения на этапе скачивания файлов. Для DoS-атак характерно устойчивое снижение показателя Херста, указывающее на усиление хаотичности и потерю корреляционных свойств в трафике, что является типичным признаком сетевой аномалии в том случае, если эти изменения сохраняются на всем интервале наблюдения [32].

Появление периодичности или изменение статистических закономерностей в структуре сетевого трафика могут быть выявлены посредством анализа АКФ. На Рисунке 1.8 представлены коррелограммы для пятиминутных последовательностей легитимного (Benign) трафика и трафика атак. Полупрозрачные области показывают разброс значений (СКО) всех интервалов данного вида трафика.

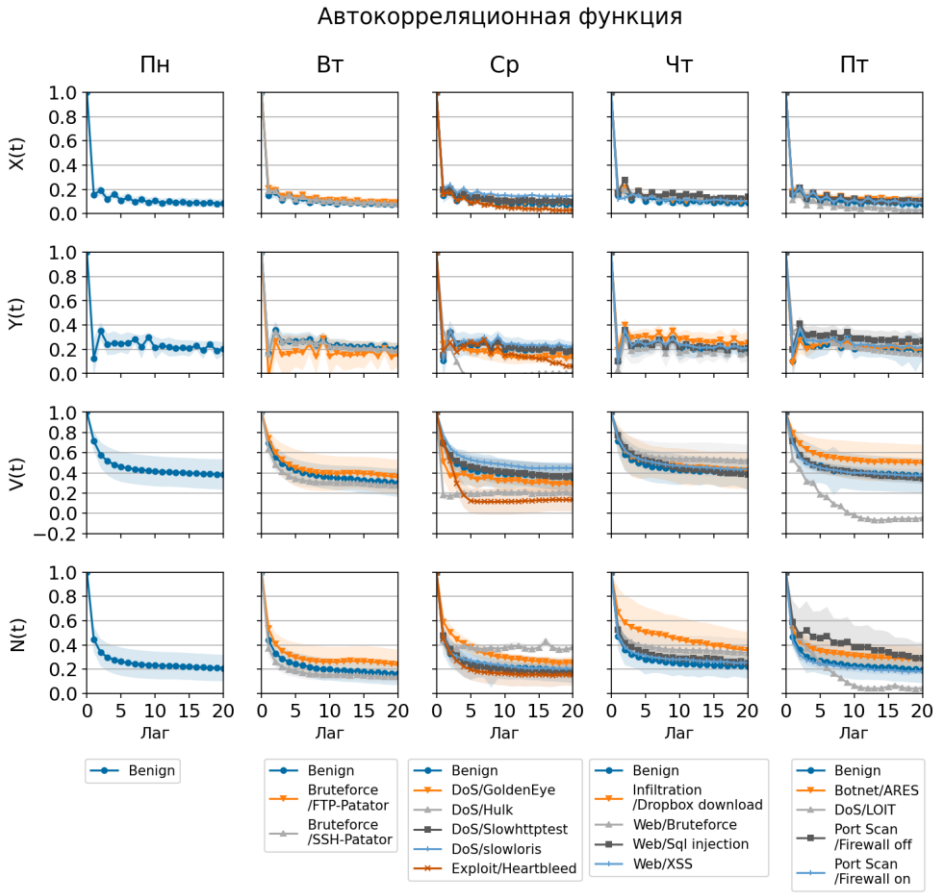


Рисунок 1.8 – АКФ последовательностей трафика

Форма АКФ исследуемого трафика из датасета CIC-IDS2017 практически идентична форме АКФ трафика MAWI (Рисунок 1.3). Это свидетельствует о том, что данные статистические закономерности присущи именно этим типам последовательностей, а не являются особенностью конкретного трафика, что также косвенно подтверждается тем, что в работе [19] были получены близкие значения коэффициентов корреляции для соответствующих последовательностей.

Для последовательности интервалов между поступлениями пакетов АКФ нормального и аномального трафика практически не различаются. Наиболее информативной оказывается АКФ временного ряда, описывающего объем трафика. Её анализ позволяет детектировать не только DoS-атаку HULK, но и DoS-атаку типа *GoldenEye* и эксплойта Heartbleed. Это свидетельствует о том, что анализ АКФ данной последовательности предоставляет более подробные данные о характере сетевой аномалии, потенциально позволяя классифицировать тип воздействия.

1.4.4. Применение методов машинного обучения для анализа трафика

Визуальный анализ графиков является эффективным методом первичного выявления атак и позволяет выделить их наиболее выраженные признаки по характерным изменениям временных рядов [14, 54]. Для более точного выделения признаков и установления пороговых значений перспективным подходом является применение методов машинного обучения.

Для их применения из трафика необходимо извлечь набор признаков, соответствующих каждому объекту (сетевому потоку или временному окну). Далее следует произвести оценку корреляции между признаками, поскольку коррелированные признаки создают избыточность и негативно влияют на точность моделей [55]. Каждому объекту присваивается метка класса (нормальный/аномальный для бинарной классификации или по типу атаки для многоклассовой). Набор объектов разделяется на обучающую и тестовую

выборки. На обучающей выборке происходит тренировка модели, при которой она «запоминает» характерные признаки объектов разных классов, а на тестовой вычисляется качество модели с использованием одной из метрик: *достоверность* (accuracy), *точность* (precision), *полнота* (recall), *F1-мера* (F1-score).

Одним из наиболее популярных алгоритмов, применяемых в машинном обучении, является метод *случайного леса* [56]. Это ансамблевый метод, при котором множество различных решающих деревьев независимо друг от друга обучаются на случайных подвыборках обучающей выборки. В каждом узле дерева происходит сравнение значения признака с пороговым значением, после чего дерево направляет его в один из дочерних узлов, где также происходит сравнение, либо выдается метка класса. Данный принцип можно использовать для выделения численных признаков атак из модели, обученной разделять образцы нормального трафика и трафика конкретного вида атаки [57].

К преимуществам метода случайного леса относится то, что он позволяет работать с несбалансированными наборами данных, назначая «вес» каждому объекту пропорционально доле объектов данного класса в общей выборке, а также вычислительная эффективность. Для построения случайного леса из n деревьев обучающая выборка $S = \{F, C\}$, где F – это вектор признаков, а C – вектор классов, разбивается на подвыборки случайным образом:

$$\{S_i\} = \{S_1, S_2, \dots, S_n\} \in S. \quad (1.11)$$

Выборка, не вошедшая в подмножество S_i называется OOB (out-of-bag) и обозначается как S_{OOB}. При больших размерах обучающей выборки, приблизительно 37% объектов не попадут в S_i и не будут использованы при обучении решающих деревьев. Использование S_{OOB} в качестве тестовой выборки позволяет значительно сократить вычислительную сложность по сравнению с кросс-валидацией, однако полученное при этом значение выбранной метрики может быть завышено [58].

Как было указано ранее, в каждом узле j дерева i данные разбиваются на две ветки. Это происходит путем сравнения значения признака $F_{i,j}$, который проверяется данным узлом, с пороговым значением $\theta_{i,j}$. Для каждого узла можно определить, в какую из двух веток модель чаще направляет аномальные объекты. Пусть $S_{i,j}$ – множество объектов, попавших в узел, тогда доля аномальных объектов:

$$p_{i,j} = \frac{a_{i,j}}{n_{i,j}}, \tag{1.12}$$

где $n_{i,j}$ – общее число объектов в $S_{i,j}$, $a_{i,j}$ – число объектов в $S_{i,j}$, принадлежащих к аномальному классу.

Соответствующий прирост доли аномальных объектов:

$$\Delta p_{i,j} = \max(p_{i,j}^L, p_{i,j}^R) - p_{i,j}, \tag{1.13}$$

где $p_{i,j}^L$ – доля аномалий в левом дочернем узле, $p_{i,j}^R$ – доля аномалий в правом дочернем узле.

Если $\Delta p_{i,j} > 0$, то определяется условие, соответствующее дочернему узлу с большей долей аномалий. Если $p_{i,j}^L > p_{i,j}^R$, то значимым считается условие $C_{i,j}: F_{i,j} \leq \theta_{i,j}$, иначе $C_{i,j}: F_{i,j} > \theta_{i,j}$. Для каждого такого условия сохраняется кортеж параметров $\left(F_{i,j}, \theta_{i,j}, \Delta p_{i,j}, C_{i,j}\right)$.

Поскольку отдельные решающие деревья могут содержать значительную долю шумовых разбиений, необходима агрегация полученных пороговых условий. Параметры группируются по признакам F и типу условия разбиения C и ранжируются по суммарному приросту доли аномальных объектов.

Полученный в результате набор пар $\left(\theta_{i,j}, \Delta p_{i,j}\right)$ можно рассматривать как выборку случайной величины θ с соответствующими весами Δp, поскольку вклад каждого порога отличается. Для оценки плотности распределения этой случайной величины можно применить метод взвешенных гистограмм [59] или ядерной оценки плотности:

$$\hat{f}(x) = \frac{1}{h\sum_{i=1}^{n} w_i} \sum_{i=1}^{n} w_i K\left(\frac{x - x_i}{h}\right), \quad (1.14)$$

где $K(\cdot)$ – ядро (неотрицательная функция, сумма которой должна быть равна 1, например плотность стандартного нормального распределения), h – параметр сглаживания, называемый *шириной полосы*, $w_i = \Delta p_i$ – вес i-го порога из выборки x.

Зная плотность вероятности, можно определить наиболее вероятное значение – *моду* случайной величины, то есть такое значение $x = M$, для которого $f(M) \geq f(x)$. В данном случае мода предпочтительнее выборочного среднего, поскольку она не подвержена влиянию выбросов.

Выборочную моду можно определить по максимуму плотности вероятности:

$$M = \text{argmax}\big(\hat{f}(x)\big), \quad (1.15)$$

где argmax – функция, которая возвращает значение аргумента, при котором функция достигает своего максимального значения.

Таким образом, для каждого признака может быть получено от 0 до 2 наиболее часто используемых порогов разбиения (для каждого типа условия). Для проверки статистической значимости выявленных порогов применяется критерий согласия Колмогорова-Смирнова. Порог считается значимым, если максимум статистики критерия находится в достаточной близости от данного порогового значения, то есть вблизи этой точки наблюдается максимальное различие между функциями распределения признака в нормальном и аномальном трафике.

Если при обучении модели использовалась нормализация признаков относительно математического ожидания и дисперсии, то перед оценкой плотности необходимо восстановить значение порога для соответствия данным:

$$\theta'_{i,j} = \theta_{i,j} \cdot \sigma_F + \mu_F, \quad (1.16)$$

где μ_F – математическое ожидание значения признака F, σ_F – его СКО.

Схема данного алгоритма представлена на Рисунке 1.9:

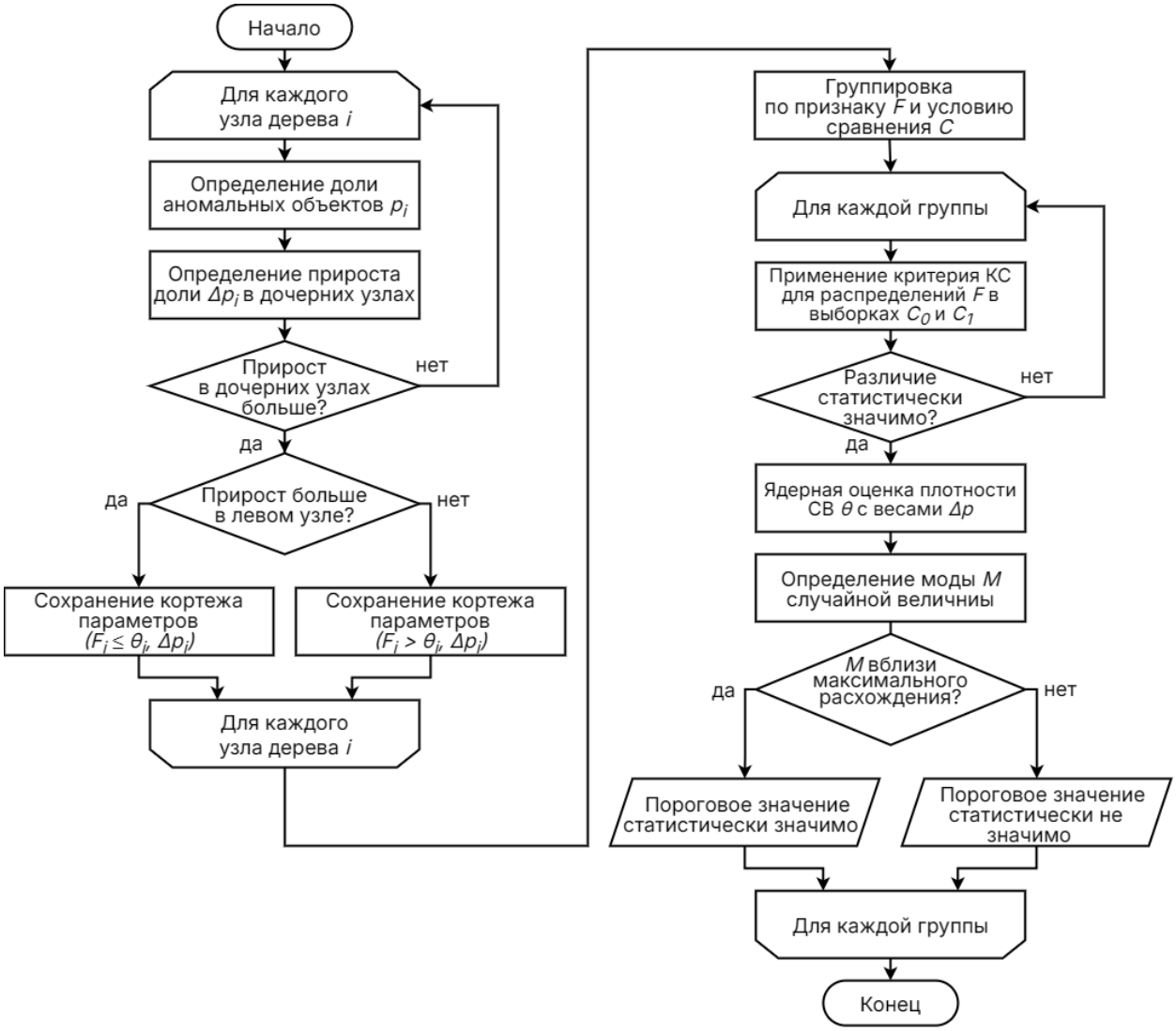


Рисунок 1.9 – Алгоритм выделения пороговых значений

Хотя в процессе признаки и ранжируются по суммарному приросту доли аномальных объектов, что можно рассматривать как важность признака, в отличие от методов отбора признаков, данный алгоритм решает задачу извлечения именно численных индикаторов атак, то есть пороговых значений, при превышении которых трафик можно классифицировать, как принадлежащий определенному виду атак.

Для метода случайного леса важность значимость признаков обычно определяется по показателю важности Джини. В отличие от него, разработанный алгоритм концентрируется на аномалиях, а не на суммарном уменьшении энтропии. Для признаков с большим диапазоном значений важность Джини дает завышенные значения, в то время как здесь будет

получено всего одно (или два) пороговых значения для каждого признака. Коррелированные признаки являются проблемой для обоих подходов. Важность после перестановок (permutation importance) является универсальным методом, который может применяться для любой модели, но требует переобучения и правильного выбора целевой метрики. Разработанный алгоритм может лучше справляться с признаками, для которых аномалии сосредоточены в узком диапазоне значений.

1.4.5. Влияние различных видов атак на характеристики трафика

Разработанный алгоритм выделения численных признаков был применен к трафику CIC-IDS2017. Объектами классификации являются неперекрывающиеся минутные интервалы трафика, поскольку длительность самой короткой атаки в датасете (SQL injection) равна 2 минутам. Первый и последний интервал в каждый день был отброшен. Каждому интервалу присваивается метка класса, в зависимости от того, какая атака проводилась в данный момент. Полученный набор данных является несбалансированным: он содержит 1975 «нормальных» меток и от 20 до 120 аномальных меток для каждого вида атак.

Для каждого интервала были вычислены значения последовательности интервалов между пакетами, размеров пакетов, временных рядов в виде количества пакетов и объема трафика. Для этих представлений были вычислены признаки, соответствующие статистическим характеристикам: среднему, СКО, медиане, сумме, коэффициентам асимметрии и эксцесса, оценка показателя Херста, а также разница между значением каждого из этих признаков по сравнению с предыдущим интервалом и коэффициенты корреляции последовательности для первых 10 лагов.

Значения корреляции между признаками для последовательности интервалов между поступлениями пакетов представлены на Рисунке 1.10.

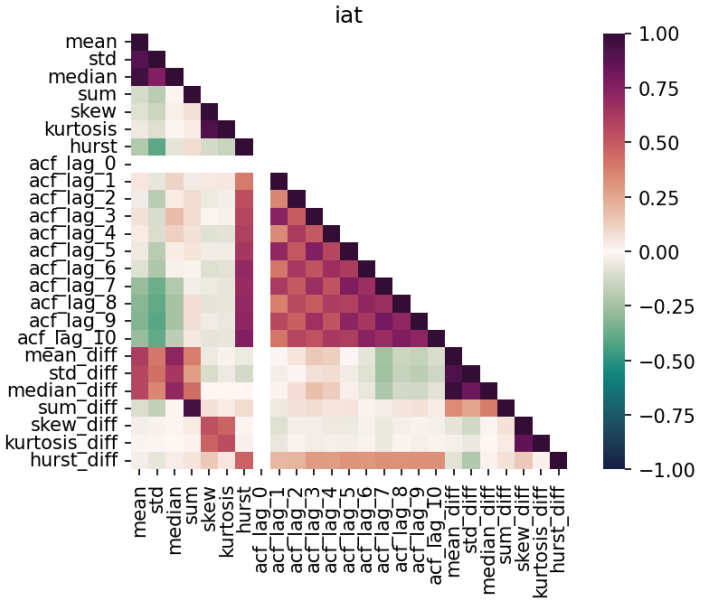


Рисунок 1.10 – Корреляция между признаками

Наиболее сильная корреляция присутствует между средним и СКО последовательности и их разницей с предыдущим интервалом, а также между признаками, соответствующими коэффициентам корреляции. Эти закономерности сохраняются и для других последовательностей.

Для выделения наиболее характерных признаков атак целесообразно рассматривать каждую группу атак отдельно по сравнению с легитимным трафиком: в этом случае наибольший вес должны иметь признаки, отличающие не атаки разных видов друг от друга, а атаки конкретного вида от нормального трафика. Для каждого представления трафика и группы атак обучается своя модель, качество которой оценивается по значению F1-меры для тренировочной и тестовой (OOB) выборок. На тренировочной выборке для большинства моделей полученное значение F1-меры составляет 0,95-1,0, что позволяет их дальнейшее использование. Значения F1-меры на тестовой выборке представлены в Таблице 1.4.

Таблица 1.4 – Значения F1-меры на тестовой выборке

Тип атаки	F1 iat	F1 buf	F1 bytes	F1 packets
Botnet/ARES	0,16	0,33	0,22	0,24
Bruteforce/FTP-Patator	0,30	0,34	0,39	0,35
Bruteforce/SSH-Patator	0,49	0,24	0,35	0,49
DoS/GoldenEye	0,25	**0,67**	0,48	0,12

DoS/Hulk	**0,97**	**1,00**	**0,97**	**0,94**
DoS/LOIT	**0,95**	**0,97**	**0,95**	**0,97**
DoS/Slowhttptest	0,09	0,21	0,03	0,21
DoS/slowloris	0,34	0,08	0,08	0,37
Exploit/Heartbleed	0,40	**0,89**	**0,83**	0,36
Infiltration/Dropbox download	**0,72**	**0,61**	0,16	**0,76**
Port Scan/Firewall off	0,14	0,17	0,10	0,38
Port Scan/Firewall on	0,05	0,07	0,05	0,04
Web/Bruteforce	0,31	0,05	0,07	0,07
Web/Sql injection	0,00	0,00	0,00	0,00
Web/XSS	**0,60**	0,06	0,02	0,04

Значения более 0,5 выделены жирным. Все обученные модели успешно распознают трафик DoS атак Hulk и LOIT, также высокие результаты получены для атак внедрения, эксплойтов, брутфорс-атак и DoS-атаки GoldenEye. Неожиданно высокие результаты (F1-мера равная 0,6) получены для модели, обученной распознавать XSS на основе статистических характеристик последовательности интервалов между поступлением пакетов, что может быть связано с особенностями реализации конкретной атаки.

Далее к обученным моделям был применен разработанный алгоритм. На Рисунке 1.11 представлены оценки плотности распределения пороговых значений для признака, соответствующего коэффициенту корреляции между соседними межпакетными интервалами, полученными из модели, обученной на трафике ботнет-атаки. Вертикальной линией отмечена оценка моды распределения.

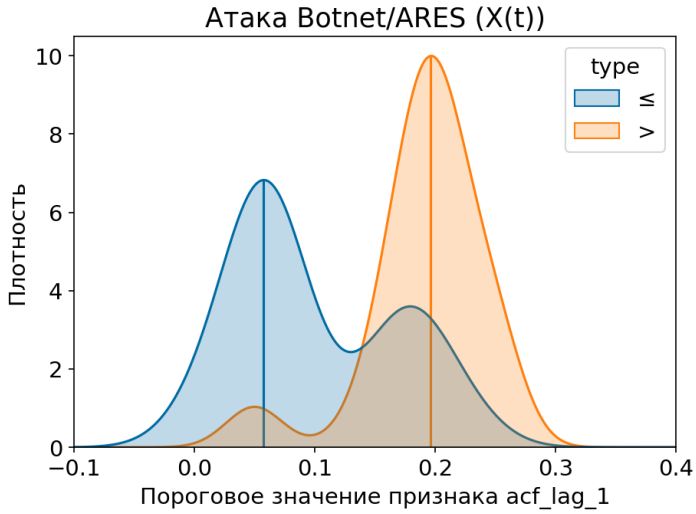


Рисунок 1.11 – Ядерная оценка плотности для коэффициента корреляции

На Рисунке 1.12 представлены эмпирические функции распределения и значение статистики критерия согласия Колмогорова-Смирнова.

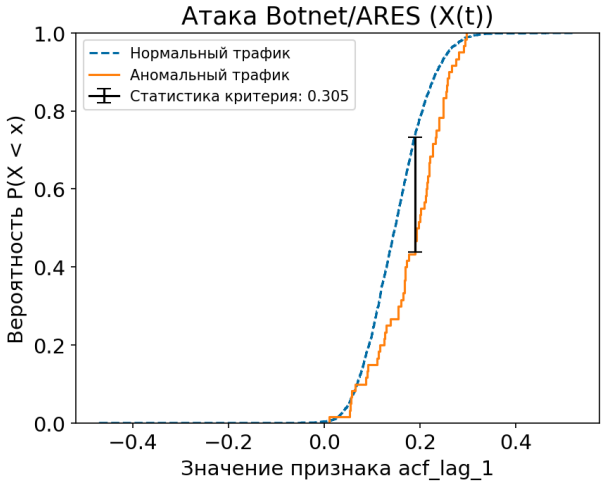


Рисунок 1.12 – Статистика критерия согласия Колмогорова-Смирнова

Наибольшее расхождение между распределениями находится в точке, приблизительно соответствующей значению 0,2. Выделенное пороговое значение также находится в ней, следовательно порог является статистически значимым. Второе пороговое значение, для условия другого типа, находится в точке 0,05, где распределения также отличаются, но гораздо слабее.

Данный алгоритм позволяет выделить численные индикаторы атак:

- **Bruteforce/FTP-Patator**: снижение коэффициентов корреляции ниже 0,3 на лаге 2 и ниже 0,2 на последующих АКФ последовательности размеров пакетов; снижение коэффициентов корреляции ниже 0,1 и изменение распределения, выражающееся в снижении дисперсии, увеличении среднего, «утяжелении» правого хвоста распределения для последовательности интервалов между пакетами.
- **Bruteforce/SSH-Patator**: снижение коэффициентов корреляции ниже 0,2 для последовательности размеров пакетов; увеличение коэффициентов корреляции выше 0,2 на 5 и последующих лагах и сдвиг пика распределения влево значений временного ряда, представляющего количество пакетов в единицу времени.
- **DoS/Hulk**: снижение среднего интервала между пакетами до значений менее 0,5 мс и снижение тяжести хвостов распределения по

сравнению с предыдущим интервалом; превышение среднего размера пакетов значения 8048 байт; увеличение коррелированности значений временного ряда, отражающего количество пакетов в единицу времени, и снижение для временного ряда, отражающего суммарный размер пакетов.

- **Infiltration/Dropbox download**: увеличение коррелированности значений временных рядов и снижение коррелированности интервалов времени между пакетами; превышение показателем Херста значения 0,87 для временного ряда суммарного размера пакетов, 0,9 для последовательности размеров пакетов и 0,8 для интервалов между пакетами.
- **Web/XSS**: снижение коэффициента асимметрии до 6 и увеличение коррелированности для последовательности межпакетных интервалов; увеличение дисперсии размеров пакетов более 881,1.

Данные значения получены для моделей, обученных на данных CIC-IDS2017, поэтому многие пороговые значения специфичны для трафика сети, в которой производилось моделирование, и конкретных инструментов, используемых для проведения атак. Тем не менее, выделенные закономерности совпадают с интуитивным пониманием особенностей атак, а разработанный подход может применяться для трафика других сетей.

У различных видов атак пороги были выделены для признаков, соответствующих значениям АКФ на разных лагах, что говорит о том, что изменение коррелированности может быть использовано для их обнаружения.

Ограничениями данного алгоритма является то, что признаки рассматриваются отдельно и сравниваются только одномерные распределения. Если аномалия проявляется в совместном изменении нескольких признаков, превышения одного из порогов недостаточно. Перспективным может быть использование пар или троек порогов, в том же порядке, в котором они встречаются в решающих деревьях. Также здесь учитывается только один наиболее значимый порог, но, если для признака были выделены два порога θ_1 и θ_2, причем $\theta_1 < \theta_2$, то может быть определен *интервал* аномальных значений, если же $\theta_1 > \theta_2$, то интервал нормальных

значений. Указанные ограничения могут стать предметом дальнейших исследований.

1.5. Выводы по главе 1

Рассмотрены задачи анализа трафика в телекоммуникационных сетях. Введены различные представления сетевого трафика: в виде случайных последовательностей интервалов времени между поступлениями пакетов и их размеров, и в виде случайных временных рядов количества и суммарного размера пакетов, поступивших на вход обрабатывающего устройства за единицу времени.

Проведен статистический анализ различных представлений реального сетевого трафика из архива MAWI. Подтверждено наличие устойчивой медленно затухающей АКФ у различных представлений трафика. Исследовано влияние DoS-атак на АКФ и распределение сетевого трафика, установлено, что атаки приводят к снижению коррелированности и изменению закона распределения интервалов между поступлениями пакетов.

Проведено исследование трафика из датасета CIC-IDS2017. Вычислены значения агрегированных статистических характеристик трафика при разбиении на сетевые потоки и на временные интервалы. Установлено, что длины потоков может быть недостаточно для вычисления достоверных оценок характеристик, и деление трафика на подинтервалы может быть более целесообразным при применении статистических методов анализа.

Установлено влияние различных видов атак на статистические характеристики трафика. Для выделения численных порогов различных признаков атак, рассмотрено применение методов машинного обучения. Разработан алгоритм выделения наиболее информативных пороговых значений для признаков из модели «случайного леса». Показано на рассмотренных данных, что изменение корреляционных свойств последовательности может использоваться для обнаружения аномалий в трафике.

2. Моделирование сетевого трафика с заданными характеристиками

2.1. Задачи моделирования трафика

2.1.1. Моделирование в телекоммуникационных сетях

Моделирование трафика применяется при проектировании и управлении сетями связи, а также для их оптимизации и достижения экономической эффективности. Результаты моделирования позволяют оценить производительность сети, прогнозировать нагрузку, разрабатывать новые технологии и алгоритмы для оптимизации передачи данных.

Одной из основных задач моделирования трафика является планирование ресурсов сети (пропускную способность, количество каналов, частот и т.д.) при проектировании её архитектуры для обслуживания прогнозируемого трафика. При этом используются методы теории массового обслуживания для расчета вероятности блокировки вызова в телефонных сетях или средней задержки, джиттера в сетях передачи данных. Расчет необходимых ресурсов проводится для исключения как перегрузок проектируемой сети, так и избыточных затрат на неиспользуемые мощности.

Другой важной задачей является анализ и прогнозирование паттернов использования сети. Это включает оценку объема и типа передаваемых данных (видео, голос, текст) и временных характеристик передачи. На основе исторических данных создаются модели, позволяющие операторам сети определить, какие ресурсы потребуются для обеспечения качественного обслуживания приоритетных пользователей при различных уровнях нагрузки.

Еще одной задачей моделирования трафика является исследование эффективности различных технологий и стратегий управления трафиком, например, для оценки внедрения новых услуг или технологий. Моделирование позволяет анализировать влияние различных параметров сети на ключевые метрики производительности, такие как пропускная способность, задержки и потери пакетов. Это позволяет обоснованно выбирать оптимальные решения для управления трафиком и повышения эффективности сети, а также снижения риски при внедрении.

2.1.2. Моделирование в задачах обеспечения ИБ

Под моделированием в области информационной безопасности (ИБ) чаще всего понимается создание модели угроз, разработка которой регламентирована рядом нормативных документов. Модели угроз содержит описание характеристик информационной системы, возможностей злоумышленника, а также возможных уязвимостей, способов их реализации и теоретических последствий [60]. Тем не менее, моделирование потоков данных также находит применение в задачах обеспечения ИБ.

Сетевой трафик имеет определенные статистические характеристики, такие как АКФ и закон распределения различных параметров трафика, на основе которых могут быть созданы модели нормального (легитимного) трафика для сети или отдельного её сегмента. Моделирование сетевого трафика позволяет определить базовые показатели нормального состояния, изучить тенденции использования сети и выявить потенциальные неизвестные угрозы, а также генерировать реалистичные данные для обучения систем защиты и их тестирования, по аналогии с *бутстреппингом* в машинном обучении, то есть генерацией новых данных на основе их распределения в исходном датасете ограниченного размера. Генерация реалистичного легитимного трафика также может быть использована для последующего смешивания с трафиком атаки и создания более реалистичных условий тестирования.

Путем создания различных моделей можно прогнозировать последствия вторжений, тестировать устойчивость инфраструктуры к различным видам воздействий, и оптимизировать конфигурацию средств защиты информации. Моделирование позволяет проводить виртуальные тренировки по реагированию на инциденты.

В отличие от разового технического расчета, моделирование угроз в ИБ это непрерывный процесс. Модель нужно регулярно актуализировать при изменениях в инфраструктуре, внедрении новых услуг или изменении ландшафта киберугроз.

2.2. Методы моделирования интернет-трафика

2.2.1. Методы моделирования самоподобного трафика

Для описания трафика, обладающего свойством самоподобия и фрактальности, за прошедшее с момента обнаружения таких свойств время были созданы различные стохастические модели [61]. Они применяются при анализе производительности различных протоколов, алгоритмов, или топологий сети, для воссоздания приближенных к реальным трасс трафика, при имитационном моделировании в симуляторах или тестовых сетях.

- *Авторегрессионные модели трафика* (AR-, MA-, ARMA-, ARIMA-, FARIMA-модели) определяют следующее значение случайного процесса в виде рекурсивной функции от предыдущих значений.
- *Фрактальное броуновское движение (ФБД)* – это стохастический Винеровский процесс, который позволяет моделировать случайный процесс с заданным коэффициентом Херста.
- *Фрактальный гауссовский шум (ФГШ)* – это последовательность приращений ФБД, которая также обладает свойствами ДВЗ и самоподобия. *Фрактальное движение Леви* представляет собой дальнейшее обобщение ФГШ [61].
- *Мультифрактальные модели трафика* позволяют учитывать присущие телетрафику ДВЗ и мультифрактальное масштабирование независимо друг от друга [61].
- *Модели на основе вейвлетов* позволяют учитывать краткосрочные и долгосрочные зависимости во временных рядах.
- *Пуассоновский процесс, управляемый марковской цепью (Markov Modulated Poisson Process, MMPP)* – это пуассоновский процесс, интенсивность которого зависит от текущего состояния. Длительность пребывания в каждом состоянии распределена по экспоненциальному закону. Интенсивности и длительности меняются в соответствии с матрицей переходов, которая в простейшем случае задает только два состояния (ON и OFF) [62].

- *Модель ON/OFF источников*. В течение ON-периодов происходит передача пакетов определенной длины с постоянной скоростью, в течение OFF-периодов источник не передает данные. Длины ON и OFF периодов задаются парой распределений и могут быть коррелированы. Объединение трафика от множества таких источников позволяет получать самоподобный трафик [63]. Модель ON/OFF позволяет достаточно близко аппроксимировать трафик локальных сетей [64, 65].

- *Процесс всплесков Пуассона-Парето (Poisson Pareto Burst Process, PPBP).* Эта модель основана на генерации серии всплесков сетевой активности, в течение которых данные передаются с постоянной скоростью, а длительности передачи подчиняются распределением Парето. Моменты возникновения всплесков задаются пуассоновским потоком событий. В любой момент времени может существовать произвольное количество источников. Данную модель можно рассматривать как предельный случай объединения большого числа независимых ON/OFF источников с тяжелохвостым распределением интервалов [66].

- *Сетевое исчисление (Network calculus)* позволяет вычислять гарантированные граничные значения характеристик функционирования сетей связи. Трафик моделируется в виде потоков, проходящих через систему, состоящую из элементов, ограничивающих передачу данных, и обусловленных пропускной способностью каналов и механизмами управления доступом. Входящий и исходящий трафик описывается функциями (кривыми) времени, а сетевые узлы – функциями обслуживания. Основу математического аппарата составляет идемпотентная алгебра (min-plus), что позволяет преобразовывать сложные нелинейные сетевые системы в линейные относительно используемых операций.

Для моделирования трафика непосредственно, существуют разнообразные *симуляторы*. Дискретно-событийный симулятор *ns-3* применяется имитационного моделирования сетевых протоколов, *Cisco Packet Tracer* и *Huawei eNSP* предназначены для учебных и

демонстрационных задач, позволяя отрабатывать базовые сценарии конфигурации сети на оборудовании Cisco и Huawei соответственно, *EVE-NG* предназначен для эмуляции сложных корпоративных и операторских сетей с использованием реальных сетевых ОС.

Исследователи также предлагают множество новых моделей: в [23] предложена модель на основе сплайнов, в [67] рассматривается модифицированная α - β ON/OFF модель, которая учитывает короткие всплески интенсивности, в [68] предлагается модель на основе смеси распределений с тяжелыми хвостами. В целом можно сказать, что единого устоявшегося подхода к моделированию реалистичного сетевого трафика на данный момент не сложилось, и анализ самоподобного Интернет-трафика и создание его реалистичной модели представляет интерес в области исследования телекоммуникационных сетей.

2.2.2. Модель процесса всплесков Пуассона-Парето в симуляторе ns-3

В ходе диссертационного исследования было проведено моделирование самоподобного трафика по модели PPBP в сетевом симуляторе ns-3 [69], для этого использовался разработанный сообществом модуль с открытым исходным кодом [70]. Данная модель позволяет непосредственно задать целевое значение показателя Херста через параметр формы распределения Парето α:

$$\alpha = 3 - 2 \cdot H. \qquad (2.1)$$

Для оценки показателя Херста сгенерированного в результате симуляции трафика применялся метод анализа графика изменения дисперсии [61]. Трафик рассматривался в виде последовательности межпакетных интервалов и временного ряда количества пакетов в каждые 10 мс. Для каждого заданного значения показателя Херста было проведено 10 симуляций, по результатам которых проведена его оценка. Усредненные значения оценок показателя Херста представлены на Рисунке 2.1.

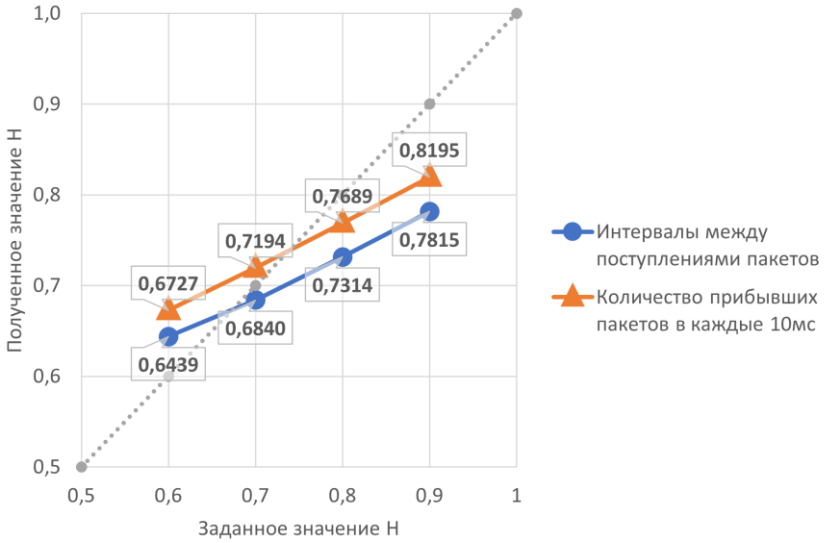


Рисунок 2.1 – Средние значения показателя Херста

Оценочные значения показателя Херста оказались достаточно близки к заданным, из чего можно сделать вывод, что PPBP является подходящей моделью для генерации самоподобного трафика. Для временного ряда оценки являются более точными, чем для последовательности межпакетных интервалов времени. При этом для обоих представлений трафика для более низких значений показателя Херста оценки завышены, а для более высоких – занижены. Данная тенденция также наблюдалась для выбранного *метода* при сравнении различных способов оценки показателя Херста в работе [29] и наиболее вероятно является именно особенностью метода, основанного на графике изменения дисперсии.

2.2.3. Моделирование и обнаружение DoS-атак

Для моделирования трафика с заданными параметрами могут применяться определенные утилиты. В работе [8] для моделирования атак типа SYN-flood, RST-flood, FIN-flood и ICMP-flood в локальной применялась консольная утилита hping3. Было выявлено, что среднее и СКО последовательности интервалов между пакетами значительно уменьшаются, что характерно для такого типа атак. Коэффициенты корреляции трафика, содержащего пакеты DoS-атаки, также значительно отличаются от коэффициентов трафика с нормальной активностью [71, 72].

В работе [73] для моделирования DoS-атаки была использована библиотека Scapy. Записи легитимного трафика и трафика атаки были объединены с использованием утилит **mergecap** и **editcap**, входящих в состав Wireshark. Трафик рассматривался в виде интервалов между пакетами и временного ряда количества пакетов в секунду. Объединенные записи трафика в формате PCAP преобразовывались в формат CSV утилитой **PcapConvert** [74], после чего для последовательностей вычислялась АКФ, для которой оценивалась степень сходства между разными записями.

На Рисунке 2.2 представлены матрицы корреляции между АКФ последовательностей межпакетных интервалов времени. Чем светлее ячейка, тем больше корреляционная связь между АКФ записей трафика, и, следовательно, тем более они схожи. Более темные ячейки обозначают более слабую корреляционную связь.

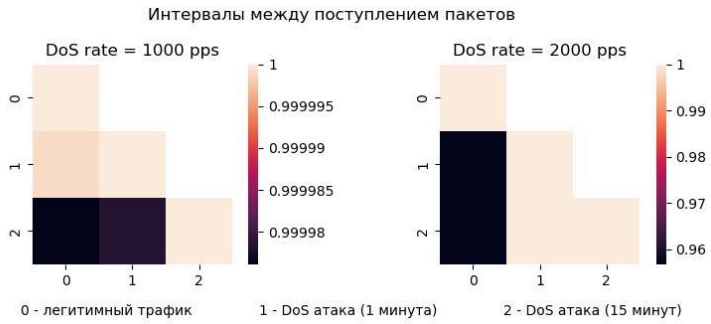


Рисунок 2.2 – Корреляция последовательностей интервалов между пакетами

Графики для временного ряда трафика представлены на Рисунке 2.3.

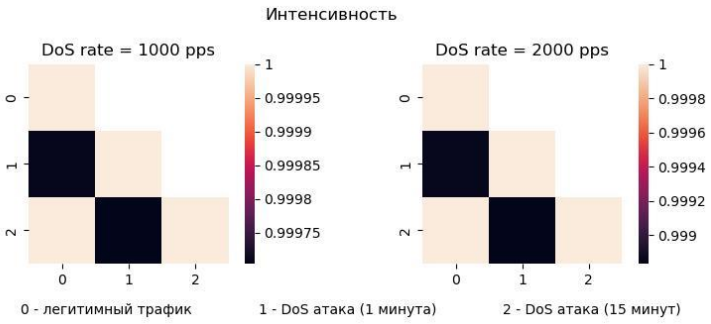


Рисунок 2.3 – Корреляция последовательностей интенсивности трафика

При анализе последовательности межпакетных интервалов, пакеты DoS-атаки «вклиниваются» между пакетами легитимного трафика, что приводит к изменению как самих значений последовательности, так и её

АКФ. Если АКФ данной последовательности для легитимного трафика является достаточно стабильной, то данное изменение может служить сигналом об аномалии. Для временного ряда влияние DoS-атаки проявляется только если она действует лишь на части рассматриваемого интервала. Атака постоянной интенсивности, действующая на всем интервале наблюдения, по сути, является детерминированным процессом с постоянной интенсивностью, а прибавление постоянной составляющей к случайному процессу не меняет его АКФ [75]. Для обнаружения DoS-атак по АКФ значений временного ряда необходимо подбирать размер окна наблюдений.

Для анализа файлов захвата трафика с использованием синтаксиса SQL была разработана программа **PcapStat** [76]. Благодаря поддержке оконных функций и пользовательских расширений, она позволяет выделять и анализировать произвольные статистические характеристики сетевого трафика на основе временных и иных параметров пакетов. Для подсчета числа TCP-пакетов, сгруппированных по значениям флагов заголовка, применяется команда, вывод которой представлен на Рисунке 2.4:

```
$ pcapstat query -f captures/syn_flood.pcap "select
  tcp_parsed_flags,
  count(1) as count,
  avg(packet_length) as avg_bytes
from @file
where type = 'TCP'
group by tcp_parsed_flags
order by count desc"
+------------------+---------+-----------+
| tcp_parsed_flags | count   | avg_bytes |
+------------------+---------+-----------+
| SYN              | 126 658 |   173.921 |
| ACK              |   5 035 |   862.343 |
| ACK|PSH         |   1 227 |   557.119 |
| ACK|FIN         |     145 |    56.276 |
| ACK|SYN         |      78 |    65.692 |
| ACK|PSH|FIN     |      17 |    54.000 |
| RST              |      14 |    60.000 |
+------------------+---------+-----------+
```

Рисунок 2.4 – Запрос количества TCP-пакетов для трафика SYN-flood атаки

DoS-атака типа SYN-flood может быть обнаружена путем сравнения количества SYN-пакетов и ACK-пакетов, для этого вида атак характерно значительное превышение первых над вторыми, а также резкий рост числа уникальных IP-адресов источника, что характерно для IP-спуфинга [77].

2.2.4. Объединение трафика от нескольких источников

Рассмотрение нормального и аномального сетевого трафика по отдельности имеет свои применения, например, для составления профиля нормального поведения или выявления специфических сигнатур атак. Однако в реальных сценариях использования, алгоритм обнаружения аномалий должен работать, когда в сети присутствует смесь нормального и аномального трафика.

Недостаток рассмотренного ранее варианта объединения трафика с использованием утилиты **mergecap** [73] заключается в том, что время прибытия соседних пакетов в объединенном файле может быть одинаковым, что затрудняет анализ последовательности межпакетных интервалов.

Для более реалистичной симуляции объединенного трафика была разработана программа **PcapReplay** [78]. Она предназначена для воспроизведения данных из файлов захвата трафика, аналогично **tcpreplay**, но доступна на ОС Windows. Создание смеси трафика осуществляется последовательным запуском воспроизведения для записей нормального трафика и трафика атаки, и захватом пакетов с этого интерфейса. Недостатком являются временные затраты из-за того, что пакеты отправляются с той же скоростью, что и в исходных файлах.

Реалистичный способ объединения трафика представляет модель на основе виртуальной выходной очереди (VOQ). Это одна из техник, используемых в сетевом оборудовании для смягчения проблемы блокировки начала очереди (head of line blocking) в коммутаторах и маршрутизаторах. По аналогии с ней алгоритм объединения трафика использует дополнительную очередь для поддержания порядка пакетов от каждого источника при их объединении. Если следующие пакеты поступают до завершения передачи предыдущего, они добавляются в очередь и ждут, пока передадутся пакеты, поступившие раньше или имеющие более высокий приоритет [79]. То, как может выглядеть трафик, от двух источников, объединенный по данному алгоритму, представлено на Рисунке 2.5

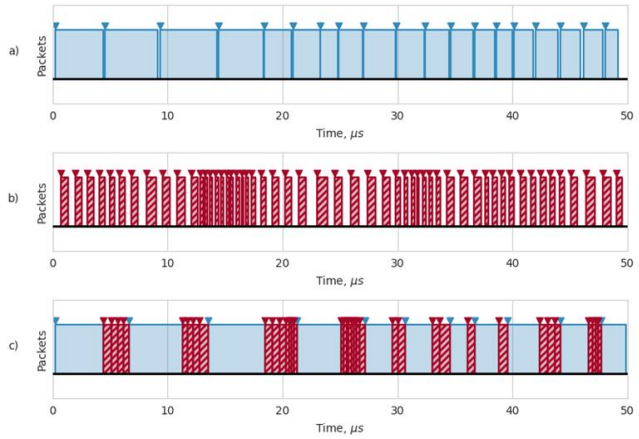


Рисунок 2.5 – Объединение трафика от двух источников

В работе [79] рассмотрено моделирование смеси трафика, сгенерированного по модели ON/OFF источников, где одни узлы являются источниками нормального трафика, а другие – аномального, и трафик объединяется с применением данной модели. Для моделирования последовательности ON и OFF интервалов, обладающей необходимыми статистическими характеристиками, используется алгоритм на основе скользящего среднего и алгоритм рекуррентного моделирования [80].

Для сгенерированных последовательностей значение статистического критерия согласия Колмогорова-Смирнова показывает соответствие эмпирического распределения заданному. Форма АКФ также получается близкой к заданной, что показано на Рисунке 2.6.

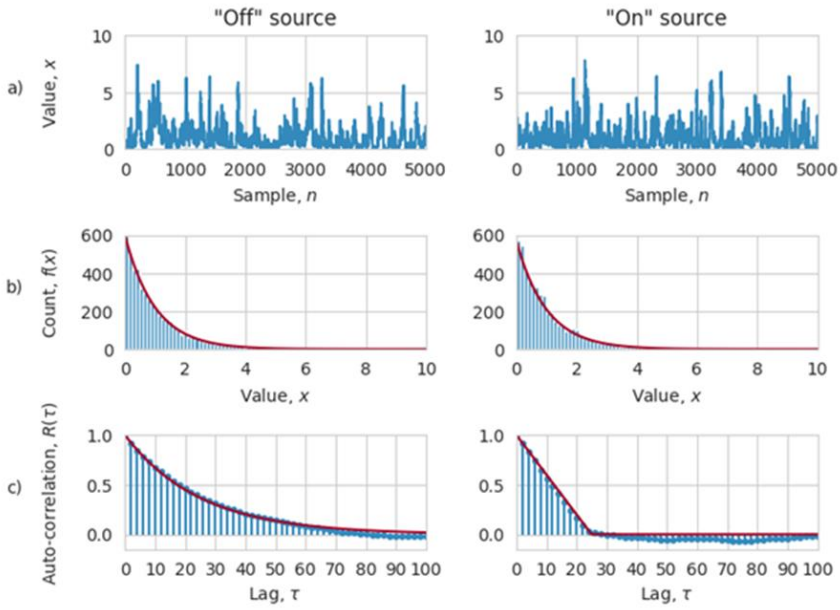


Рисунок 2.6 – Статистические характеристики сгенерированного трафика

Объединенный по модели VOQ трафик разделяется на последовательности «OFF», которая формируется из интервалов между поступлениями пакетов, и «ON», из длительностей передачи пакетов. На Рисунке 2.7 представлена эмпирические гистограммы и кореллограммы для этих последовательностей.

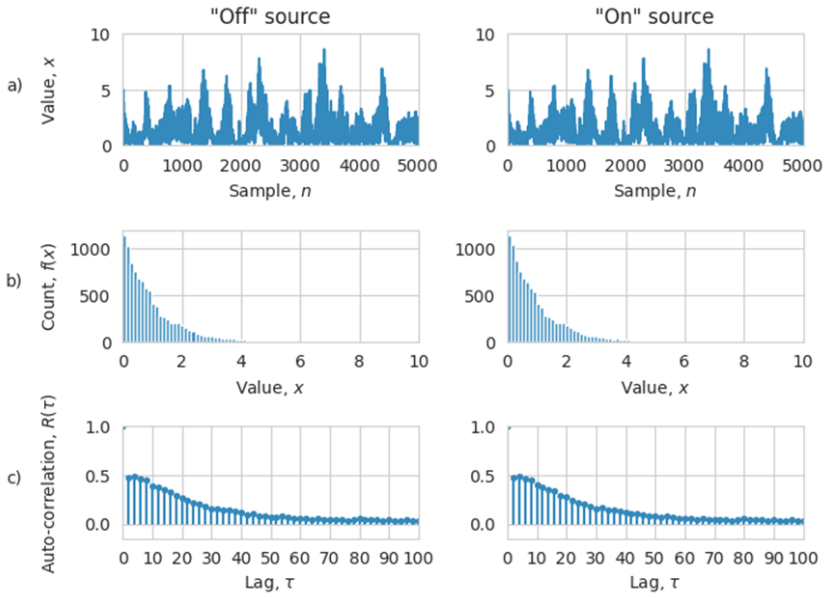


Рисунок 2.7 – Характеристики объединенного трафика

Форма гистограммы близка к распределению исходных последовательностей. АКФ меняется, приобретая более гладкую форму и выражая меньшую корреляцию между близлежащими элементами [81]. Наблюдаемый результат позволяет предположить, что агрегирование нескольких источников случайных последовательностей, которые сами по себе имеют ДВЗ, приводит скорее к потере автокорреляционных свойств результирующей последовательности. Однако, скорее всего, это вызвано тем, что в работе объединялись только два источника с разными характеристиками [79].

Так как в модели ON/OFF скорость, с которой источник генерирует данные (передает пакеты по сети), является отдельным параметром, было изучено его влияние на характеристики моделируемого трафика [82]. Скорость источника задавалась равной 1, 2, 5, 10 и 100 МБ/с, размер пакетов 1500 байт. На Рисунке 2.8 представлен сгенерированный трафик.



Рисунок 2.8 – Трафик ON OFF источников с разными скоростями

Гистограммы и кореллограммы для последовательностей интервалов между пакетами, выделенных их сгенерированного трафика, представлены на Рисунке 2.9.

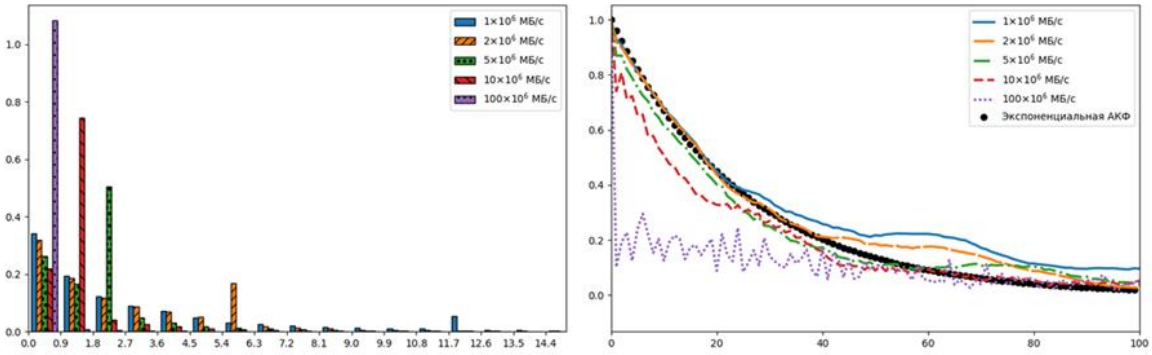


Рисунок 2.9 – Гистограмма и АКФ ON OFF источников

На всех гистограммах наблюдается основной пик в области значений менее 1, а также дополнительный, отличающийся для каждого значения скорости источника, что характерно для смеси распределений. Это может быть обусловлено тем, что межпакетные интервалы включают в себя также и OFF-интервалы источника, обладающие собственными статистическими характеристиками, задаваемыми на начальном этапе моделирования.

АКФ сгенерированного трафика при уменьшении скорости источника приближается к экспоненциальной, которая задавалась при генерации отдельных ON и OFF последовательностей. Это объясняется тем, что при низкой скорости за один ON-интервал источник передает считанные

единицы пакетов, иногда всего один, и тогда длина межпакетного интервала приблизительно совпадает с длиной OFF-интервала, и их статистические характеристики также совпадают. При максимальной скорости последовательность межпакетных интервалов состоит из близких к нулю задержек между пакетами во время ON-интервала и продолжительных OFF-интервалов, такая последовательность не обладает выраженной корреляцией. Расчет коэффициента Херста методом R/S-анализа свидетельствует о том, что трафик также не проявляет свойства самоподобия [82].

2.3. Методы моделирования случайных процессов

2.3.1. Классические методы моделирования случайных процессов

Для моделирования случайных процессов (СП) с заданным законом распределения известны стандартные способы: метод обратного преобразования, перемножение белого гауссовского шума (БГШ) и нижней треугольной матрицы корреляции, полученной через разложение Холецкого, обратное преобразование Фурье модифицированного спектрального представления сигнала, применение формирующего фильтра [80]. Все эти способы позволяют получить реализации либо некоррелированного процесса с заданным распределением, либо процесса с заданной корреляцией и нормальным распределением.

Одновременное воспроизведение и заданного закона распределения и АКФ является более сложной задачей. Известны методы для моделирования различных стационарных и нестационарных СП с распространенными одномерными законами распределения, основанные на нелинейном преобразовании исходного нормального процесса [80]. АКФ исходного процесса R_X и АКФ преобразованного процесса R_Y при этом оказываются связаны зависимостью $R_Y = \varphi(R_X)$. Соответственно, для того, чтобы АКФ преобразованного процесса соответствовала требуемой, необходимо сгенерировать исходный процесс с АКФ $R_X = \varphi^{-1}(R_Y)$, для чего может использоваться способ, включающий в себя разложение по полиномам

Эрмита и численное решение уравнений для нахождения таблицы значений функции φ^{-1} [80].

NORTA (NORmal To Anything) [83] основан на методе обратного преобразования. Основная задача метода состоит в нахождении корреляции R_X, приводящей к корреляции R_Y у преобразованного процесса [84]:

$$Y = F^{-1}[\Phi(X)], \tag{2.2}$$

где $\Phi(\cdot)$ – функция нормального распределения, $F(\cdot)$ – требуемая функция распределения.

Поскольку описанные выше методы включают шаги, использующие численные методы, получаемый результат имеет определенную погрешность. В работе [85] приводится точный способ генерации СП с произвольным законом распределения и АКФ, включая самоподобные процессы, основанный на применении *циркулянтных матриц* корреляции. Использование циркулянтных матриц связано с тем, что собственные значения обычной корреляционной матрицы и её циркулянтного аналога асимптотически сходятся, благодаря чему циркулянтная матрица может служить аппроксимацией исходной корреляционной матрицы [86].

Синтез негауссовых СП в этом методе основан на том же преобразовании, что в методе NORTA и нахождении соответствующей преобразованию исходной АКФ. Преобразование для распределения Вейбулла имеет вид:

$$Y = \left[q \left(\frac{X_1^2 + X_2^2}{2} \right) \right]^{\frac{1}{p}}, \tag{2.3}$$

где X_1, X_2 – реализации нормального СП с корреляцией R_X, p – параметр формы распределения, q – параметр масштаба.

Для экспоненциального распределения связь между АКФ выражается как $R_X = \sqrt{R_Y}$ [85]. Для распределения Вейбулла такая связь определяется через выражение, включающее гипергеометрическую функцию или

бесконечный ряд [87], поэтому вывод обратного выражения для него невозможен аналитически без применения численных методов.

В работе [88] предложен общий подход к моделированию процессов с заданным распределением и АКФ через стохастические дифференциальные уравнения (СДУ) с линейным сносом и нелинейной диффузией. Для приближенного решения и построения рекуррентного алгоритма используется численный метод Эйлера-Маруямы, что может приводить к накоплению ошибки при генерации длинных реализаций, а для процессов с ДВЗ требуется генерация и суммирование нескольких процессов, что увеличивает вычислительные затраты.

2.3.2. Способ выражения взаимосвязи АКФ на основе копулы

Классические методы, основанные на преобразовании нормальных процессов, такие как NORTA, требуют численного решения нелинейных уравнений для выражения связи АКФ, что приводит к погрешностям [84, 85]. Данную проблему возможно устранить, выразив взаимосвязь между АКФ исходного и преобразованного процессов аналитически, например, с помощью копулы [89].

Копула – это функция двух или более переменных, определенная на множестве $[0,\ 1]^n$, где n – число переменных, и обладающая определенными свойствами [90]. Совместное распределение двух случайных величин включает в себя информацию о распределении каждой из этих величин и о том, как значение одной величины влияет на значение другой. Согласно теореме Склара, копула позволяет выделить информацию о взаимосвязи случайных величин, при этом не включая информацию о распределении каждой из них, в виде функции от одномерных распределений:

$$F(X_1, X_2) = C\big(F(X_1),\ F(X_2)\big). \tag{2.4}$$

Совместная плотность вероятности двух случайных величин может быть записана через производную (плотность) копулы:

$$f(X_1, X_2) = c\big(F(X_1), F(X_2)\big) \cdot f(X_1) \cdot f(X_2), \tag{2.5}$$

где $f(\cdot)$ – плотность вероятности, $c(u,v) = \frac{\partial^2 C(u,v)}{\partial u\, \partial v}$ – производная копулы.

Различные копулы представляют разные виды зависимости между распределениями случайных величин. Копула Фарли-Гумбеля-Моргенштерна (ФГМ) имеет следующий вид:

$$C(u,s) = us + \theta us(1-u)(1-s), \tag{2.6}$$

$$c(u,s) = 1 + \theta(1-2u)(1-2s), \tag{2.7}$$

где θ – параметр копулы, $-1 \le \theta \le 1$.

Полезной особенностью копул семейства ФГМ является то, что они позволяют выразить параметр θ через коэффициент корреляции. Для двумерной нормальной плотности вероятности $\theta = r/\pi$ [90]. Для распределения Вейбулла выражение для параметра θ копулы ФГМ примет следующий вид [91]:

$$\theta = r \cdot \frac{\Gamma\left(1+\frac{2}{p}\right) - \Gamma^2\left(1+\frac{1}{p}\right)}{\Gamma^2\left(1+\frac{1}{p}\right)\left[1-\left(1-2^{-\left(1+\frac{1}{p}\right)}\right)\cdot 2^{\left(1-\frac{1}{p}\right)}\right]} = r \cdot k(p). \tag{2.8}$$

Обратное выражение для нахождения АКФ исходного процесса может быть получено с использованием копулы ФГМ.

Закон распределения Вейбулла:

$$f(z) = \frac{p}{q} \cdot \left(\frac{z}{q}\right)^{p-1} \exp\left[-\left(\frac{z}{q}\right)^{p}\right], \;\; z > 0, \tag{2.9}$$

где $p > 0$ – параметр формы, $q > 0$ – параметр масштаба.

Элементы корреляционной матрицы процесса $Z(t)$ определяются как:

$$r_{ij} = \frac{E\left(z_i, z_j\right) - E(z_i) \cdot E\left(z_j\right)}{\sqrt{D^2(z_i) \cdot D^2\left(z_j\right)}}, \tag{2.10}$$

где $E(z)$ – математическое ожидание, $D^2(z)$ – дисперсия, $E\left(z_i, z_j\right)$ – второй совместный момент случайной величины.

Частными случаями распределения Вейбулла являются экспоненциальное (при $p = 1$) и распределение Рэлея (при $p = 2$, $q = \sqrt{2}\sigma$). Случайную величину с распределением Вейбулла можно получить из

случайной величины с экспоненциальным распределением, если возвести ее в степень $1/p$, или с распределением Рэлея, если возвести её в степень $2/p$, во втором случае параметр масштаба $q = (2\sigma^2)^{1/p}$. С учетом этого преобразование (2.3) можно разделить на два этапа [87]:

$$z = v^{\frac{2}{p}}, \tag{2.11}$$

$$v = \sqrt{x^2 + y^2}, \tag{2.12}$$

тогда параметр масштаба $q = (2\sigma^2)^{\frac{1}{p}}$, а второй совместный момент случайной величины можно выразить следующим образом:

$$E(z_i, z_j) = \iint_{00}^{\infty\infty} v_i^{\frac{2}{p}} \cdot v_j^{\frac{2}{p}} \cdot f(v_i, v_j) dv_i dv_j, \tag{2.13}$$

где $f(v_i, v_j)$ – совместная плотность вероятности случайных величин с законом распределения Рэлея.

Если v_i и v_j не коррелированы, то:

$$f(v_i, v_j) = \frac{v_i v_j}{\sigma^4} \cdot e^{-\frac{v_i^2 + v_j^2}{2\sigma^2}} = \frac{v_i}{\sigma^2} \cdot e^{-\frac{v_i^2}{2\sigma^2}} \cdot \frac{v_j}{\sigma^2} \cdot e^{-\frac{v_j^2}{2\sigma^2}} = f(v_i) \cdot f(v_j). \tag{2.14}$$

В противном случае совместная плотность вероятности может быть выражена через производную копулы (2.5). Функцию вероятности v_i (и аналогично v_j) можно найти как интеграл от плотности $f(v_i)$, который для распределения Рэлея равен:

$$F(v_i) = 1 - e^{-\frac{v_i^2}{2\sigma^2}}. \tag{2.15}$$

Подставляя данную функцию вероятности в выражение плотности копулы ФГМ, и выполняя необходимые преобразования можно найти совместную плотность вероятности:

$$f(v_i, v_j) = \left[1 + \theta\left(4e^{-\frac{v_i^2 + v_j^2}{2\sigma^2}} - 2e^{-\frac{v_i^2}{2\sigma^2}} - 2e^{-\frac{v_j^2}{2\sigma^2}} + 1\right)\right] \frac{v_i v_j}{\sigma^4} \cdot e^{-\frac{v_i^2 + v_j^2}{2\sigma^2}}, \tag{2.16}$$

и подставляя её в (2.13) окончательно получить следующее выражение:

$$E(z_i, z_j) = \frac{1}{\sigma^4} \iint_{00}^{\infty\infty} v_i^{\frac{2}{p}+1} v_j^{\frac{2}{p}+1} \left[1 + \theta\left(4e^{-\frac{v_i^2+v_j^2}{2\sigma^2}} - 2e^{-\frac{v_i^2}{2\sigma^2}} - 2e^{-\frac{v_j^2}{2\sigma^2}} + 1\right)\right] e^{-\frac{v_i^2+v_j^2}{2\sigma^2}} dv_i dv_j. \quad (2.17)$$

Поменяв местами операции интегрирования и суммирования, можно заметить, что для каждого слагаемого интеграл распадается на две части:

$$E(z_i, z_j) = \sum_{k=1}^{5} \frac{a_k}{\sigma^4} \int_0^{\infty} v_i^{\frac{2}{p}+1} e^{-\frac{v_i^2}{b_k\sigma^2}} dv_i \int_0^{\infty} v_j^{\frac{2}{p}+1} e^{-\frac{v_j^2}{c_k\sigma^2}} dv_j, \quad (2.18)$$

где $a = \{1,\ 4\theta,\ -2\theta,\ -2\theta,\ \theta\}$, $b = \{2,\ 1,\ 1,\ 2,\ 2\}$, $c = \{2,\ 1,\ 2,\ 1,\ 2\}$.

Каждый интеграл здесь является табличным (3.326.2 в [92]):

$$\int_0^{\infty} x^m e^{-\beta x^n} dx = \frac{\Gamma(\gamma)}{n\beta^{\gamma}},\ \ \gamma = \frac{m+1}{n}, \quad (2.19)$$

где $m = \frac{2}{p} + 1$, $\beta = \frac{1}{d\sigma^2}$, $n = 2$.

Учитывая это, можно обозначить интеграл как:

$$\phi(d) = \int_0^{\infty} x^{\frac{2}{p}+1} e^{-\frac{x^2}{d\sigma^2}} dx = \frac{\Gamma\left(\frac{1}{p}\right)(d\sigma^2)^{\frac{1}{p}+1}}{2p}, \quad (2.20)$$

и упростить выражение (2.18):

$$E(z_i, z_j) = \sum_{k=1}^{5} \frac{a_k \phi(b_k)\phi(c_k)}{\sigma^4} = \frac{\phi(2)^2 + \theta(2\phi(1) - \phi(2))^2}{\sigma^4}. \quad (2.21)$$

Выполняя необходимые подстановки и преобразования, а также учитывая, что при трансформации из распределения Рэлея $\sigma = \sqrt{q^p/2}$, окончательно получаем следующее выражение для взаимосвязи коэффициента корреляции и параметра копулы θ для случайного процесса с распределением Вейбулла, полученным преобразованием (2.3):

$$r = \frac{\frac{q^2}{p^2}\Gamma\left(\frac{1}{p}\right)^2\left[1 + \theta\left(2^{-\frac{1}{p}} - 1\right)^2\right] - \mu_W^2}{\sigma_W^2}, \quad (2.22)$$

где μ_W – математическое ожидание распределения Вейбулла, σ_W^2 – его дисперсия.

На Рисунке 2.10 представлен график зависимости коэффициента корреляции r от значения θ при различных параметрах формы p для выражений А: $r = \theta/k(p)$ (из (2.8)) и Б: (2.22) при параметре масштаба $q = 1$.

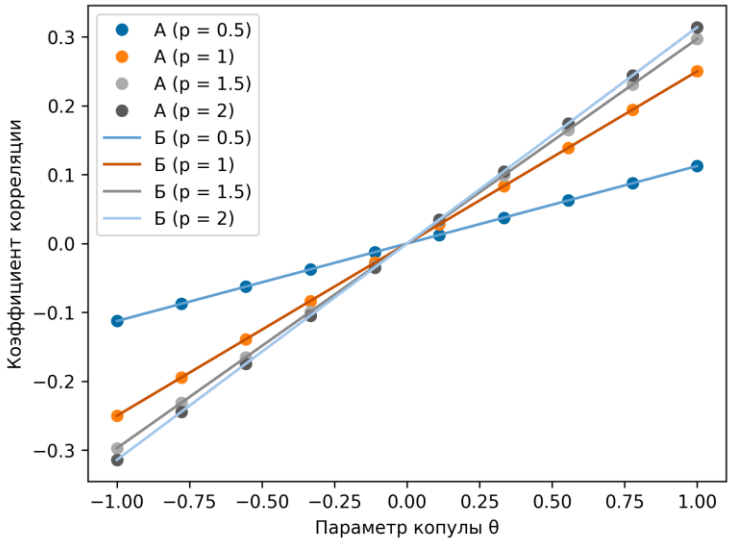


Рисунок 2.10 – Зависимость коэффициента корреляции от параметра копулы

Значения r при одинаковых p совпадают для двух способов, что означает, что параметр копулы не зависит от того, выражается ли корреляция для случайной величины, изначально имеющей распределение Вейбулла, или полученной в ходе преобразования случайной величины с распределением Рэлея.

Случайная величина с распределением Вейбулла также может быть получена путем преобразования случайной величины с экспоненциальным распределением, путем возведения ее в степень $1/p$, так как эти распределения являются частным случаем распределения Вейбулла при $p = 1$ и $p = 2$. В обоих случаях преобразование (2.3) распадается на два этапа. Для того, чтобы вычислить необходимую АКФ нормального случайного процесса на первом этапе R_X, для получения заданной АКФ R_Z у случайного процесса с законом распределения Вейбулла, необходимо применять соответствующие этапам преобразования к R_Z в обратном порядке:

$$R_Y = \varphi_2^{-1}(R_Z), \qquad (2.23)$$

$$R_X = \varphi_1^{-1}(R_Y). \quad (2.24)$$

Для экспоненциального распределения $\varphi_1^{-1}(R_X) = \sqrt{R_Y}$ [85, 87]. Для распределения Рэлея выражение для такой взаимосвязи включает в себя бесконечный ряд, поэтому получить его аналитическое представление невозможно, но в [80] приводится приближенное выражение, полученное при удержании первых двух членов ряда:

$$R_X = \sqrt{\frac{\pi}{4-\pi}\left(\frac{2(R_Y+\mu^2)}{\pi\sigma^2} - 1\right)}. \quad (2.25)$$

Таким образом, параметр копулы используется для выражения связи между требуемыми коэффициентами корреляции преобразованного СП (с распределением Вейбулла), с коэффициентами корреляции исходного СП (с распределением Рэлея или экспоненциальным) на втором этапе преобразования:

$$\varphi_2^{-1}(R_Z) = \frac{\text{rescale}(R_Y \cdot k(n))}{k(p)}, \quad (2.26)$$

где rescale – функция для приведения числа к диапазону $[-1, 1]$ (ограничение параметра θ), $n = 1$ для преобразования из случайной величины с экспоненциальным распределением, $n = 2$ с распределением Рэлея.

2.3.3. Результаты вычислительного эксперимента

Было проведено сравнение различных способов генерации реализаций СП с заданными законом распределения Вейбулла и формой АКФ: способ на основе нелинейного преобразования и разложения двумерной плотности вероятности по полиномам Эрмита [80], NORTA [83], преобразование двух реализаций нормального СП (2.3) [85]. Для последнего использовались различные комбинации преобразований АКФ на двух этапах: без преобразования, через известные соотношения, и через параметр копулы (для

двумерной нормальной плотности вероятности $\theta = r/\pi$ [90]). Рассмотренные варианты преобразований представлены в Таблице 2.1:

Таблица 2.1 – Преобразования АКФ

№	Обозначение на графике	Преобразование φ_2^{-1}	Преобразование φ_1^{-1}
1.	b	См. [80]	-
2.	n	См. [84]	-
3.	w-g 1	$R_Y = k(p)/\theta$ (2.8)	$R_X = \pi R_Y$
4.	w-g 2	$R_Y = R_Z$	$R_X = \sqrt{R_Y}$
5.	w-g 3	$R_Y = R_Z$	(2.25)
6.	w-e-g 1	(2.26), $n = 1$	$R_X = \sqrt{R_Y}$
7.	w-e-g 2	(2.26), $n = 1$	$R_X = \pi R_Y$
8.	w-r-g 1	(2.26), $n = 2$	$R_X = \sqrt{R_Y}$
9.	w-r-g 2	(2.26), $n = 2$	(2.25)
10.	w-r-g 3	(2.26), $n = 2$	$R_X = \pi R_Y$

Всего было сгенерировано по 10 последовательностей из 2^{16} элементов Для каждого сочетания способа, параметра формы $p = \{0.4,\ 0.6,\ 1,\ 1.5,\ 2\}$, и АКФ (экспоненциальной или треугольной), задаваемой соответственно формулами (2.27) и (2.28):

$$R(\tau) = \sigma^2 e^{-\frac{|\tau|}{\tau_0}}, \tag{2.27}$$

$$R(\tau) = \begin{cases} \sigma^2\left(1 - \dfrac{|\tau|}{\tau_0}\right), & |\tau| \le \tau_0 \\ 0, & |\tau| > \tau_0 \end{cases}. \tag{2.28}$$

где $\sigma^2 = 1$ – дисперсия последовательности, $\tau_0 = 1$ – интервал корреляции,

Поскольку копула ФГМ позволяет моделировать только слабую корреляционную связь $|r| < 1/3$ [90] (что также видно и из Рисунка 2.10), также рассматриваются отмасштабированные версии АКФ, где значения коэффициента корреляции для всех лагов, кроме первого, делятся на 3.

Для проверки точности воспроизведения заданной АКФ рассчитывается евклидово расстояние между заданной АКФ и полученной экспериментально, при этом учитывались только первые 64 лага, поскольку полные данные демонстрируют аналогичные тенденции. Полученные расстояния для каждого эксперимента представлены точками на Рисунке 2.11.

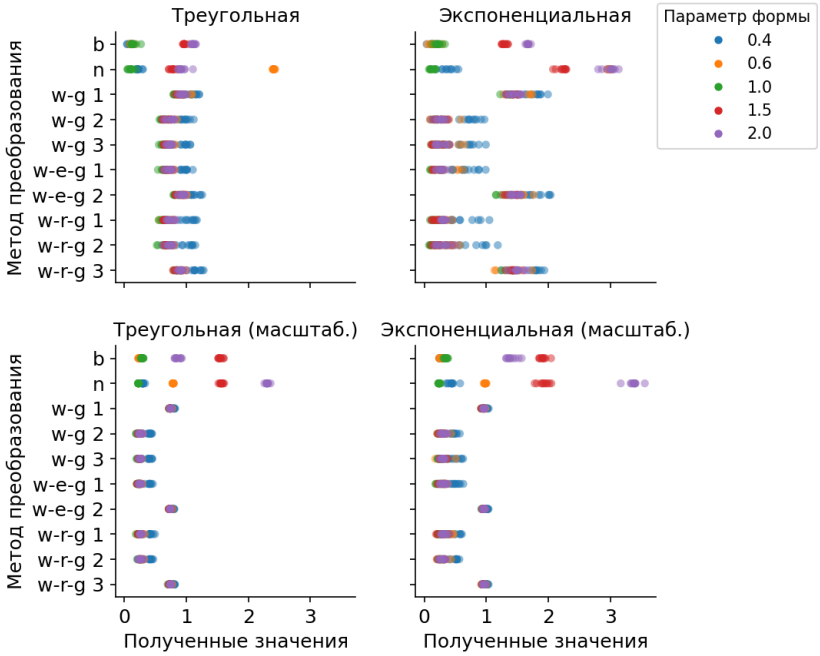


Рисунок 2.11 – Евклидово расстояние от заданной АКФ

Оценка «тяжести» хвостов распределения, которыми распределение Вейбулла должно обладать при $p < 1$, была произведена на основе значений коэффициента эксцесса. Полученные значения представлены на Рисунке 2.12.

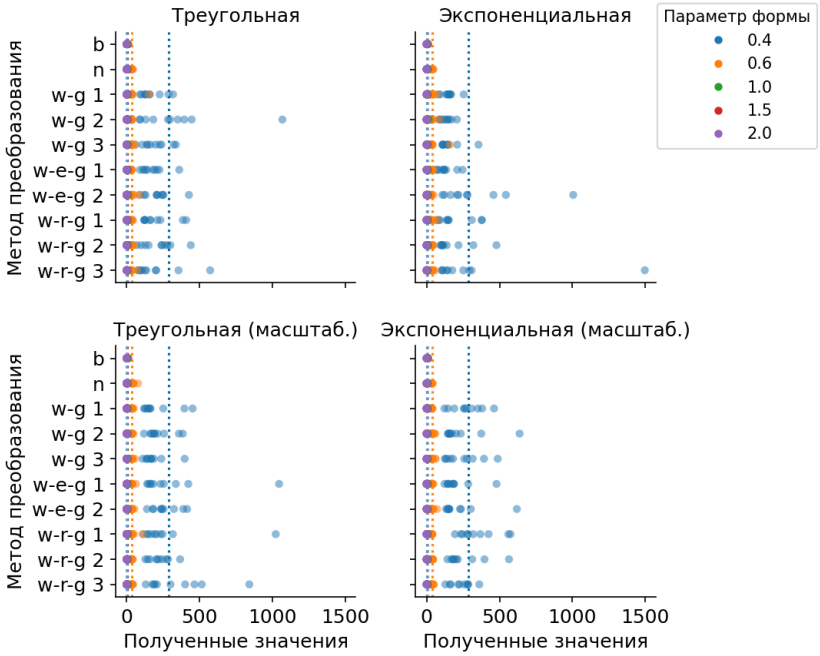


Рисунок 2.12 – Коэффициент эксцесса

Для проверки принадлежности к распределению с заданными параметрами используется статистический критерий согласия Колмогорова-Смирнова с уровнем значимости 95%, то есть при получении p-значения,

большего чем 0,05, нельзя отвергнуть нулевую гипотезу о принадлежности сгенерированной выборки к заданному распределению. Значения статистики критерия представлены на Рисунке 2.13 а p-значения – на Рисунке 2.14.

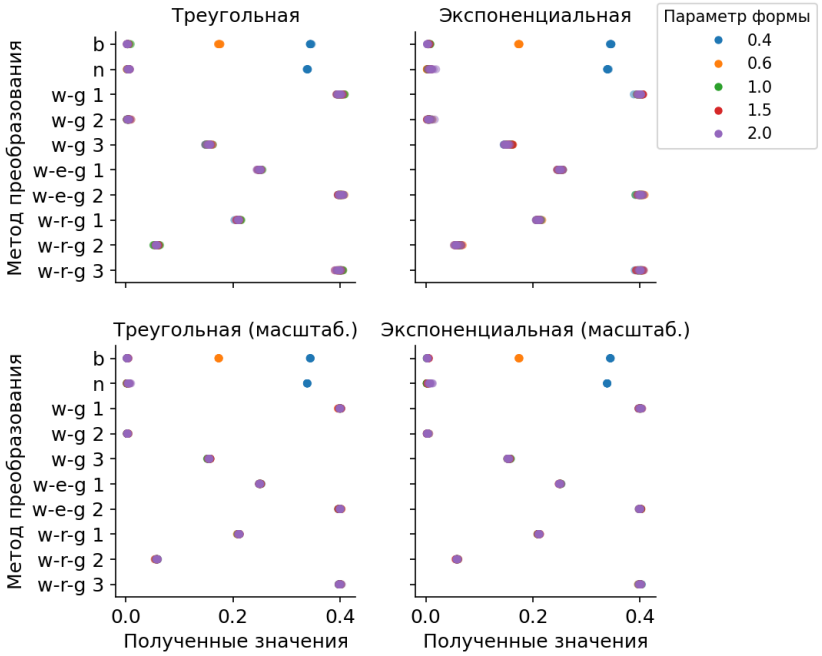


Рисунок 2.13 – Значение статистики критерия Колмогорова-Смирнова

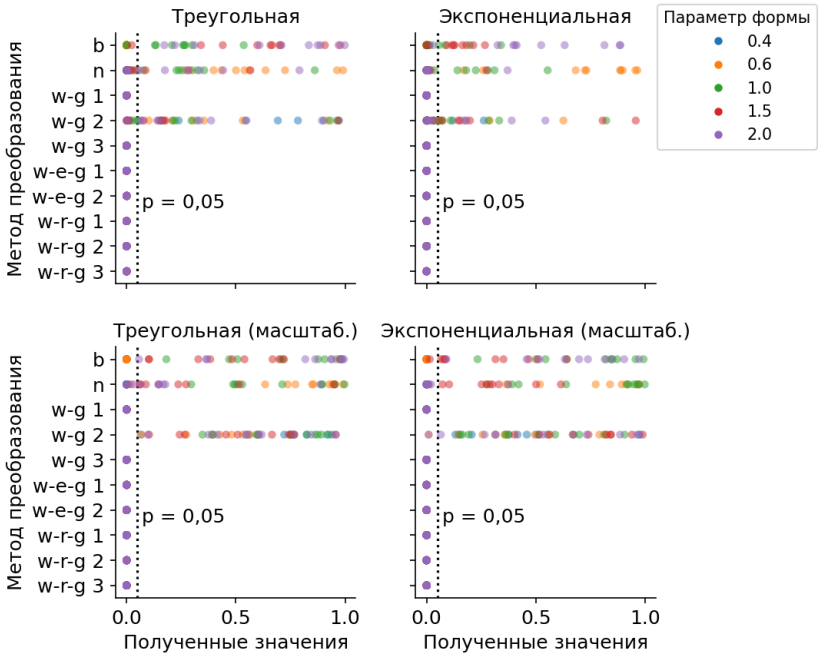


Рисунок 2.14 – p-значение критерия Колмогорова-Смирнова

На Рисунке 2.11 видно, что для способов 1 и 2 близость АКФ к заданной сильно зависит от конкретного значения p, для остальных результаты получаются лучше при масштабировании АКФ, что обусловлено

условием применимости копулы ФГМ. Кроме того, преобразование $R_X = \pi R_Y$ на втором этапе дает худшие результаты по сравнению с другими преобразованиями.

На Рисунке 2.12 можно видеть, что коэффициент эксцесса для всех последовательностей с $p < 1$, сгенерированных способом 1, значительно ниже теоретического значения, для способа 2 ниже только для $p = 0.4$, для остальных коэффициент эксцесса изменяется в широких пределах, что обусловлено ограниченностью выборки. Для отмасштабированной (менее коррелированной) АКФ коэффициент эксцесса ближе к теоретическому значению для распределения.

Рисунок 2.13 подтверждает, что способы 1 и 2 дают худшие результаты при $p < 1$ и $p = 0.6$ (более высокое значение статистики соответствует большему различию между теоретической и эмпирической функциями распределения). Наименьшее значение получается для способов 4 и 9.

На Рисунке 2.14 видно, что p-значение получается больше 0,05 для трех способов: 1 и 2 (для определенных p) и 4, причем если рассматривается отмасштабированная экспоненциальная АКФ, такой результат получается во всех экспериментах для любых p. При этом, хотя для других способов формально нулевая гипотеза должна быть отвергнута, расхождение с теоретической функцией распределения для некоторых способов все еще достаточно мало, что показано на Рисунке 2.15.

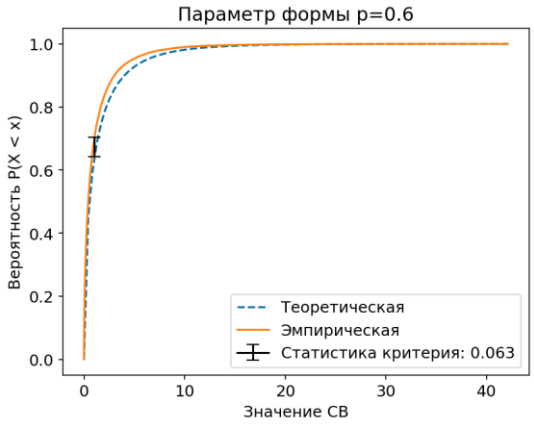


Рисунок 2.15 – Функция распределения для способа 9 при $p = 0.6$

Таким образом, среди всех способов наиболее эффективными оказываются 4 ($R_X = \sqrt{R_Z}$) и 9:

$$R_X = \sqrt{\frac{\pi}{4-\pi}\left(\frac{2[\text{rescale}(R_Z \cdot k(2))/k(p) + \mu^2]}{\pi\sigma^2} - 1\right)}. \qquad (2.29)$$

На Рисунке 2.16 представлены усредненные по всем сгенерированным определенным способом АКФ последовательностей. Предложенный способ обеспечивает более точное воспроизведение АКФ всех видов, кроме треугольной.

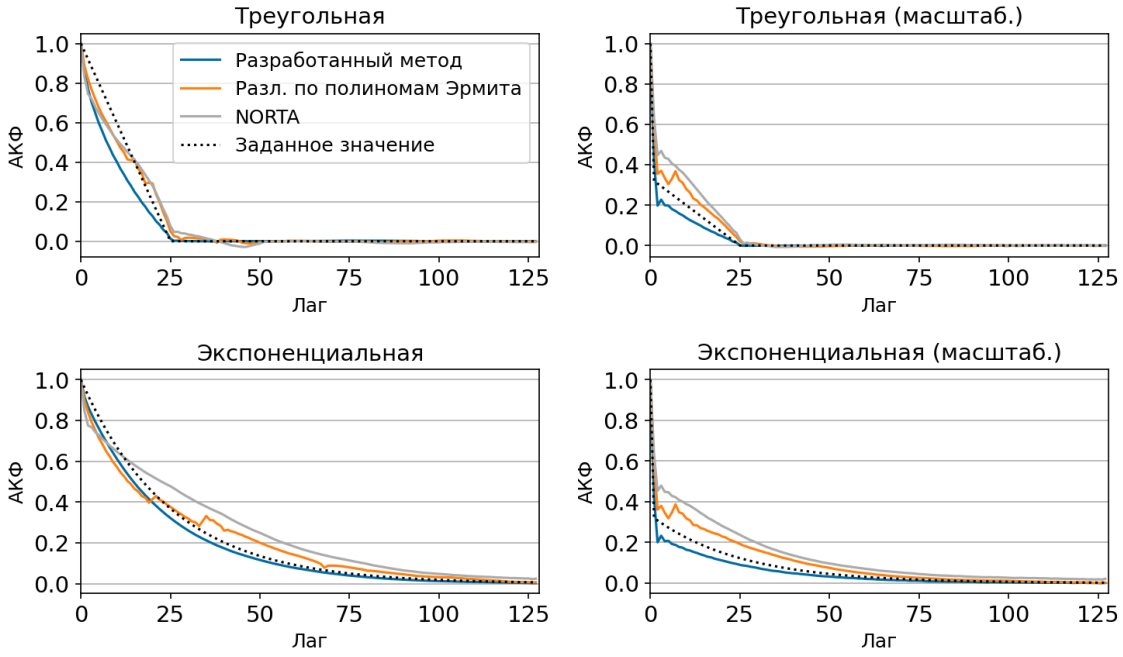


Рисунок 2.16 – Сравнение АКФ

На Рисунке 2.16 представлены усредненные по всем сгенерированным определенным способом эмпирические функции вероятности последовательностей. Предложенный способ превосходит классические методы при моделировании распределения Вейбулла с параметром формы = 0,4 и метод на основе нелинейного преобразования [80] для параметра формы = 0,6. В остальных случаях способ дает достаточно близкие, но не идеальные результаты.

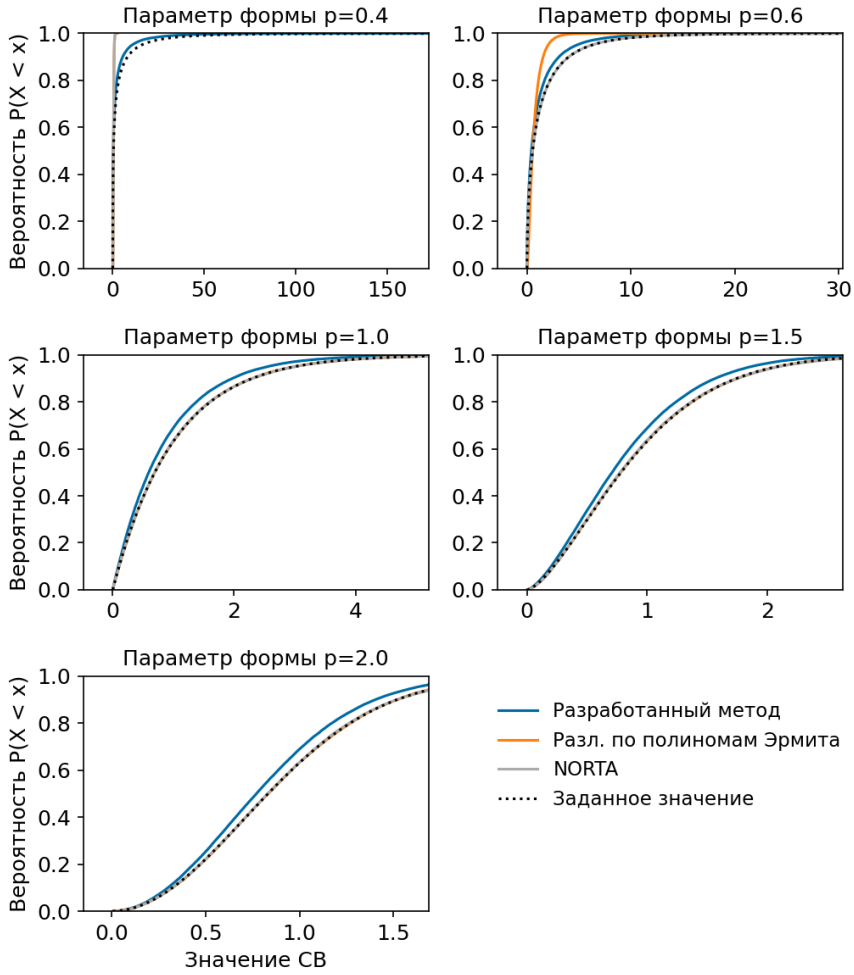


Рисунок 2.17 – Сравнение функций распределения

Предложенный способ на основе копул ФГМ позволяет выразить связь между АКФ исходного и преобразованного процессов аналитически, чем отличается от ранее известных численных методов. Данный подход устраняет необходимость аппроксимации гипергеометрических функций для закона распределения Вейбулла [85] и сокращает вычислительные затраты, так как не требует итерационного подбора R_Z как в методе NORTA [83]. Метод [88] решает задачу в более общем случае, но требует решения СДУ и использует рекуррентные соотношения, что приводит к накоплению ошибки. Способ на основе копул позволяет получить более точное воспроизведение заданной АКФ (евклидово расстояние между теоретической и эмпирической АКФ для первых 64 лагов в среднем меньше на 0,53 или 54,88%) и закона распределения (значение критерия Колмогорова-Смирнова ниже в среднем на 0,03 или 34,33%).

Несмотря на то, что копула ФГМ позволяет выразить только слабую корреляционную связь, разработанный способ позволяет достаточно точно воспроизвести АКФ с $r \geq 1/3$. Другим неожиданным результатом является то, что наилучшие показатели достигаются без преобразования с коэффициентом $k(p)$, когда АКФ нормального процесса определяется как $R_X = \sqrt{R_Z}$, причем не только для $p = 1$ (экспоненциальное распределение), но для других значений параметра формы. В дальнейшем следует рассмотреть преобразование с использованием других видов копул, которые также легко могут быть выражены через коэффициент корреляции.

2.4. Выводы по главе 2

Рассмотрено моделирование трафика в телекоммуникационных сетях и в задачах обеспечения ИБ. Рассмотрены методы моделирования самоподобного интернет-трафика, такие как модель ON/OFF источников и модель Poisson-Pareto Burst Process, которая позволяет достаточно точно генерировать самоподобный трафик с заданным значением показателя Херста. Рассмотрены варианты моделирования DoS-атак и основные признаки их выявления.

Исследованы различные варианты объединения записей трафика, представляющие легитимный трафик и трафик атаки. Проведено моделирование и объединение трафика по модели ON/OFF источников. Описано влияние объединения трафика атаки с легитимным трафиком на статистические характеристики для различных представлений трафика. При рассмотрении трафика как последовательности межпакетных интервалов, атака приводит к изменению корреляционных связей, при рассмотрении трафика в виде количества пакетов в единицу времени DoS-атака постоянной интенсивности не приводит к изменению статистических характеристик в случае, если она присутствует на всем интервале наблюдения. По результатам моделирования при способе объединения трафика от ON/OFF

источников, вероятностное распределение меняется незначительно, а корреляционная связь между интервалами прибытия пакетов уменьшается.

Рассмотрены различные методы моделирования трафика в виде случайного процесса с заданными статистическими характеристиками. Разработан новый метод моделирования случайных процессов с одновременно заданным законом распределения и АКФ на основе копулы – функции двух переменных, показывающей взаимосвязь двух случайных величин, не включающей информацию об их маргинальных распределениях. Проведено моделирование случайных процессов с экспоненциальной и треугольной АКФ, а также заданным законом распределения Вейбулла, который при значении параметра формы меньше единицы обладает «тяжелыми хвостами».

Для проверки точности воспроизведения заданной АКФ рассчитано евклидово расстояние между теоретической и выборочной АКФ. Для проверки принадлежности значений смоделированного процесса к распределению с заданными параметрами использовался статистический критерий согласия Колмогорова-Смирнова. Оценка тяжести хвостов распределения произведена на основе значений коэффициента эксцесса. По результатам моделирования делается вывод о том, что метод на основе копул ФГМ достаточно точно воспроизводит заданные параметры случайного процесса и позволяет выразить связь между АКФ исходного и преобразованного процессов аналитически, чем отличается от ранее известных численных методов.

3. Алгоритмы обнаружения аномалий на основе применения оптимальной линейной фильтрации

3.1. Обнаружение аномалий в компьютерных сетях

3.1.1. Сетевые аномалии

В общем смысле *аномалией* называется такое наблюдение, которое отличается от совокупности остальных наблюдений настолько сильно, что возникает предположение о его происхождении в результате действия иного порождающего механизма, несовместимого с понятием случайности. Аномалии в компьютерных сетях – это неожиданные и значительные отклонения, возникающие из-за различных ситуаций, таких как ошибки программного обеспечения, недобросовестное использование ресурсов, сбои, неправильная настройка и хакерские атаки.

Аномалия представляет собой статистически значимое отклонение характеристик трафика, которое не обязательно является признаком атаки. Аномалии могут быть также вызваны действиями легитимных пользователей или кратковременными сбоями в работе оборудования. В случае действий злоумышленников, аномалии могут быть признаком реализации сразу нескольких угроз. Для алгоритмов обнаружения аномалий важно держать баланс между высокой точностью обнаружений и низким показателем ложных тревог.

Можно выделить следующие типы аномалий [93]: точечные, когда аномальным является только одно наблюдение, контекстуальные, когда наблюдение считается аномальным только если оно произошло при определенных условиях, например, активность на рабочем компьютере корпоративного пользователя вне рабочего времени, и коллективные, когда наблюдения считаются аномальными, только если в эту группу входит достаточно большое число наблюдений.

3.1.2. Системы обнаружения вторжений

СОВ (Система обнаружения вторжений) – это аппаратно-программное средство зашиты информации, предназначенное для выявления фактов несанкционированного доступа к компьютерной системе. СОВ используются для выявления посторонней вредоносной активности. Расширением СОВ являются системы обнаружения и предотвращения вторжений, которые при выявлении вредоносной деятельности предпринимают активные защитные действия, например, вносят IP-адрес источника такой деятельности в список заблокированных межсетевым экраном (МСЭ). Для обнаружения вторжений могут применяться различные подходы [94].

Подход на основе злоупотреблений включает в себя сравнение трафика с заранее определенными сигнатурами, свойственными для того или иного типа атак. Важной частью СОВ, построенной по такому принципу, является своевременной обновление баз известных сигнатур.

Подход на основе обнаружения аномальной активности состоит в создании профиля нормального поведения системы, включающий в себя определенный набор признаков и последующее сравнение текущего состояния системы с этим профилем. Типичные действия, которые человек или компьютерная программа совершает в системе, могут следовать некоторым паттернам, и метод обнаружения аномалий основан на выявлении отклонений от этих паттернов, где отклонения могут быть вызваны разными причинами – от заражения ВПО до проникновения постороннего в помещение в необычное время [39]. Универсальность данного подхода заключается в том, что для него не требуется знание сигнатур всех возможных атак, анализируются лишь отклонения от нормы.

Нейросетевой подход предполагает извлечение набора признаков из трафика, обучение модели на размеченных данных, валидацию модели на тестовых данных и последующее применение модели к трафику по принципу «черного ящика».

3.1.3. Обзор существующих методов обнаружения аномалий

Одним из основных методов обнаружения аномалий во временных рядах является определение точек изменения (Change point detection), то есть моментов времени, в которые статистические характеристики ряда изменяются. К таким методам относятся контрольные карты Шухарта, процедура Ширяева-Робертса, EWMA, CUSUM, Binseg [95]. Самоподобные процессы, к которым относится и сетевой трафик, обладают бесконечным математическим ожиданием и дисперсией, поэтому не все методы на основе этих численных характеристик могут быть применимы к трафику [96]. Другим популярным направлением является моделирование с помощью авторегрессионных моделей: ряд моделируется как ARIMA-процесс, затем анализируются расхождения реальных значений временного ряда с спрогнозированными моделью, после удаления тренда и сезонности. Вейвлеты применяются для обнаружения аномалий в виде всплесков на разных частотах в рассматриваемом временном ряду.

Зная распределения таких параметров трафика как IP-адреса, порты, TCP-флаги, номера протоколов, длительности сессий, можно построить гистограммы для показателей нормального трафика. Для обнаружения аномалий анализируется отклонение гистограмм текущего трафика на основе подхода LOF (Local Outlier Factor) [97] или кластеризации k-средних [98].

Нейросети находят самое широкое применение в данной задаче. Модели типа TFT (Temporal Fusion Transformer) используются для прогнозирования временных рядов, GNN (Graph Neural Network) выявляют подозрительные подграфы взаимодействий между узлами сети, автоэнкодеры обнаруживают аномалии на основе ошибки при восстановлении данных из сжатого представления данных, а языковые модели могут применяться для анализа логов системы как текстов на естественном языке. В работе [99] генеративно-состязательная нейросеть используется для классификации HTTP-запросов для применения на уровне WAF (Web Application Firewall).

Также широко используется анализ коэффициента Херста. Всплеск количества новых TCP-соединений в момент начала DoS-атаки приводит к изменению коэффициента Херста [100], его выход за интервал «трех сигм» может служить сигналом аномалии [101]. В [102] показано, что использование коэффициента Херста в качестве параметра механизма внимания LSTM (Long Short-Term Memory) нейросети может улучшить точность предсказания на 10%. Анализ коэффициента Херста можно использовать и совместно с вейвлет-разложением [103].

Анализ современных средств защиты в области NTA-решений показал, что наиболее частым методом обнаружения атак является сигнатурный метод. SNORT-подобные сигнатуры применяются в PT ISIM [104], KATA [105], eSensor [106]. В PT NAD [107] машинное обучение применяется для установления пороговых значений пользовательских правил профилирования. В KUMA [108] пороговые значения для статистических характеристик определяются через межквартильный размах. В KICS [109] применяется LSTM нейросеть для анализа данных телеметрии промышленного оборудования, и также применяются сигнатуры Suricata. В Dataplan от NGR Softlab [110] поведенческие профили формируются динамически на основе временных рядов из различных источников, обнаружение аномалий осуществляется путем сравнения различных статистических характеристик: среднего, суммы, перцентилей, а также схожести распределений и энтропии. В целом в современных NDR и XDR решениях основным подходом все еще является сигнатурный подход, нейросети набирают популярность, а статистические методы, в основном, состоят в простом сравнении целевого параметра с динамически определяемыми граничными значениями. Автокорреляция и анализ сигналов как основа для обнаружения аномалий в вендорских решениях не упоминается.

Оптимальная линейная фильтрация обычно применяется для уменьшения шума в данных для последующего сравнения с профилем нормального поведения [111, 112]. Для этого может применяться как фильтр

Калмана [113, 114], так и фильтр Винера [115]. В [116, 117] фильтр Винера применяется к данным показателей загрузки разных портов коммутатора, определяемым по SNMP переменным, вывод о наличии аномалии принимается на основе значения минимальной среднеквадратическая ошибки фильтрации для текущего трафика. В [118] описаны асимптотические соотношения для предсказания самоподобного трафика на основе оптимальных линейных фильтров, отклонение от предсказанного значения может являться признаком аномалии.

3.2. Оптимальная линейная фильтрация

3.2.1. Фильтр Винера

Фильтр Колмогорова-Винера, также часто называемый просто фильтром Винера, применяется в различных областях, включая обработку сигналов и изображений [119]. Он используется для оценки полезного сигнала по его зашумленной версии:

$$x(t) = s(t) + n(t), \tag{3.1}$$

где $s(t)$ – полезный сигнал, $n(t)$ – аддитивный шум.

Для расчета фильтра Винера необходимо знать статистические характеристики случайных процессов, соответствующих сигналу и шуму. Если на входе линейного фильтра с постоянными параметрами, описываемого импульсной характеристикой (ИХ) $h(t)$, наблюдается непрерывный сигнал $x(t)$, который является суммой полезного сигнала $s(t)$ и шума $\eta(t)$, причем оба эти сигнала являются стационарными в широком смысле, обладают нулевым средним, а также известны их корреляционные функции $R_s(\tau)$ и $R_\eta(\tau)$, или энергетические спектры $G_s(\omega)$ и $G_\eta(\omega)$, то сигнал на выходе фильтра Винера является наилучшей по критерию минимума среднеквадратической ошибки оценкой $\hat{s}(t)$ исходного сигнала.

Оценка (отклик) стационарного линейного фильтра:

$$\hat{s}(t) = y(t) = h(t) * x(t) = \int_{-\infty}^{\infty} h(t-u)x(u)du\,, \tag{3.2}$$

где $*$ – операция свертки, $h(t)$ – импульсная характеристика фильтра.

Ошибкой фильтрации (оценивания) является величина

$$e(t) = s(t) - \hat{s}(t) = s(t) - \int_{-\infty}^{\infty} h(u)x(t-u)du\,. \tag{3.3}$$

Принципиальная схема фильтра Винера представлена на Рисунке 3.1:

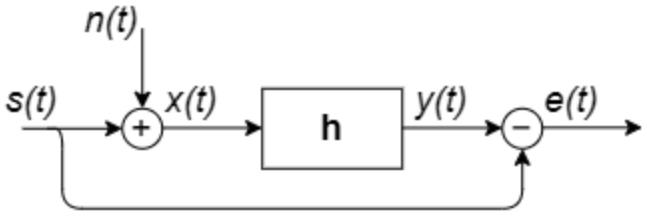


Рисунок 3.1 – Схема фильтра Колмогорова-Винера

Основной принцип заключается в минимизации среднеквадратичной ошибки оценивания (Mean Square Error, далее будет обозначаться как MSE, чтобы избежать путаницы со среднеквадратическим отклонением – СКО) между оригинальным сигналом и его восстановленной версией:

$$E[e^2(t)] = E[(\hat{s}(t) - s(t))^2] \to \min, \tag{3.4}$$

где $E[\cdot]$ – символ усреднения, $e(t)$ – ошибка фильтрации, $\hat{s}(t)$ – оценка полезного сигнала.

Для вычисления импульсной характеристики используется уравнение фильтрации. При выводе уравнения фильтрации используется принцип ортогональности, согласно которому ошибка фильтрации ортогональна входному воздействию и некоррелирована с сигналом [120].

При рассмотрении трафика как случайного процесса непрерывного времени, оптимальная ИХ $h(t) = h_{\text{опт}}(t)$ может быть получена путем решения интегрального уравнения Винера-Хопфа [121]:

$$R_{xs}(\tau) = \int_{-\infty}^{\infty} h(u)R_x(\tau - u)du\,, \tag{3.5}$$

где $R_{xs}(\tau)$ – ВКФ полезного сигнала и его зашумленной версии, $R_x(\tau)$ – АКФ процесса на входе фильтра.

По теореме Винера-Хинчина $S(\omega) = \mathcal{F}[R(\tau)]$, поэтому уравнению Винера-Хопфа в частотной области соответствует следующее [120]:

$$S_{xs}(\omega) = H(i\omega)S_x(\omega), \tag{3.6}$$

где $H(i\omega) = \mathcal{F}[h(t)]$ – частотная характеристика (ЧХ) фильтра, $\mathcal{F}[\cdot]$ – преобразование Фурье.

Решением уравнения Винера-Хопфа в частотной области является

$$H_{\text{опт}}(i\omega) = \frac{S_{xs}(\omega)}{S_x(\omega)}, \tag{3.7}$$

а если сигнал и шум некоррелированы [120]:

$$H_{\text{опт}}(i\omega) = \frac{S_s(\omega)}{S_s(\omega) + S_x(\omega)}, \tag{3.8}$$

Выражение для минимальной ошибки можно записать как:

$$\varepsilon^2_{\min} = \frac{1}{2\pi}\int_{-\infty}^{\infty}\left[S_s(\omega) - \frac{|S_{xs}(\omega)|^2}{S_x(\omega)}\right]d\omega, \tag{3.9}$$

или, при некоррелированности сигнала и шума [120]:

$$\varepsilon^2_{\min} = \frac{1}{2\pi}\int_{-\infty}^{\infty}\frac{S_s(\omega)S_n(\omega)}{S_s(\omega) + S_n(\omega)}d\omega. \tag{3.10}$$

Фильтр стремится усилить компоненты сигнала, одновременно подавляя компоненты шума и сохраняя баланс между усилением и подавлением. Если энергетические спектры сигнала и шума не пересекаются, то есть $S_s(\omega) \cdot S_n(\omega) = 0$, то минимальная ошибка фильтрации равна нулю и сигнал восстанавливается безупречно, ЧХ фильтра Винера равна единице внутри частотного диапазона сигнала и нулю вне этого диапазона [120]. В противном случае импульсная характеристика будет подавлять перекрывающуюся часть, чтобы минимизировать MSE, что показано на Рисунке 3.2 [119] и значение минимальной среднеквадратической ошибки оценивания будет отлично от нуля.

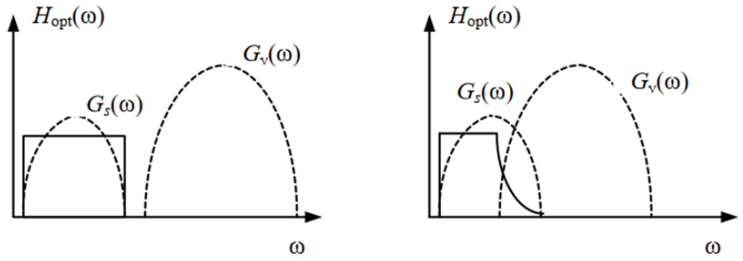


Рисунок 3.2 – ЧХ фильтра Винера

Помимо оптимальной оценки полезного сигнала в текущий момент времени, фильтр Винера также может быть использован для предсказания значений сигнала на один или несколько отсчетов «вперед» или «назад». В случае предсказания на один шаг вперед уравнение Винера-Хопфа сводится к системе линейных уравнений, совпадающих с уравнениями Юла-Уолкера, которые определяют коэффициенты авторегрессионной (AR) модели.

Учитывая, что трафик предполагается наблюдать, захватывать и анализировать с использованием программных средств, то есть в системе с дискретным временем, случайные процессы, представляющие трафик и шум можно рассматривать как случайные векторы, тогда сигнал на входе фильтра можно записать как

$$x_k = s_k + n_k. \tag{3.11}$$

Оценка сигнала на выходе фильтра представляется в виде дискретной свертки:

$$\hat{s}_k = y_k = \sum_{n=0}^{N-1} h_k \, x_{n-k}\,, \tag{3.12}$$

или в векторной форме:

$$y_k = \boldsymbol{h}^T \boldsymbol{X}_k = \boldsymbol{X}_k^T \boldsymbol{h}, \tag{3.13}$$

где $\boldsymbol{X}$ – квадратная матрица, содержащая отсчеты сигнала x к моменту времени k.

Дискретный аналог уравнения Винера-Хопфа (3.5):

$$\boldsymbol{r}_{xs} = \boldsymbol{R}_x \boldsymbol{h}, \tag{3.14}$$

где $\boldsymbol{r}_{xs}$ – вектор ВКФ полезного сигнала и сигнала на входе системы, $\boldsymbol{R}_x$ – корреляционная матрица входной последовательности, $\boldsymbol{h}$ – вектор отсчетов ИХ фильтра.

Также его можно записать в следующем виде [120]:

$$\begin{bmatrix} r_{xs}(0) \\ r_{xs}(1) \\ r_{xs}(2) \\ \vdots \\ r_{xs}(N-1) \end{bmatrix} = \begin{bmatrix} R_x(0) & R_x(1) & \cdots & R_x(N-1) \\ R_x(1) & R_x(0) & \dots & R_x(N-2) \\ R_x(2) & R_x(1) & \dots & R_x(N-3) \\ \vdots & \vdots & \ddots & \vdots \\ R_x(N-1) & R_x(N-2) & \cdots & R_x(0) \end{bmatrix} \begin{bmatrix} h_0 \\ h_1 \\ h_2 \\ \vdots \\ h_{N-1} \end{bmatrix} \quad (3.15)$$

Поскольку корреляционная матрица является *тёплицевой* матрицей, она является невырожденной и, соответственно, для неё существует обратная матрица. Из этого следует, что импульсная характеристика $\boldsymbol{h} = \boldsymbol{h}_{\text{опт}}$ может быть получена из (3.14) следующим образом:

$$\boldsymbol{h} = \boldsymbol{R}_x^{-1} \cdot \boldsymbol{r}_{xs}. \quad (3.16)$$

Минимальное значение среднего квадрата ошибки при этом:

$$\varepsilon_{\min}^2 = \sigma_s^2 - \boldsymbol{h}_{\text{опт}}^{\boldsymbol{T}} \boldsymbol{r}_{xs}, \quad (3.17)$$

его также можно выразить независимо от неизвестной импульсной характеристики, выразив его через известную корреляцию рассматриваемых случайных процессов [120, 122]:

$$\varepsilon_{\min}^2 = \sigma_s^2 - \boldsymbol{r}_{xs}^{\boldsymbol{T}} \boldsymbol{R}_x^{-1} \boldsymbol{r}_{xs}, \quad (3.18)$$

или если сигнал s_k и шум n_k не коррелированы:

$$\varepsilon_{\min}^2 = \sigma_s^2 - \boldsymbol{r}_s^T \cdot (\boldsymbol{R}_s + \boldsymbol{R}_n)^{-1} \cdot \boldsymbol{r}_s. \quad (3.19)$$

Фильтр Винера оптимален только если характеристики сигнала и шума на входе фильтра, совпадают с характеристиками, которые учитывались при вычислении ИХ фильтра, и не меняются со временем, то есть случайный процесс на входе фильтра является стационарным в широком смысле [122]. Если процесс нестационарный, то ИХ фильтра должна меняться со временем, тогда оценка сигнала на выходе примет следующий вид:

$$y_k = \boldsymbol{h}_k^{\boldsymbol{T}} \boldsymbol{X}_k, \quad (3.20)$$

где $\boldsymbol{h}_k$ – вектор ИХ фильтра в момент времени k.

Синтез фильтра Винера с переменными параметрами значительно сложнее процедуры синтеза стационарного фильтра Винера, так как для каждого момента времени необходимо решать уравнение (3.14). Упростить расчет можно, представив вектор ИХ в рекуррентной форме [120]:

$$\boldsymbol{h}_{k+1} = \boldsymbol{h}_k + \Delta\boldsymbol{h}_k, \tag{3.21}$$

где $\Delta\boldsymbol{h}_k$ – обновление координат вектора ИХ в момент k.

Использование рекурсивной процедуры обновления ИХ для адаптации к меняющимся или неизвестным условиям называется *адаптивной фильтрацией*. Если процесс является стационарным, алгоритм адаптивной фильтрации сходится к оптимальному решению. Адаптивные фильтры различаются методом формирования обновления $\Delta\boldsymbol{h}_k$, например метод наискорейшего спуска (steepest descent), метод стохастического градиента, метод наименьших квадратов (МНК).

3.2.2. Фильтр Калмана

Фильтр Калмана представляет собой рекурсивный алгоритм оптимальной оценки состояния динамической системы на основе последовательности неполных или зашумленных измерений. Основная идея заключается в комбинировании информации о состоянии системы из двух источников: предыдущей оценки состояния и нового измерения, что позволяет уточнять представление о состоянии системы на основе имеющихся данных. Фильтр Винера является частным случаем фильтра Калмана, можно показать, что в стационарной среде они оба дают идентичные решения [122].

Процесс на входе фильтра описывается парой уравнений: уравнением сообщения (состояния), которое описывает динамическое поведение случайного процесса, изменяющееся по обычно неизвестным правилам, и уравнением измерения (наблюдения), которое описывает получаемые о процессе данные. Вектор измерений предоставляет некоторый датчик или

сенсор в системе. Задача состоит в совместном решении обоих уравнений в оптимальном по критерию минимума MSE смысле [120].

Уравнение сообщения:

$$x_{n+1} = \Phi_n x_n + \Gamma_n w_n, \tag{3.22}$$

где Φ_n – матрица переходов, Γ_n – матрица шума процесса, w_n – шум.

Уравнение измерения:

$$Y_n = H_n x_n + v_n, \tag{3.23}$$

где H_n – матрица наблюдения, v_n – шум измерений.

Центральное уравнение фильтра Калмана – это линейное рекурсивное уравнение, которое состоит из двух частей: прогноза (предсказания) нового состояния и его коррекции (обновления). На этапе прогноза вычисляется оценка следующего состояния на основе предыдущей оценки и модели динамики системы. На этапе коррекции априорная оценка уточняется с учетом нового измерения, а также обновляются ковариационные характеристики ошибок оценки. Оценка следующего состояния:

$$\hat{x}_{n+1} = \Phi_n \hat{x}_n + K_{n+1}(y_{n+1} - H_{n+1}\Phi_n \hat{x}_n), \tag{3.24}$$

где K_n – коэффициент усиления Калмана, y_{n+1} – следующее измерение.

Априорная матрица ковариации ошибки:

$$\tilde{P}_{n+1} = \Phi_n P_n \Phi_n^{\boldsymbol{T}} + \Gamma_n Q_n \Gamma_n^{\boldsymbol{T}}, \tag{3.25}$$

где P_n – апостериорная матрица ковариации ошибок на предыдущем шаге, Q_n – матрица ковариации шума процесса.

Ключевой величиной здесь является K_{n+1} (Kalman gain). Его вычисление основано на том, что ошибка предсказания фильтра частично содержит новую информацию об изменении скрытого состояния системы. Его можно выразить через ковариационную матрицу ошибки оценки состояния [122].

$$K_{n+1} = \tilde{P}_{n+1} H_{n+1}^{\boldsymbol{T}} (H_{n+1} \tilde{P}_{n+1} H_{n+1}^{\boldsymbol{T}} + R_{n+1})^{-1}, \tag{3.26}$$

где R_n – матрица ковариации шума измерений.

Апостериорная матрица ковариации ошибки:

$$P_{n+1} = (I - K_{n+1} H_{n+1}) \tilde{P}_{n+1}, \tag{3.27}$$

где I – единичная матрица.

Преимуществами фильтра Калмана является применимость к нестационарным процессам и хранение лишь последнего состояния, а не всей истории наблюдений для вычисления новой оценки [122].

Недостатки заключаются в том, что случайный процесс на входе фильтра, должен быть, по сути, марковским процессом, поскольку для него существует матрица переходов F. В теории фильтрации Калмана основные выводы получаются при рассмотрении гауссовских процессов, что не подходит для представления самоподобного сетевого трафика. Фильтр Калмана не позволяет выразить в явном виде значение минимальной ошибки оценивания, наиболее близким к этому является выражение для матрицы ковариации ошибок предсказания. Существует проблема расходимости, выраженная в том, что истинные ошибки оценивания во много раз превышают теоретические предсказания [120].

Также, динамическая природа фильтра может привести к нежелательным последствиям, в случае если злоумышленник сможет внедрить в сеть источник трафика, который поначалу не будет заметно влиять на характеристики совокупного трафика в сети, но постепенно начнет усиливать свое присутствие, то постоянное обновление коэффициентов фильтра Калмана приведет к тому, что аномальный источник трафика больше не будет считаться таковым.

3.3. Ошибка фильтрации как критерий обнаружения аномалий

3.3.1. Метод на основе отклонения ошибки фильтрации

Значение минимальной среднеквадратической ошибки фильтрации для заданного сигнала и шума можно использовать в качестве характерного признака трафика, изменение которого сигнализирует об аномалии. Как было указано ранее, сетевой трафик можно рассматривать как случайный процесс. Для этого может использоваться одно из представлений, рассмотренных в главе 1. Если на интервале локальной стационарности статистические

характеристики этого процесса известны, то можно рассматривать задачу его фильтрации (оценки) по суммарному процессу:

$$x_k = s_k + n_k, \tag{3.28}$$

где s_k – случайный сигнал, представляющая легитимный трафик, n_k – шум измерений (наблюдений), характеризующий неточность измерения характеристик трафика.

Оценка статистических характеристик легитимного трафика может быть получена усреднением по множеству реализаций, полученных во время периода наблюдения за системой в нормальным режиме работы, если предположить эргодичность случайного процесса. Также в качестве модели процесса может быть принят самоподобный процесс с заданным коэффициентом Херста, задаваемый через структурную функцию [118]. Оценка АКФ может последовательности интервалов времени может производится на основе факторизации энергетического спектра [123].

Шум наблюдений может быть коррелирован или некоррелирован с легитимным трафиком. Шум можно оценить с использованием различных методов [124, 125], но для простоты его можно рассматривать как некоррелированный БГШ (нормальный случайный процесс) с заданной дисперсией σ_n^2.

В случае отсутствия шума как такового, минимальная MSE будет равна нулю, но и сам фильтр при этом будет пропускать сигнал на входе без изменений, то есть фильтрация не будет производится, импульсная характеристика фильтра в данном случае будет выглядеть как дельта-функция или единичный импульс [96, 126]. Следовательно, дисперсия шума не должна равняться нулю.

Зная характеристики легитимного трафика s_k и шума n_k, можно рассчитать минимальную среднеквадратическую ошибку фильтрации (3.19). При достаточно низком значении σ_n^2 она будет близка к нулю [127]. Данное значение можно принять в качестве «эталонного» значения ошибки ε_0^2.

Если добавление аномального процесса приводит к изменению статистических характеристик суммарного процесса по сравнению с x_k, то значение MSE отфильтрованного процесса будет существенно отличаться от «эталонного» значения ε_0^2, полученного для легитимного трафика [128]. Это также справедливо для неоптимального фильтра.

Случайный процесс на входе фильтра при возникновении в сети источника аномального трафика можно обозначить как:

$$x'_k = x_k + a_k = s_k + n_k + a_k, \tag{3.29}$$

где a_k – случайный процесс, представляющий аномальный трафик.

Оценка процесса с аддитивной аномалией:

$$\begin{aligned} y'_k &= \boldsymbol{h^T X'_k} \\ &= \boldsymbol{h^T}(\boldsymbol{X_k} + \boldsymbol{A_k}) \\ &= \boldsymbol{h^T X_k} + \boldsymbol{h^T A_k} \\ &= y_k + z_k, \end{aligned} \tag{3.30}$$

где $\boldsymbol{A}$ – квадратная матрица, содержащая отсчеты аномального процесса a к моменту времени k, y_k – реакция фильтра на ожидаемый входной сигнал, z_k – реакция фильтра на аномальную компоненту входного трафика.

Среднеквадратическая ошибка [120]:

$$J = E[(e_k)^2] = E[(s_k)^2] - 2\boldsymbol{r_{xs}^T H} + \boldsymbol{H^T R_x H}, \tag{3.31}$$

где $e_k = s_k - \hat{s}_k = s_k - y_k$ – ошибка фильтрации.

Для процесса с аддитивной аномалией выражение ошибки примет вид:

$$e'_k = s_k - y'_k = s_k - y_k - z_k = e_k - z_k, \tag{3.32}$$

среднеквадратическая ошибка:

$$\begin{aligned} J' &= E[(e_k - z_k)^2] \\ &= E[(e_k)^2] - 2E[e_k \boldsymbol{h^T A_k}] + E[(\boldsymbol{h^T} A_k)^2] \\ &= J - 2\boldsymbol{h^T} E[e_k \boldsymbol{A_k}] + \boldsymbol{h^T R_a h}. \end{aligned} \tag{3.33}$$

Выражение $E[e_k \boldsymbol{A_k}]$ можно переписать в виде:

$$\begin{aligned} E[e_k \boldsymbol{A_k}] &= E[(s_k - \boldsymbol{h^T X_k})\boldsymbol{A_k}] \\ &= E[s_k \boldsymbol{A_k}] - \boldsymbol{h^T} E[X_k A_k] \\ &= \boldsymbol{r_{sa}} - \boldsymbol{R_{ax} h}. \end{aligned} \tag{3.34}$$

Разница между эталонной MSE и MSE в случае аддитивной аномалии:

$$\Delta\varepsilon^2 = J' - J = -2\boldsymbol{h^T r}_{sa} + 2\boldsymbol{h^T R}_{ax}\boldsymbol{h} + \boldsymbol{h^T R}_a\boldsymbol{h}. \quad (3.35)$$

В данном выражении отрицательный член означает, что если аномалия коррелирована с полезным сигналом и имеет «правильную» фазу, она может частично компенсировать ошибку за счет уменьшения влияния шума.

В случае, если аномалия не коррелирована с трафиком и шумом, выражение можно упросить:

$$\Delta\varepsilon^2 = \boldsymbol{h^T R}_a\boldsymbol{h} = E[(\boldsymbol{h^T A}_k)^2] = E[(z_k)^2]. \quad (3.36)$$

Таким образом, отклонение MSE на выходе фильтра от эталонного значения при возникновении аддитивной аномалии равняется дисперсии аномальной составляющей после фильтрации.

В качестве признака аномалии можно принять величину, на которое дисперсия отличается от нуля. Даже после извлечения корня, чтобы привести ошибку к размерности рассматриваемого случайного процесса, нужно определить пороговые значения, при выходе за которые фиксируется обнаружение аномалии.

Нормализованная среднеквадратическая ошибка (NMSE) [122]:

$$\epsilon = \frac{\varepsilon^2_{\min}}{\sigma_s^2} = 1 - \frac{\sigma_y^2}{\sigma_s^2}, \quad (3.37)$$

где σ_y^2 – дисперсия оценки полезного сигнала на выходе фильтра.

Для оптимального фильтра Винера, при условии, что на входе нет аддитивного аномального процесса, $0 \le \epsilon \le 1$. При появлении аномалии, она может принимать значения меньше нуля.

В работе [129] предлагается использовать значение NMSE в качестве меры аномальности, причем в качестве нижней границы аномалии принимается нормализованное значение MSE фильтра Винера:

$$\frac{\varepsilon^2_{\min}}{\sigma_s^2} \le \max\left(\frac{\varepsilon^2_{\min}}{\sigma_s^2}, 1 - \frac{\sigma_y^2}{\sigma_s^2}\right) \le 1. \quad (3.38)$$

Обозначим нормализованную MSE, вычисляемую для случайного процесса на выходе фильтра, как:

$$\tilde{\varepsilon}_y^2 = \max\left(\frac{\varepsilon_{\min}^2}{\sigma_s^2}, 1 - \frac{\sigma_y^2}{\sigma_s^2}\right) - \frac{\varepsilon_{\min}^2}{\sigma_s^2}. \quad (3.39)$$

Тогда, выбирая пороговое значение θ, можно определить условие аномальности трафика, наблюдаемого в текущем временном окне:

$$\tilde{\varepsilon}_y^2 \geq \theta \Longrightarrow \text{аномалия}, \quad \theta \in [0,1] \quad (3.40)$$

Реализация данного метода представлена на Рисунке 3.3:

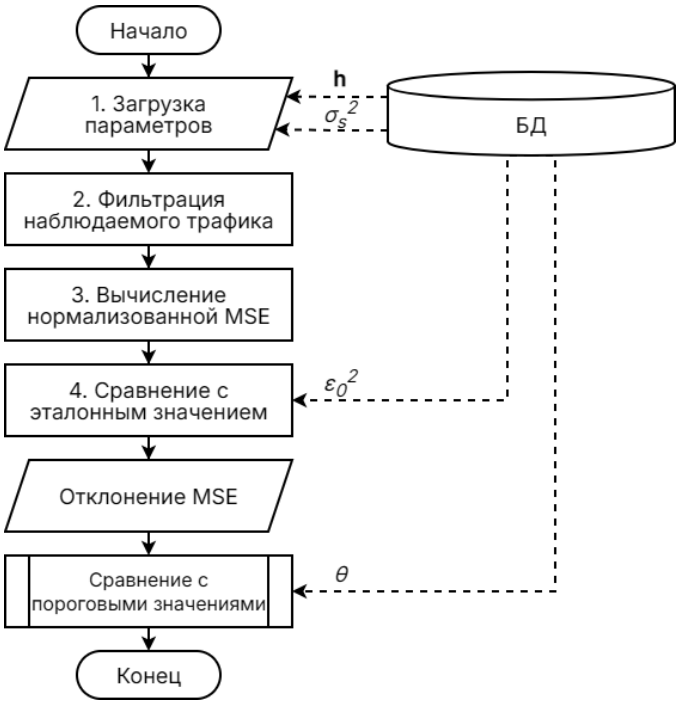


Рисунок 3.3 – Алгоритм обнаружения аномалий на основе отклонения MSE

Вычислительная сложность алгоритма на этапе оценки равна сложности выполнения фильтрации: $O(MN)$, где M – это длина сигнала, N – порядок фильтра, или $O(M\log M)$, если для вычисления свертки используется быстрое преобразование Фурье и $M \gg N$.

3.3.2. Метод на основе значения ошибки фильтрации

Если статистические характеристики случайного процесса, представляющего легитимный трафик, считаются известными, то на входе фильтра можно рассматривать как смесь нормального и аномального трафика:

$$x_k = s_k + a_k. \quad (3.41)$$

ИХ фильтра в данном подходе не рассматривается. Значение минимальной среднеквадратической ошибки, вычисляемое для процесса на

выходе фильтра, в общем случае определяется по формуле (3.18). На практике ВКФ между ожидаемым сигналом и сигналом на выходе фильтра рассчитывать в каждом временном окне достаточно проблематично, потому что для этого требуется хранить исходный образец полезного сигнала. Если предположить некоррелированность полезного сигнала и аномалии, достаточно хранить только вектор коэффициентов корреляции $\boldsymbol{r}_s$, в этом случае значение ошибки определяется по формуле (3.19), и оно будет больше, чем для оптимального фильтра с учетом всех параметров.

В случае отсутствия аномалии формула для определения минимальной MSE примет вид:

$$\varepsilon_{\min}^2 = \sigma_s^2 - \boldsymbol{r}_s^{\boldsymbol{T}}\, \boldsymbol{R}_s^{-1}\, \boldsymbol{r}_s. \tag{3.42}$$

Автокорреляционный вектор полезного сигнала $\boldsymbol{r_s}$ можно переписать как:

$$\boldsymbol{r_s} = \boldsymbol{u}_1^{\boldsymbol{T}} \boldsymbol{R}_s, \tag{3.43}$$

где $\boldsymbol{u}_1 = [1,0,\dots,0]^{\boldsymbol{T}}$ – единичный вектор.

Второе слагаемое в выражение ошибки можно представить как:

$$\begin{aligned} \boldsymbol{r}_{\boldsymbol{s}}^{\boldsymbol{T}}\, \boldsymbol{R}_s^{-1}\, \boldsymbol{r_s} &= \boldsymbol{u}_1^{\boldsymbol{T}} \boldsymbol{R}_s \boldsymbol{R}_s^{-1}\, \boldsymbol{r_s} \\ &= \boldsymbol{u}_1^{\boldsymbol{T}} \boldsymbol{E}\, \boldsymbol{r}_s \\ &= \boldsymbol{r}_s[0] \\ &= \sigma_s^2, \end{aligned} \tag{3.44}$$

где $\boldsymbol{E} = \boldsymbol{R}\boldsymbol{R}^{-1}$ – единичная матрица.

Тогда выражение MSE примет вид:

$$\varepsilon_{\min}^2 = \sigma_s^2 - \sigma_s^2 = 0, \tag{3.45}$$

то есть, в случае отсутствия аномалии, значение минимальной MSE фильтра Винера равно нулю. В случае, если в трафике содержится аномальная составляющая (ненулевой шум), значение MSE будет отлично от нуля, что было показано в предыдущих разделах.

Так как рассматриваемый в данном случае фильтр является оптимальным по критерию минимума MSE, нормализованная относительно дисперсии полезного сигнала ошибка NMSE (3.37) принимает значения в

интервале $0 \leq \epsilon \leq 1$. Условие аномальности наблюдаемого трафика определяется как:

$$\epsilon \geq \delta \Longrightarrow \text{аномалия}, \quad \delta \in [0,1] \tag{3.46}$$

Реализация данного метода представлена на Рисунке 3.4:

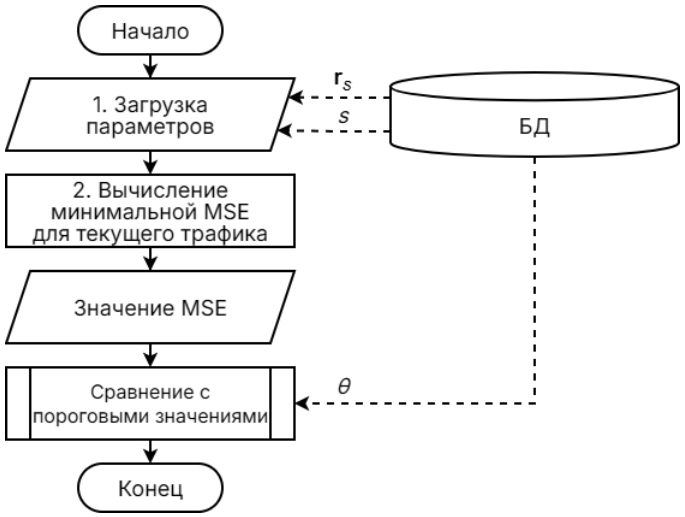


Рисунок 3.4 – Алгоритм обнаружения аномалий на основе значения MSE

Вычислительная сложность алгоритма равна $O(MN + N^3)$, где MN соответствует сложности оценке АКФ и ВКФ, или $O(MN + N^2)$, если при решении (3.16) используется алгоритм Левинсона-Дурбина.

3.3.3. Пороговые значения

В разработанных методах для определения того, является ли трафик аномальным, получаемое значение индикатора сравнивается с некоторым пороговым значением, которое необходимо определить.

Если исследуемый случайный процесс обладает некоторыми известными параметрами, их можно использовать при определении пороговых значений из требуемых вероятностей ошибок первого и второго рода (ложноположительных и ложноотрицательных заключений) [114, 130].

Известно отношение Рэлея:

$$R(M,x) = \frac{x^* M x}{x^* x}, \quad R(M,x) \in [\lambda_{\min}, \lambda_{\max}], \tag{3.47}$$

где M – эрмитова матрица, x^* – эрмитово сопряженный вектор, $\lambda_{\min}, \lambda_{\max}$ – минимальное и максимальное собственные числа матрицы M.

Отношение Рэлея принимает минимальное значение, когда x равен минимальному собственному вектору $v_{\min}$ матрицы M, и максимальное, когда $x = v_{\max}$.

Корреляционная матрица является эрмитовой и содержит только вещественные числа, поэтому операция эрмитова сопряжения превращается в транспонирование вектора, а числитель примет вид $x^T Mx$. Можно заметить, что подобное выражение встречается в формуле минимальной MSE (3.18), что позволяет определить диапазон «нормальных» значений на основе собственных чисел автокорреляционной матрицы полезного сигнала.

Выражение минимальной MSE можно переписать в виде:

$$\begin{aligned} \varepsilon_{\min}^2 &= \sigma_s^2 - \boldsymbol{r}_{xs}^T \boldsymbol{R}_x^{-1} \boldsymbol{r}_{xs} \\ &= \sigma_s^2 - \frac{\boldsymbol{r}_{xs}^T \boldsymbol{R}_x^{-1} \boldsymbol{r}_{xs}}{\|\boldsymbol{r}_{xs}\|^2} \|\boldsymbol{r}_{xs}\|^2 \\ &= \sigma_s^2 - R(\boldsymbol{R}_x^{-1}, \boldsymbol{r}_{xs}) \|\boldsymbol{r}_{xs}\|^2, \end{aligned} \tag{3.48}$$

где $\|x\| = x^T x$ – норма вектора.

Собственные числа обратной матрицы:

$$\lambda_i^{-1} = \mu_i = \frac{1}{\lambda_i}, \tag{3.49}$$

причем:

$$\mu_{\min} = \frac{1}{\lambda_{\max}}, \quad \mu_{\max} = \frac{1}{\lambda_{\min}}. \tag{3.50}$$

Тогда выражение для пороговых значений минимальной MSE примет следующий вид:

$$\varepsilon_{\min}^2 \in \left[\sigma_s^2 - \frac{\|\boldsymbol{r}_{xs}\|^2}{\lambda_{\min}}, \sigma_s^2 - \frac{\|\boldsymbol{r}_{xs}\|^2}{\lambda_{\max}} \right], \tag{3.51}$$

где $\lambda_{\min}, \lambda_{\max}$ – минимальное и максимальное собственные числа $\boldsymbol{R}_x$.

Если аномалия отсутствует, то есть $x = s$, то значение этого выражения показывает величину MSE при проекции АКФ на ось, определяемую соответствующим собственным вектором. Причем для верхней и нижней границы θ можно использовать не только оси в направлении максимальной и

минимальной дисперсии, но и второй наибольшей, второй наименьшей и т.д., для сужения диапазона «нормальных значений»:

$$\theta(i) = \sigma_s^2 - \frac{\|\boldsymbol{r}_s\|^2}{\lambda_i}. \quad (3.52)$$

Таким образом, пороговое значение для алгоритма обнаружения аномалий на основе значения среднеквадратической ошибки можно определить через собственные числа матрицы корреляции случайного процесса, представляющего легитимный пользовательский трафик.

3.3.4. Бинарная классификация

Для определения значимости отклонения ошибки от ожидаемого значения можно определить некоторый статистический критерий. Данную задачу можно сформулировать как задачу проверки статистических гипотез, определив нулевую гипотезу H_0 – рассматриваемый трафик не аномален и альтернативную гипотезу H_1 – трафик содержит аномалию. Тогда, задав определенный уровень значимости, можно вычислить значение критерия и принять решение о том, отвергается ли гипотеза H_0 (является ли трафик аномальным) или нет.

Так как решаемая задача определения, является ли наблюдаемый отрезок трафика аномальным или нет, является задачей бинарной классификации, то для определения оптимального порогового значения можно использовать график ROC-кривой (Receiver Operator Characteristic). ROC-кривая, или кривая рабочей характеристики приемника, первоначально появилась в теории обнаружении сигналов. Она используется для иллюстрации связи между относительным количеством правильных попаданий *TPR* (True Positive Rate, детектировании сигнала при наличии шума) и ложных тревог *FPR* (False Positive Rate, детектировании сигнала при его отсутствии). Аналогичным образом ROC-кривая применяется для иллюстрации чувствительности бинарных классификаторов. На Рисунке 3.5 показан пример такой кривой.

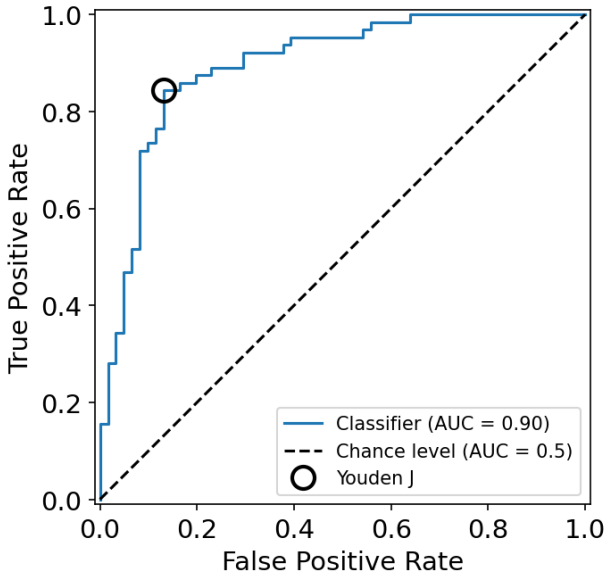


Рисунок 3.5 – ROC-кривая

Пунктирной линией обозначена кривая, которая получилась бы в случае, если классификация объектов происходила случайным образом. ROC-кривая качественного классификатора должна быть расположена в левой верхней части графика и отстоять от кривой случайного угадывания как можно дальше. В случае идеально точной классификации она выглядит как прямоугольная линия вдоль левой и верхней границы графика. Пороговое значение можно выбрать так, чтобы максимизировать TPR, минимизировать FPR, или одновременно максимизировать TPR и минимизировать FPR, для чего используется, например, J-статистика Юдена.

Показатель *AUC* (Area Under Curve, площадь под кривой) позволяет количественно интерпретировать качество бинарного классификатора и представляет собой площадь под ROC-кривой, ограниченную осью доли ложноположительных результатов. AUC принимает значения от 0 до 1, более высокое значение соответствует лучшему различению классов, значение 0.5 соответствует случайному угадыванию.

3.3.5. Основные этапы алгоритма обнаружения аномалий

Алгоритм бинарной классификации трафика (аномальный/не аномальный), с использованием одного из разработанных методов, включает

фазу обучения, которая выполняется во время штатного режима работы сети и необходима для выделения типичных сценариев сетевой активности и вычисления статистических характеристик случайных процессов, соответствующих легитимному трафику, для их последующего использования в алгоритме обнаружения аномалий. Основные этапы фазы обучения представлены на Рисунке 3.6:



Рисунок 3.6 – Диаграмма фазы обучения

На первом этапе осуществляется захват сырого трафика с пограничного или внутреннего сетевого устройства, обладающего необходимым доступом. Сбор и анализ образцов трафика проводится в штатном режиме функционирования сети (без вторжений).

Затем производится разбиение трафика на удобные для исследования образцы, например на локально-стационарные периоды, либо выделение характерных сетевых потоков с использованием протоколов SNMP, OpenFlow. Данный шаг связан с тем, что фильтр Винера применим только к стационарным случайным процессам. Если трафик не является стационарным, то алгоритм будет допускать ложноположительные

срабатывания [8]. Это актуально и для периода обучения, и для периода применения. Для предотвращения этого необходимо определить некоторый критерий, который обеспечивает разбиение последовательности на стационарные подинтервалы.

Так как в реальности любой алгоритм обнаружения аномалий применяется не ко всей исторической совокупности наблюдений трафика, а лишь к некоторому «скользящему окну», то есть наблюдаемому в текущий момент временному интервалу, то значения статистических характеристик на нем могут быть недостаточно точны. Для эффективного обнаружения атак в реальном времени необходим баланс между размером периода и минимизацией задержки обнаружения [131, 132].

После этого выделяются случайные последовательности, представляющие, например, суммарный объем трафика V_t или число пакетов N_t, поступивших на вход обрабатывающего устройства за интервал времени t, интервалы между поступлениями пакетов X_n или размеры пакетов Y_n.

Для них вычисляются значения случайных характеристик (дисперсия, средние значения для вычисления шума измерений, минимальная MSE для метода на основе отклонения ошибки). Производится синтез фильтра Винера и определение минимальной ошибки фильтрации на основе типичного сигнала и уровня шума.

Затем выполняется классификация трафика по внешним (источник, время) или внутренним (заголовки пакетов) признакам, и трафик относится к одному из типичных *сценариев использования сети* $U = \{U_1, U_2, \dots, U_n\}$. Примеры сценариев: трафик в сети филиала А с 8:00 до 12:00, с 12:00 до 16:00, трафик в нерабочие часы, выходные, трафик в сети филиала Б, или трафик сетевых потоков определенных портов: корпоративного приложения, электронной почты и т.д. В общем случае задачу выделения схожих участков некоторой последовательности решают алгоритмы сегментации и кластеризации, например k-means, k-nearest neighbors (KNN). Данные

сценарии и соответствующие им статистические характеристики трафика и значения среднеквадратической ошибки сохраняются в базе данных.

Статистические характеристики трафика в сети меняются с течением времени из-за изменений в использовании сети и её топологии, поэтому статистические характеристики выделенных сценариев должны регулярно обновляться и корректироваться.

Основные этапы алгоритма обнаружения аномалий после завершения фазы обучения представлены на Рисунке 3.7:

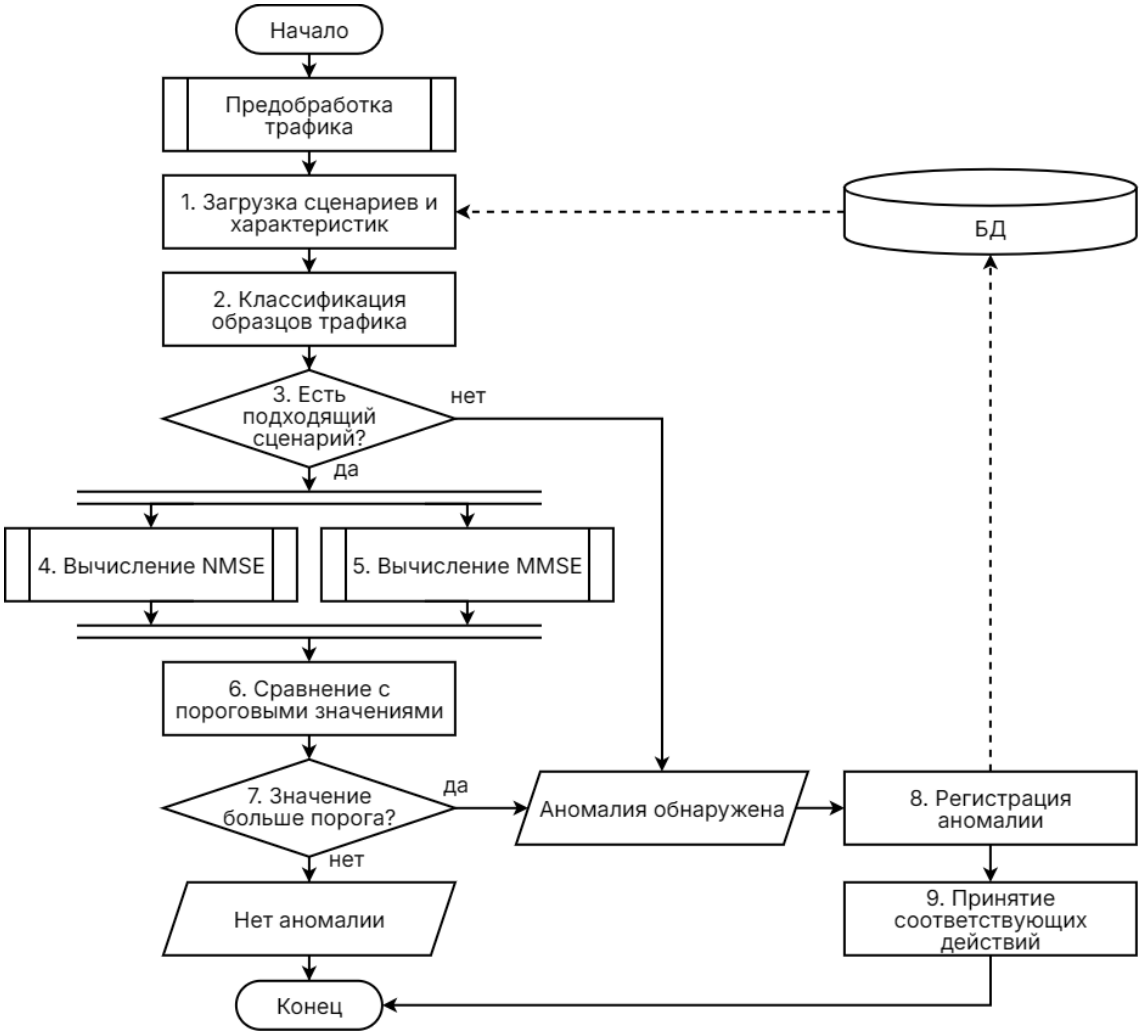


Рисунок 3.7 – Диаграмма обнаружения аномалий

На этапе применения алгоритма трафик сначала проходит предобработку, идентичную описанной в шагах 1–4 фазы обучения, чтобы привести его к сопоставимому виду. Если во время фазы обучения алгоритм применялся к сетевым потокам, то на данном этапе из сырого трафика также требуется выделить потоки.

Затем выполняется загрузка известных сценариев из базы и определение сценария, подходящего под текущий трафик. Выполняется классификация текущего периода либо потока, то есть отнесение его к одному из ранее выделенных сценариев. Если ни один сценарий не определяется как подходящий, это может также служить признаком аномалии. Если характеристики трафика подходят под сценарий, который в данный момент не является допустимым (например, использование корпоративной сети в нерабочее время), то это также может служить признаком аномалии и в данном случае генерируется предупреждение.

После этого вычисляется значение MSE для текущего трафика (для метода на основе отклонения ошибки) или вычисляется минимальная MSE для текущего трафика (для метода на основе значения ошибки) и сравнивается с пороговыми значениями. При превышении пороговых значений, определенных экспериментально или из собственных значений матрицы корреляции, принимаются соответствующие действия, такие как уведомление администратора безопасности, блокировка доступа и т.д. Информация об аномалии фиксируется в базе данных для последующего разбора инцидента.

Главным ограничением является прежде всего то, что разработанные методы обнаружения аномалий основаны на сравнении АКФ случайной последовательности, выделяемой из трафика, поэтому алгоритм может обнаруживать только те аномалии, которые явно влияют на статистические характеристики сетевого трафика, например сканирование сети, которое может быть первым этапом разведки перед основными действиями злоумышленников, распространение червей, необычные паттерны удаленного доступа и т.д. Резкие всплески интенсивности трафика из-за DoS- и DDoS-атак также должны приводить к изменению характеристик трафика, и соответственно тоже должны быть обнаружены. Данный подход не позволяет обнаруживать атаки уровня хоста, которые эксплуатируют уязвимости конкретного устройства и не связаны с передачей

дополнительных данных по сети: вирусы, уязвимости ОС и приложений (переполнение буфера, повышение прав и т.п.), точечный перехват трафика, не влияющий на общую картину (Man in the Middle, MITM), атаки уровня приложений (PHP-, SQL-инъекции) и т.д.

Для классификации наблюдаемого трафика или отдельных сетевых потоков необходимо сравнивать статистические характеристики последовательностей с целью определения степени их сходства. Для этого используются различные метрики расстояния, позволяющие сравнивать последовательности в статистическом пространстве. Важнейшей статистической характеристикой для разрабатываемого алгоритма является АКФ или матрица автокорреляции.

В работе [133] был проведен сравнительный анализ метрик расстояния, применимых к матрицам автокорреляции. Расчет производился для последовательностей интервалов поступления пакетов, выделенных из трафика архива MAWI [35]. АКФ, полученная для трафика в каждый день недели, сравнивалась с первым днем. Результаты расчета расстояний с использованием различных метрик представлены на Рисунке 3.8.

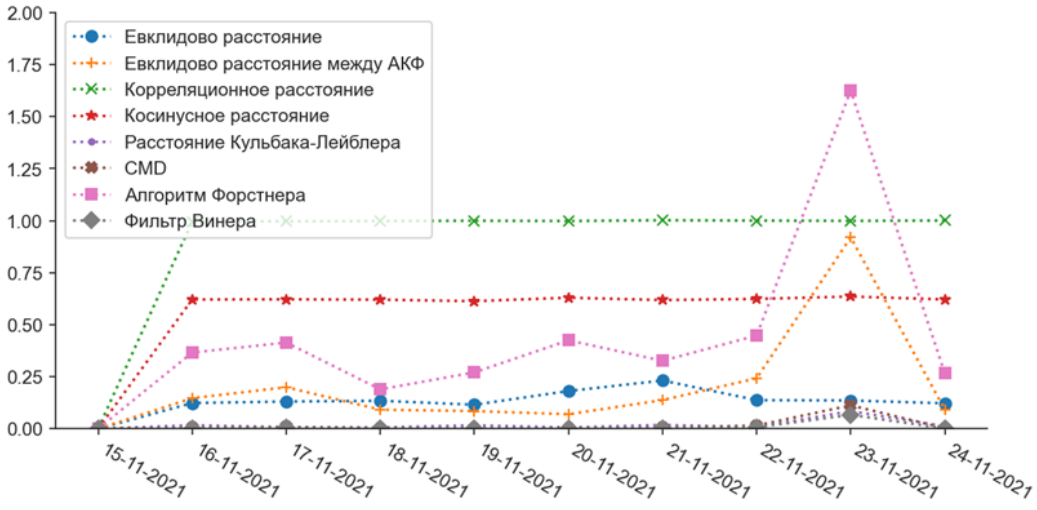


Рисунок 3.8 – Сравнительный анализ метрик расстояния АКФ

Наличие выраженного пика в значениях некоторых метрик для трафика за 23 ноября 2021 года свидетельствует об их чувствительности к корреляционным свойствам процесса, поскольку именно в этот день форма

АКФ значительно отличалась от исходной. Метрика CMD (Correlation Matrix Distance) [134] обладает следующими характеристиками: относительная простота вычисления, математическая обоснованность, ограниченный диапазон значений $[0, 1]$, и разработана именно для сравнения корреляции сигналов, поэтому оптимальна для рассматриваемой задачи.

В Таблице 3.1 приведены основные характеристики и свойства каждой метрики, которые были рассмотрены в исследовании [133]:

Таблица 3.1 – Описание метрик

Метрика	Формула	Вычислительная сложность
Евклидово расстояние	$\sqrt{\sum_i (x_i - y_i)^2}$	$O(n)$
Евклидово расстояние между АКФ	$\sqrt{\sum_i (R(x)_i - R(y)_i)^2}$	$O(n^2)$
Корреляционное расстояние	$1 - \rho(x, y)$	$O(n)$
Косинусное расстояние	$1 - \frac{x \cdot y}{\|x\| \|y\|}$	$O(n)$
Расхождение Кульбака-Лейблера	$\sum_i [p(x) \cdot \ln(p(x)/ p(y))]$	$O(n^3)$
CMD	$1 - \frac{tr(X,Y)}{\|x\| \|y\|}$	$O(n^2)$
Оператор Форстнера	$\sqrt{\sum_i \ln^2 (\lambda_i(X, Y))}$	$O(n^3)$
MSE фильтра Винера	(3.18)	$O(n^3)$

Метод на основе значения среднеквадратической ошибки также может применяться для определения расстояния между АКФ [127], но он обладает более высокой вычислительной сложностью, что делает его применение в задачах классификации нерациональным.

3.4. Выводы по главе 3

Проведен обзор существующих методов обнаружения сетевых аномалий в компьютерных сетях, применяющиеся в СОВ. Разработаны методы обнаружения аномалий на основе минимальной среднеквадратической ошибки фильтра Винера, применяемого к случайному процессу, выделяемому из трафика. Один из методов основан на сравнении ошибки фильтрации текущего наблюдаемого трафика с эталонным

значением, а другой на вычислении минимальной ошибки для текущего трафика. Оба метода требуют построения модели нормального трафика без воздействия аномалий. Представлено теоретическое обоснование разработанных методов и оценка их вычислительной сложности в нотации «О» большое.

Рассмотрены варианты получения пороговых значений из ROC-кривых бинарного классификатора и на основе собственных чисел матрицы корреляции случайного процесса, представляющего легитимный трафик.

Разработан алгоритм обнаружения аномалий на основе двух разработанных подходов. Дано подробное описание шагов алгоритма и особенностей предобработки трафика, которые необходимо учитывать. Описаны ограничения, связанные с применимостью фильтра Винера только к стационарным процессам, необходимостью обновления моделей нормального трафика при изменении топологии сети или характера её использования, а также возможности обнаружения только сетевых атак, влияющих на статистические характеристики трафика. Проведен сравнительный анализ различных метрик расстояния для сравнения АКФ, которые могут использоваться в алгоритме.

4. Оценка эффективности разработанных алгоритмов обнаружения аномалий в трафике

4.1. Обнаружение аномалий в смоделированном трафике

4.1.1. Моделирование смеси трафика с различной формой АКФ

Для проверки разработанного алгоритма обнаружения аномалий было проведено моделирование фильтрации нормального и аномального трафика [135]. Сперва производится оценивание ошибки фильтрации трафика и сравнение ее с ожидаемым значением для нормального трафика (смеси $s(t)$ и $n(t)$, имеющими разные АКФ). Затем к этой смеси добавляется случайный процесс $a(t)$, представляющий аномальную составляющую, вычисляется значение NMSE и сравнивается со значением, полученным для нормального трафика. Рассматриваются три варианта формы АКФ процессов: без корреляции (БГШ), с треугольной АКФ:

$$R(\tau) = \sigma^2 e^{-\frac{|\tau|}{\tau_0}}, \tag{4.1}$$

и экспоненциальной АКФ:

$$R(\tau) = \begin{cases} \sigma^2 \left(1 - \dfrac{|\tau|}{\tau_0}\right), & |\tau| \le \tau_0 \\ 0, & |\tau| > \tau_0 \end{cases}. \tag{4.2}$$

Для повышения точности оценки в рамках каждого эксперимента с заданной АКФ было проведено 20 независимых испытаний. На первом этапе генерируются случайные последовательности с заданной формой АКФ. Закон распределения случайного процесса во всех случаях гауссовский. Реализации последовательностей были сгенерированы методами авторегрессии (для экспоненциальной АКФ) и скользящего среднего (для треугольной АКФ) [80]. На Рисунке 4.1 представлены графики АКФ сгенерированных процессов, пунктирной линией обозначена целевая АКФ, цветными – АКФ сгенерированных реализаций. Расхождения объясняются конечным размером последовательностей.

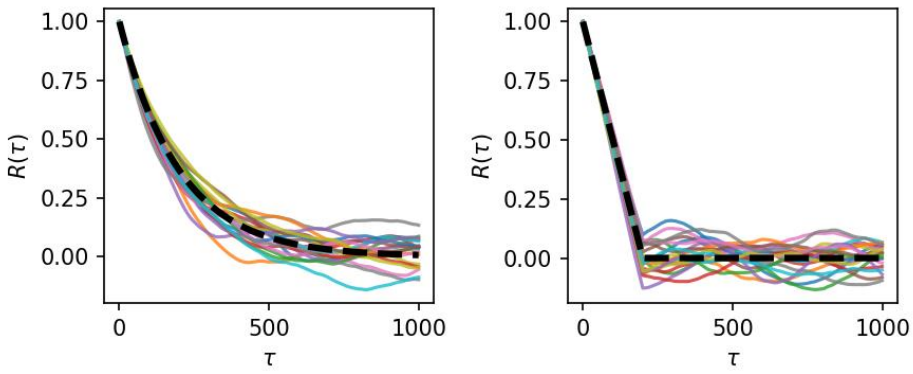


Рисунок 4.1 – АКФ сгенерированных последовательностей

Для каждого из трех случаев получено ожидаемое значение минимальной NMSE по формуле (3.37), произведена линейная фильтрация смеси последовательностей с рассматриваемыми АКФ и вычислены реальные значения NMSE. Значения ожидаемых и реальных ошибок для каждой последовательности приведены на графике на Рисунке 4.2. По оси абсцисс отмечены ожидаемые (эталонные) значения ошибки фильтрации, а по оси ординат – реальные значения нормализованной среднеквадратической ошибки, полученные для отфильтрованного процесса. Пунктиром отмечена линия $y = x$, в которой значение ожидаемой ошибки совпадает с реальным. Расхождения объясняются неидеальным совпадением моделируемой АКФ из-за ограниченности размера выборки.

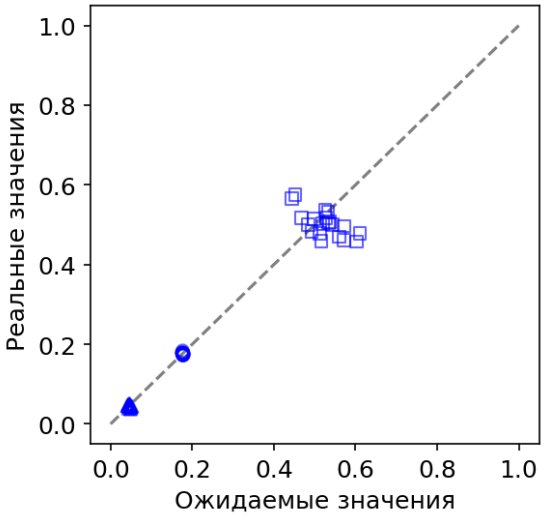


Рисунок 4.2 – NMSE нормального трафика

При моделировании учитывались первые 1000 отсчетов корреляционных функций, то есть порядок фильтра равен 1000. Дальнейшее

увеличение порядка фильтра не приводит к существенному улучшению результатов, но заметно замедляет вычисления, поскольку размер корреляционных матриц, перемножаемых при фильтрации, квадратично зависит от порядка фильтра.

Затем к полученным на предыдущем шаге реализациям нормального трафика с шумом добавляется аномальный процесс с определенной АКФ, затем производится фильтрация и вычисляются значения NMSE. Ожидаемые значения ошибки совпадают со значениями из предыдущих расчетов, поскольку характеристики аномального процесса не учитываются при синтезе фильтра. График представлен на Рисунке 4.3:

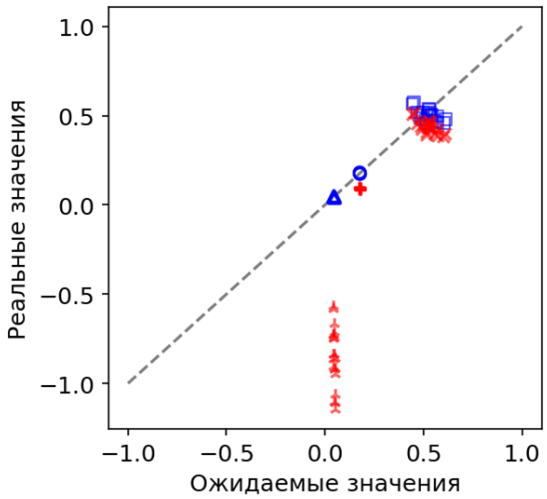


Рисунок 4.3 – NMSE аномального трафика

По графику видно, что отличие величины значения полученной NMSE зависит от формы АКФ нормального трафика, шума и аномалии. В некоторых случаях отличие минимально, для такой ситуации трафик является подозрительным и подлежит более детальному анализу [136].

Для определения статистической значимости наблюдаемого отклонения ожидаемой ошибки от реальной (с аномалией и без) в работе [135] применяется t-критерий Стьюдента для зависимых выборок:

$$t = \frac{M_d}{\sigma_d/\sqrt{n}}, \tag{4.3}$$

где M_d – средняя разность значений, σ_d – стандартное отклонение разностей, n – количество наблюдений.

При этом оценивание значения ошибки фильтрации процесса выполняется для одних и тех же сгенерированных реализаций процесса с заданной АКФ. В данном случае нулевая гипотеза H_0 состоит в том, что математическое ожидание в двух выборках совпадает и, соответственно, аномалия не обнаруживается. Уровень значимости принимался равным 0,05. Результаты расчетов представлены в Таблице 4.1

Таблица 4.1 – Проверка статистической значимости отклонений

Форма $R_s(\tau)$	Форма $R_n(\tau)$	Форма $R_a(\tau)$	Значение критерия	H_0
Экспоненциальная	Треугольная	-	1,396	Не отвергается
Дельта-импульс	Экспоненциальная	-	0,572	Не отвергается
Треугольная	Дельта-импульс	-	1,354	Не отвергается
Экспоненциальная	Треугольная	Дельта-импульс	5,270	Отвергается
Дельта-импульс	Экспоненциальная	Треугольная	82,994	Отвергается
Треугольная	Дельта-импульс	Экспоненциальная	23,277	Отвергается

Все отклонения NMSE для трафика под воздействием аномалии можно считать статистически значимыми, следовательно отклонение реального значения нормализованной среднеквадратической ошибки может служить признаком наличия аномальной составляющей в случайном процессе, представляющем сетевой трафик.

4.1.2. Зависимость ошибки от отношения сигнал/шум

Для определения влияния задаваемого уровня шума наблюдений на эффективность алгоритма на основе отклонения ошибки фильтрации, проведено моделирование сетевого трафика с учетом наличия или отсутствия аномалий, формы АКФ, а также различных уровней отношения сигнал/шум [127].

Для моделирования $s(t)$ используется случайный процесс с законом распределения Вейбулла с параметрами формы и масштаба, равными единице и синусоидальной АКФ:

$$R_s(\tau) = \sigma_s^2 \frac{sin(\tau/\tau_0)}{\tau/\tau_0}. \quad (4.4)$$

В качестве модели $n(t)$ принимается некоррелированный случайный процесс с нормальным законом распределения. Дисперсия шума определяется из соотношения:

$$\sigma_n^2 = \frac{E[(s(t)^2)]}{SNR}, \tag{4.5}$$

где $E[(\cdot)^2]$ – второй момент случайной величины, SNR – отношение сигнал/шум.

Для моделирования случайного процесса с заданным законом распределения и АКФ используется подход, описанный в [85], основанный на получении циркулянтной корреляционной матрицы и преобразовании Фурье. После моделирования определяется NMSE при различных значениях отношения сигнал/шум и реальное значение ошибки, для случая, когда фильтр применяется к трафику без аномалии и когда в трафике появляется аномальный процесс $a(t)$, имеющий АКФ различной формы. Рассматривается три вида АКФ аномального процесса: синусоидальная (4.4), синусоидальная (4.1) и синусоидальная (4.2).

Рассматривается несколько значений отношения сигнал шум: 1/100, 1/10, 1/2, 1, 2, 10, 100. Для каждого значения синтезируется фильтр и проводится 10 независимых испытаний, в каждом генерируются случайные последовательности с заданным законом распределения и АКФ, к которым затем применяется фильтр. Вычисляется среднеквадратическая ошибка фильтрации, нормируемая по теоретической дисперсии распределения Вейбулла:

$$\sigma_s^2 = q^2 \left[\Gamma\left(1 + \frac{2}{p}\right) - \Gamma^2\left(1 + \frac{1}{p}\right) \right], \tag{4.6}$$

где $p > 0$ – параметр формы, $q > 0$ – параметр масштаба.

На Рисунке 4.4 представлены результаты для процесса без воздействия аномалии. Пунктирной линией представлены теоретические нормализованные минимальные значения среднеквадратической ошибки, полученные с использованием формулы СКО для распределения Вейбулла с

заданными параметрами. Сплошной линией показаны средние за 10 испытаний значения среднеквадратической ошибки фильтрации, вычисленные экспериментально. Вертикальные линии показывают разброс значений (СКО) для каждого уровня сигнал/шум.

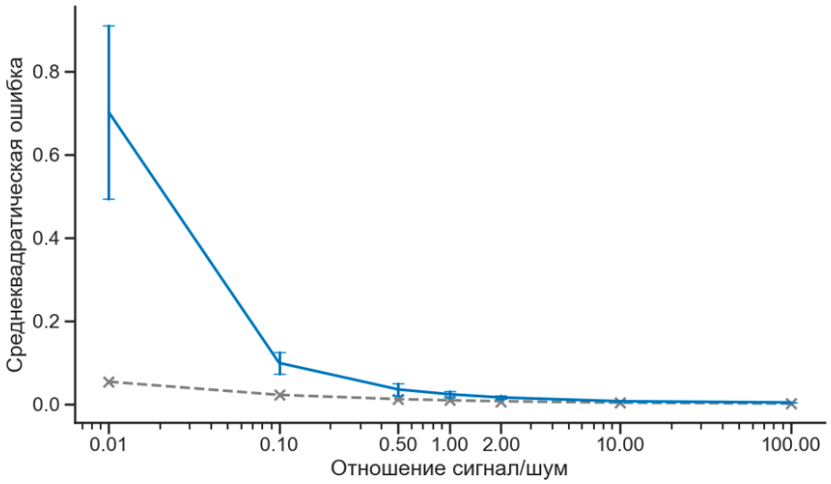


Рисунок 4.4 – NMSE нормального трафика при различных уровнях шума

По графику видно, что в случаях, где шум преобладает, фактическое значение ошибки значительно отклоняется от минимального. При снижении уровня шума фактическое значение ошибки приближается к минимальному.

На Рисунке 4.5 представлен график для процесса с различными видами аномалий, где дополнительно было отмечено значение NMSE равное 1.

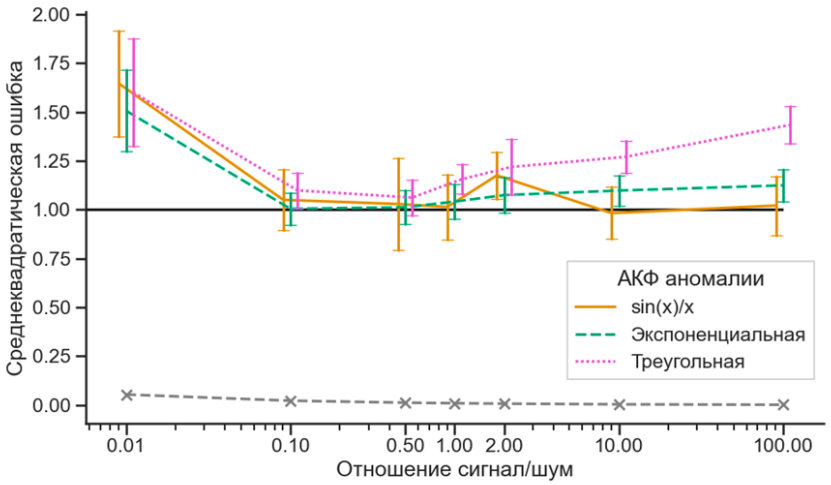


Рисунок 4.5 – NMSE смеси нормального трафика с аномальным при различных уровнях шума

Если входной сигнал фильтра представлен процессом $x(t)$ без аномалий, то значение нормированной ошибки должно оставаться в диапазоне от 0 до 1 [122]. Из графика следует, что практически в каждом случае наличие аномалий в трафике приводит к увеличению значения ошибки и превышению верхней границы. При добавлении к поступающему на вход фильтра трафику аномального процесса $a(t)$, значение среднеквадратической ошибки фильтрации значительно возрастает, и оказывается больше единицы, что является признаком наличия аномалии в обрабатываемом трафике.

4.2. Обнаружение аномалий в реальном сетевом трафике

4.2.1. Обнаружение аномалий в трафике MAWI

Для проверки разработанного алгоритма обнаружения аномалий на данных реального сетевого трафика, проведено исследование трафика из данных архива MAWI. Каждая запись из него включает в себя анонимизированный PCAP-файл, состоящий из 15 минут трафика с транзитного канала, а также XML и CSV файлы с описанием аномалий. Разметка данных производится на основе таксономических признаков, по сути являющихся сигнатурами. XML файлы также включают в себя информацию о детектировании аномалии различными способами: на основе отклонения статистик трафика от гамма-распределения, на основе расхождения Кульбака-Лейблера между нормальным и текущим распределением трафика, и на основе преобразования Хафа, выделяющего структурные аномалии в сетевых данных [137].

Основные категории атак, входящих в состав датасета MAWI: сканирование портов, адресов и сервисов, DoS- и DDoS-атаки, альфа-потоки, IPv6 туннелирование, ошибки TTL, ICMP, другие неизвестные аномалии.

Записи трафика с 11 по 17 октября 2021 года разбиваются на минутные интервалы, каждый из которых рассматривается как отдельный сценарий U. Каждому интервалу присваивается метка аномальности на основе того,

присутствуют ли на этом интервале аномалии любого типа в исходном датасете. Аномальными были признаны 64 из 105 (60%) минут во всех записях, то есть датасет является практически сбалансированным [129].

На записях трафика, собранных в один день, производится «обучение модели», то есть синтез фильтров для каждого минутного интервала. Можно сказать, что для каждой минуты используется своя собственная модель. Шум принимается гауссовским с дисперсией равной дисперсии выделенного из трафика случайного процесса.

Затем алгоритм обнаружения аномалий применяется к каждой соответствующей минутной записи за другие дни, производится фильтрация и вычисляется значение NMSE. Обнаружение аномалий производится путем синтеза фильтра для одного дня, условно признанного «нормальным» и применения фильтра к трафику остальных дней.

Полученные значения NMSE приводятся к диапазону значений [0,1] и рассматриваются как оценка бинарного классификатора. Полученные в результате графики ROC-кривой и кривой Precision-Recall (точности-полноты) для трафика в виде межпакетных интервалов и временного ряда, отражающего число пакетов в секунду, представлены на Рисунке 4.6

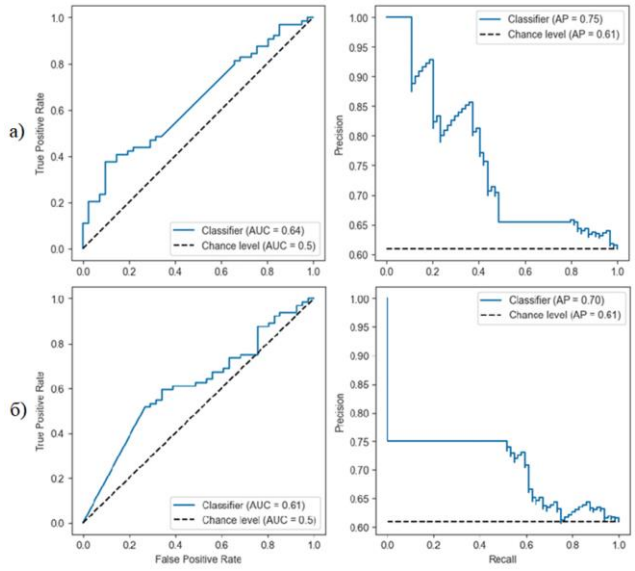


Рисунок 4.6 – Графики ROC-кривой и кривой Precision-Recall

Во всех случаях метрика AUC составляет около 0,6. Это говорит о том, что алгоритм на основе отклонения NMSE применительно к данным

трафиковым последовательностям в качестве бинарного классификатора обладает не очень высокой предсказательной способностью [138]. Это может быть обусловлено как неточностью алгоритма, так и ошибками в проведении эксперимента, поскольку данные лишь условно разделялись на нормальные и аномальные, отмеченные в датасете аномалии присутствовали в данных для обучения (в трафике практически отсутствуют интервалы, на которых нет хотя бы одной аномалии).

Также стоит заметить, что те алгоритмы обнаружения аномалий, на основе применения которых производилась разметка данных в записях из архива MAWI, могут обнаруживать атаки по специфическим сигнатурам, и соответственно некоторые аномалии, которые были выделены ими, не могут быть обнаружены, поскольку не влияют на характеристики трафика.

4.2.2. Обнаружение аномалий в трафике CIC-IDS2017

Для проверки разработанного алгоритма обнаружения аномалий на данных реального сетевого трафика, также был исследован трафик датасета CIC-IDS2017. Штатный режим функционирования сети соответствует трафику, собранному в понедельник, когда никаких атак не производилось. Данный трафик был разбит на часовые интервалы, каждый из которых соответствовал сценарию использования сети, всего 8 сценариев.

Трафик, собранный в остальные дни и содержащий трафик атак, разбивается на интервалы по 1 минуте, так же как в главе 1 при применении моделей машинного обучения. Для каждого такого интервала вычисляется текущее значение NMSE и минимальное значение NMSE. Дисперсия шума σ_n^2 в алгоритме на основе отклонения ошибки фильтрации принимается равной $0.25 \cdot \sigma_s^2$. Экспериментально было установлено, что выбор конкретного уровня шума, в случае если он не превышает дисперсию нормального сигнала, не оказывает существенного влияния на результаты, что также подтверждается в работе [127] при сравнении NMSE при разных значениях отношения сигнал/шум.

Производится сравнение обоих показателей с «эталонными» значениями образца нормального трафика, собранного в то же время (час) в понедельник и представленного в виде последовательности межпакетных интервалов времени X_n , размеров пакетов Y_n , временных рядов со значениями, представляющими суммарный объем трафика V_t и количество пакетов N_t за интервал времени t. Для последовательностей в понедельник была произведена оценка стационарности, по результатам которой все они были признаны стационарными, что позволяет применение фильтра Винера.

Для классификации каждого вида атак рассматривается трафик, содержащий как трафик атаки, так и весь остальной **легитимный** трафик в тот же день, в который проводилась атака. Для каждого алгоритма строится график ROC-кривой при различных пороговых значениях и вычисляется значение AUC. Полученные результаты для алгоритма на основе отклонения ошибки фильтрации представлены в Таблице 4.2

Таблица 4.2 – Показатели AUC для алгоритма на основе отклонения ошибки фильтрации

Тип атаки	Подтип атаки	AUC X_n	AUC Y_n	AUC V_t	AUC N_t
Bruteforce	FTP-Patator	0,607	0,660	0,667	0,683
Bruteforce	SSH-Patator	0,807	0,520	0,656	0,759
DoS	slowloris	0,476	0,688	0,563	0,474
DoS	Slowhttptest	0,576	0,430	0,494	0,511
DoS	Hulk	0,578	0,110	0,120	0,154
DoS	GoldenEye	0,583	0,224	0,234	0,246
DoS	LOIT	0,887	0,071	0,133	0,172
Exploit	Heartbleed	0,800	0,148	0,350	0,737
Web	Bruteforce	0,416	0,746	0,784	0,781
Web	XSS	0,424	0,508	0,573	0,620
Web	Sql injection	0,515	0,324	0,351	0,460
Infiltration	Dropbox download	0,694	0,549	0,548	0,442
Botnet	ARES	0,641	0,385	0,443	0,587
Port Scan	Firewall on	0,706	0,380	0,419	0,493
Port Scan	Firewall off	0,701	0,578	0,520	0,531

Полученные результаты для алгоритма на основе значения ошибки фильтрации представлены в Таблице 4.3

Таблица 4.3 – Показатели AUC для алгоритма на основе значения ошибки фильтрации

Тип атаки	Подтип атаки	AUC X_n	AUC Y_n	AUC V_t	AUC N_t
Bruteforce	FTP-Patator	0,698	0,484	0,735	0,769
Bruteforce	SSH-Patator	0,641	0,759	0,785	0,665
DoS	slowloris	0,592	0,263	0,529	0,527
DoS	Slowhttptest	0,235	0,422	0,533	0,527
DoS	Hulk	0,689	0,941	0,786	0,480
DoS	GoldenEye	0,426	0,497	0,373	0,280
DoS	LOIT	0,875	0,962	0,950	0,729
Exploit	Heartbleed	0,605	0,949	0,952	0,895
Web	Bruteforce	0,815	0,211	0,672	0,673
Web	XSS	0,314	0,382	0,444	0,487
Web	Sql injection	0,318	0,444	0,453	0,493
Infiltration	Dropbox download	0,565	0,776	0,854	0,700
Botnet	ARES	0,332	0,558	0,630	0,587
Port Scan	Firewall on	0,553	0,632	0,697	0,689
Port Scan	Firewall off	0,562	0,805	0,821	0,800

Для визуализации результатов были отобраны типы атак, для которых среднее значение AUC для всех подтипов атаки превышает 0.5. Графики, полученные для алгоритма на основе отклонения ошибки фильтрации, представлены на Рисунке 4.7:

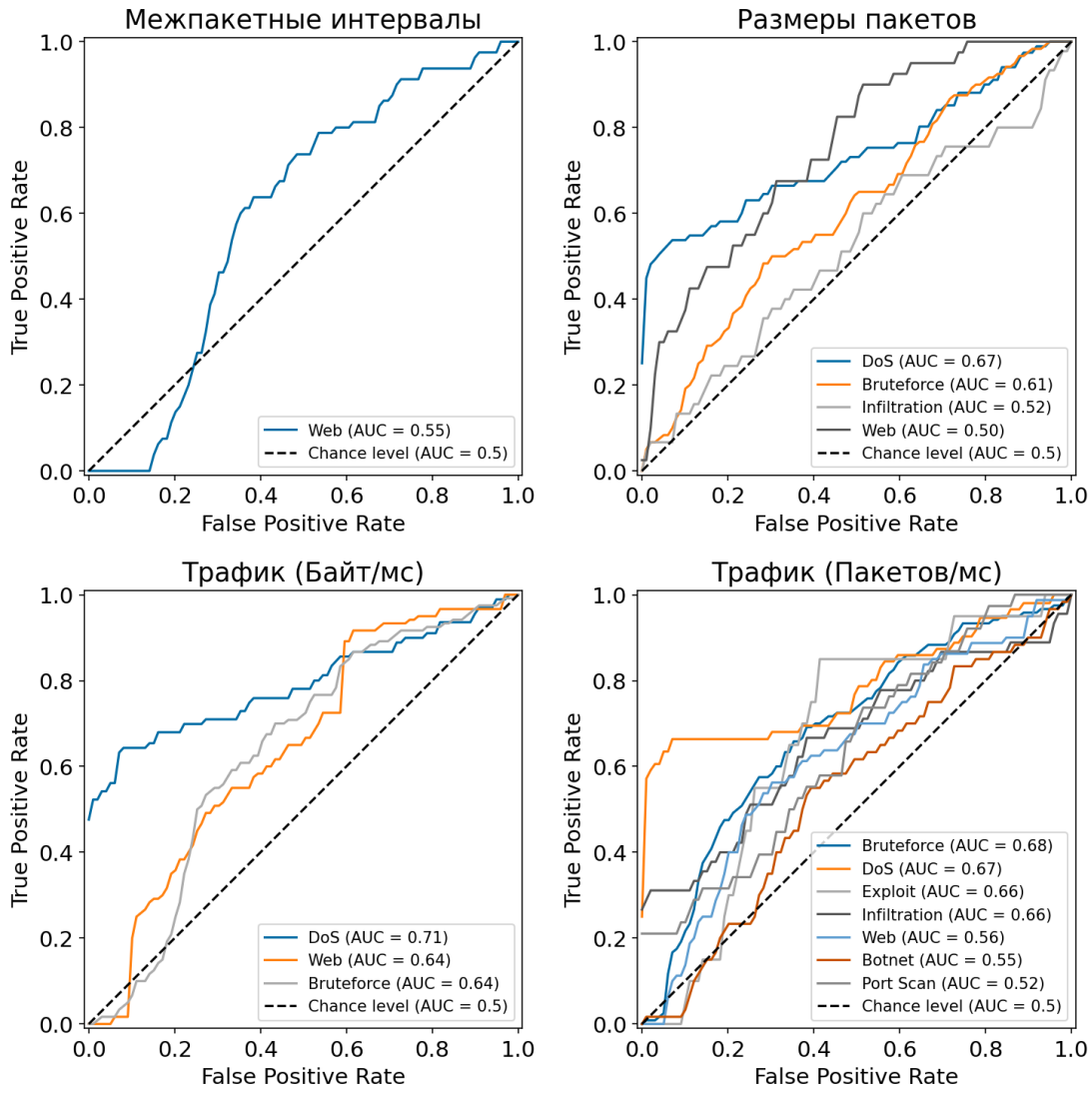


Рисунок 4.7 – ROC-кривые для алгоритма на основе отклонения ошибки

При рассмотрении отклонения ошибки фильтрации больше всего информации можно получить из временного ряда, представляющего число пакетов. Наибольшее значение AUC в среднем получено для эксплойтов, брутфорс-атак Patator и атак внедрения.

Графики, полученные для алгоритма на основе значения ошибки фильтрации, представлены на Рисунке 4.8:

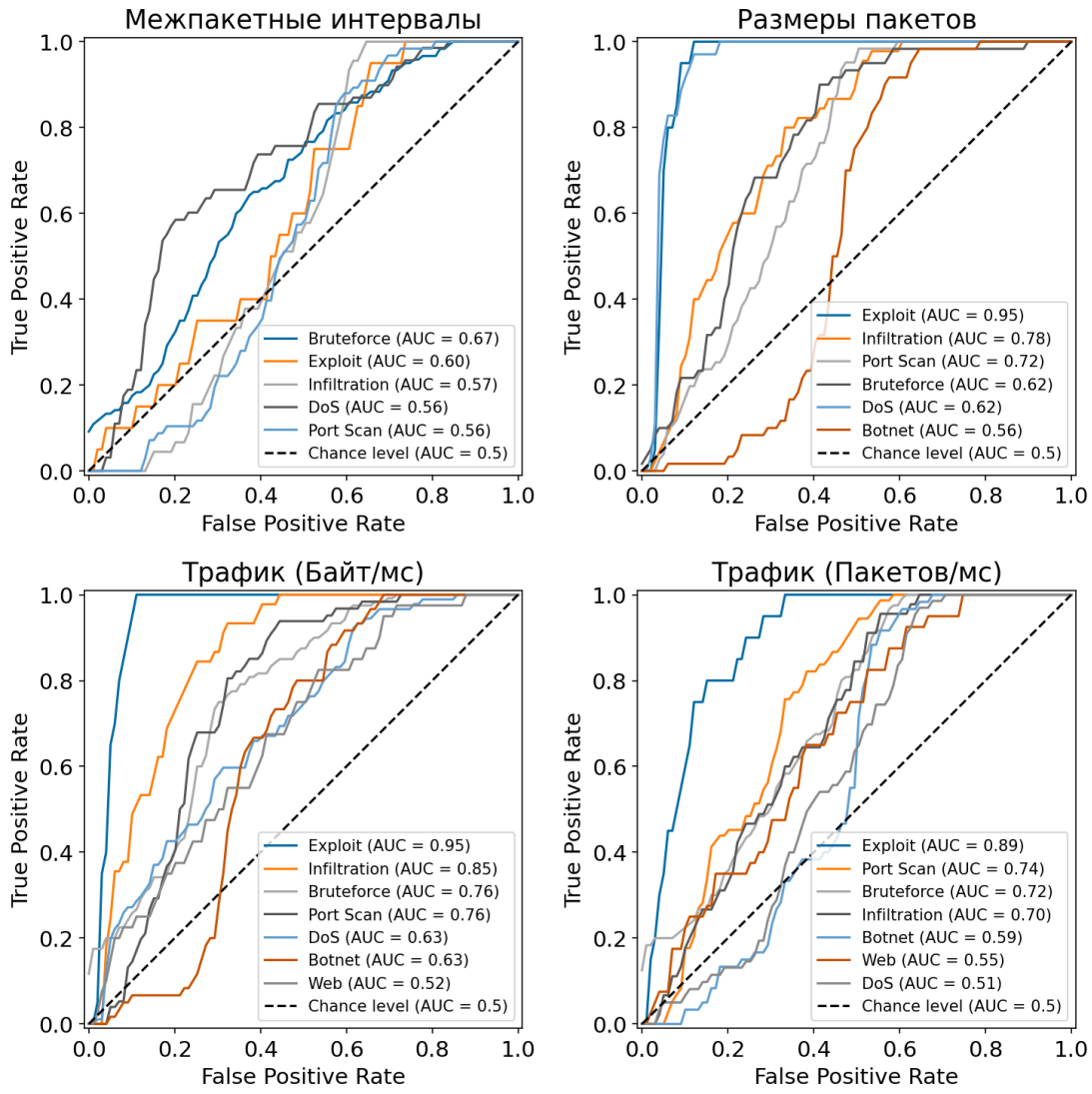


Рисунок 4.8 – ROC-кривые для алгоритма на основе значения ошибки

Для алгоритма на основе значения ошибки фильтрации помимо DoS-атак и брутфорс-атак, достаточно высокие показатели AUC получены также для сканирования портов, эксплойтов и атак внедрения.

Было проведено сравнение с классическими методами, применяющимися для обнаружения аномалий на основе статистических характеристик, для среднего: выход скользящего среднего за интервал в 3σ, CUSUM, для АКФ: значение упомянутой ранее метрики CMD [134], для распределения: статистика критерия согласия Колмогорова-Смирнова и расстояние Вассертштейна. Результаты представлены на Рисунке 4.9. Точками отмечены атаки, для которых один из разработанных алгоритмов дает наибольшие значения метрики AUC.

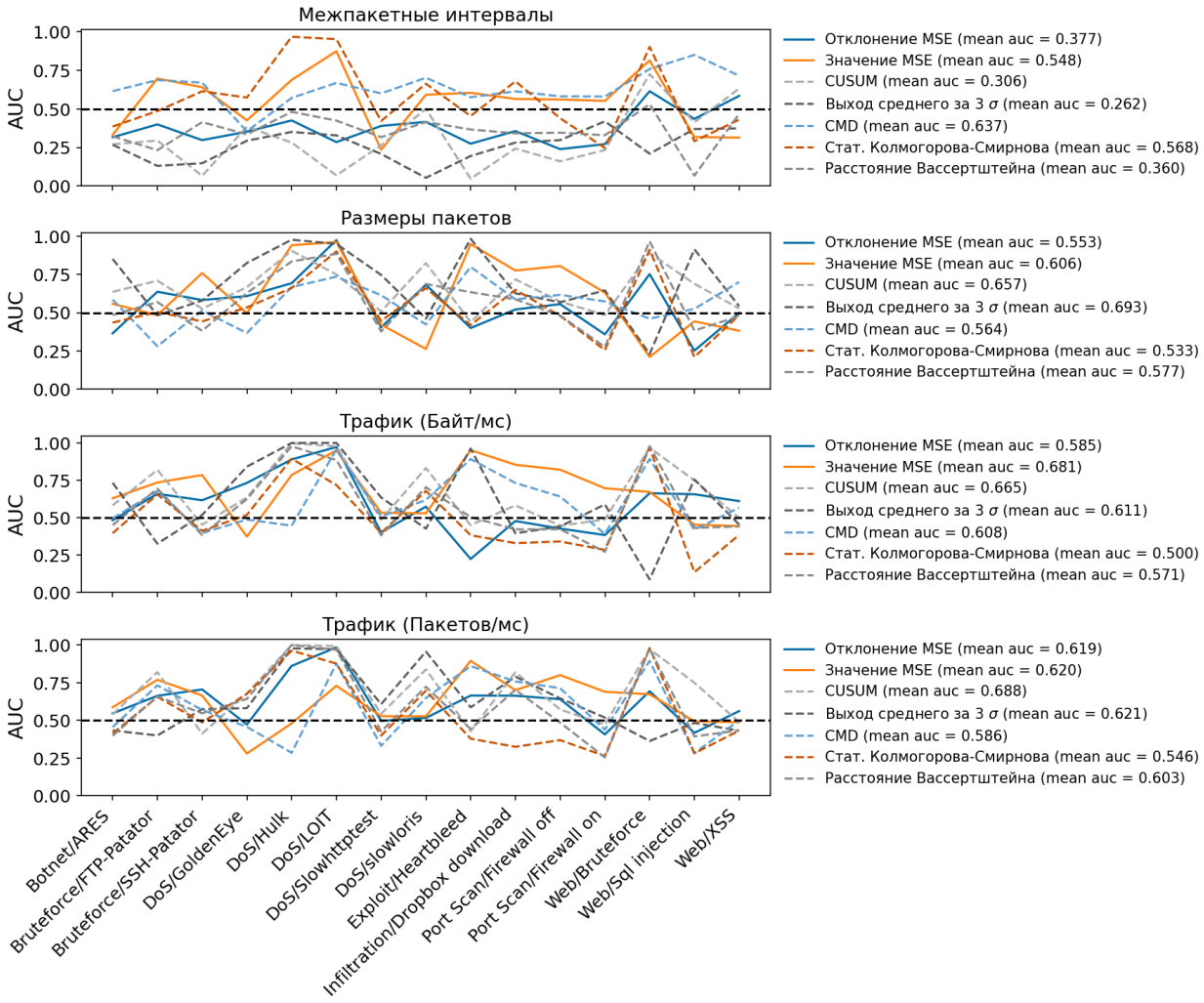


Рисунок 4.9 – Сравнение AUC для различных алгоритмов

Метод на основе отклонения ошибки дает наилучшие результаты при применении к последовательности межпакетных интервалов, позволяя обнаруживать брутфорс, сканирование портов и атаки внедрения. В то же время, для других последовательностей он дает невысокие результаты, не позволяя обнаруживать даже DoS-атаки, направленные на исчерпание физических ресурсов сети, с которыми справляются почти все остальные алгоритмы. Метод на основе значения ошибки позволяет получить наибольшие значения AUC, превышающие значения для других методов, при обнаружении атак внедрения и сканирования портов.

Таким образом, использование среднеквадратической ошибки фильтрации случайной последовательности, выделенной из наблюдаемого трафика, в качестве бинарного классификатора аномалий позволяет получить

значения AUC до 0,8 и 0,95 соответственно при рассмотрении отклонения и значения ошибки для отдельных видов атак. Разработанные алгоритмы могут обнаруживать только те виды атак, которые приводят к изменению статистических характеристик рассматриваемой последовательности трафика.

4.2.3. Ошибка фильтрации как дополнительный признак в алгоритмах машинного обучения

При использовании методов машинного обучения как правило рассматривается несколько признаков в совокупности [99, 139]. Разработанные алгоритмы обнаружения аномалий на основе отклонения и значения среднеквадратической ошибки фильтрации позволяют получить значения MSE, которые можно использовать в качестве дополнительных признаков. Добавление новых признаков, несущих дополнительную информацию, может улучшить качество классификации.

В работе [39] рассматривается трафик датасета MAWI, собранный 7 декабря 2019 года, в виде отдельных потоков. В качестве «нормального» трафика принимаются все двунаправленные потоки узла с адресом 202.171.168.50, а в качестве «аномального» – потоки узла с адресом 202.4.27.109. Используются следующие представления трафика:

- **STATS** – статистические характеристики потока: длительность, количество пакетов и байт в секунду, характеристики размеров пакетов (среднее, СКО, квантили распределения, минимальное и максимальное значения);
- **SIZES** – размеры пакетов в байтах;
- **IAT** – интервалы между поступлениями пакетов в секундах;
- **SAMP-NUM** – временной ряд в виде количества пакетов;
- **SAMP-SIZE** – временной ряд в виде размеров пакетов в байтах.

Каждый поток представляется как вектор признаков фиксированной длины:

$$F_i = \{F_1, F_2, \dots, F_N\}. \quad (4.7)$$

Чтобы получить одинаковый размер вектора N, длина ограничивается по 90-му перцентилю всех длин потоков, для всех представлений кроме **STATS**, так как оно и так имеет фиксированный размер по количеству характеристик.

Для классификации трафика используются методы обучения без учителя: *модель гауссовских смесей* (GMM), *ядерная оценка плотности* (KDE), *изоляционный лес* (IF), *метод главных компонент* (PCA), *автокодировщик* (AE) и *одноклассовый метод опорных векторов* (OCSVM).

Добавление размеров пакетов и отдельных полей заголовков TCP пакетов увеличивает эффективность алгоритмов классификации, выраженную в значении AUC [39]. Аналогично к последовательностям, выделенным из трафика, можно добавить признаки, соответствующие отклонению ошибки от эталонного значения и минимальной MSE, полученные при применении алгоритмов обнаружения аномалий на основе отклонения и значения среднеквадратической ошибки фильтрации.

Для последовательностей интервалов между поступлениями пакетов X_n, размеров пакетов Y_n, временных рядов со значениями, представляющими суммарный объем трафика V_t и количество пакетов N_t за интервал времени t, вычисляются отклонение нормализованной среднеквадратической ошибки фильтрации (3.37) (NMSE) и значение минимальной среднеквадратической ошибки фильтрации (3.19) (MMSE). В качестве модели легитимного трафика принимается усредненное значение последовательности для всех потоков «нормального» узла. Для представлений IAT, SIZES, SAMP-NUM и SAMP-SIZE модифицированные векторы признаков определяются как:

$$F_{i\,NMSE} = \{F_1, F_2, \dots, F_N, F_{NMSE}\}, \tag{4.8}$$

$$F_{i\,MMSE} = \{F_1, F_2, \dots, F_N, F_{MMSE}\}, \tag{4.9}$$

$$F_{i\,BOTH} = \{F_1, F_2, \dots, F_N, F_{NMSE}, F_{MMSE}\}, \tag{4.10}$$

где F_{NMSE} – отклонение минимальной ошибки фильтрации, F_{MMSE} – значение минимальной ошибки фильтрации.

Для вектора признаков, соответствующих статистическим характеристикам потоков, добавляются все значения отклонений от эталонной NMSE и минимальной NMSE, вычисленные для последовательностей X_n, Y_n, V_t и N_t. Размер вектора признаков в данном случае увеличивается на 4 или 8.

Обучение моделей производится на выборке, содержащий признаки только нормальных потоков. Размер обучающей и тестовой выборки приблизительно одинаковы, но в тестовой содержится одинаковое количество нормальных и аномальных потоков. Значения всех исходных признаков нормализуются относительно их среднего и дисперсии, значения ошибок считаются уже нормализованными, поскольку используется NMSE. Полученные в результате значения AUC и его прирост, полученный при добавлении новых признаков для последовательностей, представлены в Таблице 4.4.

Таблица 4.4 – Прирост AUC для последовательностей

Последовательность		Модель					
		OCSVM	PCA	GMM	IF	KDE	Среднее
IAT	AUC	0,64	0,67	0,68	0,63	0,64	0,65
	ΔNMSE, %	1,83	0,22	-0,98	7,34	2,05	2,02
	ΔMMSE, %	-6,35	-3,76	-7,13	1,90	1,10	-2,94
	ΔBOTH, %	-5,98	-4,30	-7,37	1,82	0,73	-3,12
SIZE	AUC	0,45	0,49	0,57	0,68	0,68	0,58
	ΔNMSE, %	0,50	-0,30	2,87	1,42	0,00	0,93
	ΔMMSE, %	2,57	0,07	9,28	2,85	0,43	3,04
	ΔBOTH, %	3,99	0,06	10,85	1,67	0,46	3,30
SAMP_NUM	AUC	0,56	0,53	0,52	0,50	0,56	0,53
	ΔNMSE, %	-0,75	0,38	3,22	19,38	-4,19	3,28
	ΔMMSE, %	3,93	1,43	2,76	10,59	3,80	4,42
	ΔBOTH, %	4,96	1,56	3,54	10,08	0,50	4,02
SAMP_SIZE	AUC	0,55	0,53	0,52	0,50	0,55	0,53
	ΔNMSE, %	-1,07	-0,84	1,00	21,79	-4,68	2,92
	ΔMMSE, %	6,94	1,37	0,25	11,43	4,86	4,91
	ΔBOTH, %	8,08	0,08	1,33	10,21	2,35	4,35

Производительность различных классификаторов при добавлении новых признаков существенно различается для разных представлений

трафика. В среднем прирост положительный, максимум (4,91%) наблюдается для временного ряда в виде суммарного объема трафика в байтах. Для последовательности интервалов времени между пакетами добавление признака в виде значения минимальной среднеквадратической ошибки приводит к уменьшению AUC, что может быть вызвано тем, что «нормальный» и «аномальный» узлы генерируют почти одинаковый трафик, значения минимальной MSE получаются почти одинаковыми, и по полному вектору признаков различить их становится, наоборот, труднее.

Значения и прирост AUC для вектора признаков на основе статистических характеристик представлены в Таблице 4.5

Таблица 4.5 – Прирост AUC для статистических характеристик

	Модель					
Значение	OCSVM	PCA	GMM	IF	KDE	Среднее
AUC	0,46	0,57	0,55	0,67	0,68	0,59
ΔNMSE, %	4,51	11,85	5,31	7,41	2,98	6,39
ΔMMSE, %	30,52	1,24	19,58	-0,77	2,40	9,09
ΔBOTH, %	31,76	12,64	22,22	7,81	2,88	14,06

Для данного вектора признаков прирост более значительный. Значения, полученные для каждого алгоритма, в среднем увеличивают метрику AUC, причем добавление обоих признаков приводит к приросту, практически равному сумме прироста для признаков по отдельности.

Как было отмечено в первой главе, размеры потоков могут быть недостаточными для вычисления достоверных оценок статистических характеристик, в данном случае АКФ. Тем не менее, добавление новых признаков на основе значений, получаемых в результате применения разработанных алгоритмов, в среднем приводит к увеличению качества классификации трафика. Также, поскольку рассматриваемые трафиковые последовательности коррелированы между собой, в дальнейшем можно рассмотреть возможность применения метода главных компонент для уменьшения размерности вектора дополнительных признаков.

4.3. Выводы по главе 4

Представлены результаты моделирования обнаружения аномалий для различных сценариев. Исследовано влияние формы АКФ на эффективность обнаружения аномалий. Установлено, что при любой форме АКФ полезного трафика и аномалии, алгоритм позволяет получить статистически значимые результаты отклонения NMSE от эталонного значения.

Проведено моделирование при различных значениях шума наблюдений, используемого на этапе обучения модели. Установлено, что обнаружение аномалий на основе сравнения значения NMSE с граничными значениями достоверно производится при отношениях сигнал/шум от 0,01 до 100.

Проведено исследование эффективности алгоритма при применении к реальному сетевому трафику из архива MAWI и из датасета CIC-IDS2017. Установлено, что использование среднеквадратической ошибки фильтрации в качестве бинарного классификатора аномалий позволяет получить значения AUC до 0,8 и 0,95 соответственно при рассмотрении отклонения и значения ошибки для брутфорс атак, сканирования портов, DoS-атак и атак внедрения.

Предложено использование значений NMSE, получаемых в результате применения алгоритмов обнаружения аномалий, в качестве дополнительных признаков для методов машинного обучения. Рассматриваются различные методы обучения без учителя: Гауссовские смеси распределений, ядерная оценка плотности, изоляционный лес, анализ главных компонент и одноклассовый метод опорных векторов. Рассматриваются потоки трафика. Из сетевых потоков выделяются признаки для различных представлений трафика, на части образцов нормального трафика производится обучение, а затем классификация остальных образцов.

Производительность различных моделей при добавлении новых признаков существенно различается для разных представлений трафика. Добавление новых признаков увеличивает значение AUC в среднем на 2,3%. Для набора признаков на основе статистических характеристик потоков трафика увеличение AUC составляет от 6,39% до 14,06%.

Заключение

В диссертационной работе проведено научное исследование по повышению защищенности телекоммуникационных систем за счет повышения эффективности алгоритмов обнаружения аномалий в сетевом трафике, которые могут быть вызваны проводимыми злоумышленником атаками.

В первой главе рассмотрены основные методы анализа трафика, включая DPI и статистический анализ. Трафик рассматривается как случайная последовательность межпакетных интервалов и размеров пакетов, или как временной ряд, представляющий количество пакетов или суммарный объем пакетов (в байтах) в единицу времени. Вычислены типичные значения статистических характеристик для различных представлений трафика для штатного режима работы и под воздействием атак. Разработан алгоритм определения численных индикаторов атак на основе метода «случайного леса» и установлены пороговые значения для различных статистических характеристик трафика на данных датасета CIC-IDS2017. Показано, что изменение АКФ трафика является характерным признаком ряда сетевых атак из этого набора данных.

Во второй главе рассмотрены методы моделирования самоподобного трафика и случайных процессов с заданными параметрами, а также методы моделирования DoS-атак и основные признаки их выявления. Проведено моделирование трафика с использованием моделей PPBP и ON/OFF источников, исследовано влияние параметра скорости отдельного источника на полученные результаты. Увеличение скорости приводит к снижению коррелированности результирующего трафика. Проведено моделирование смеси трафика DoS-атаки и легитимного трафика. Добавление трафика атаки приводит к изменению формы АКФ. Разработан метод моделирования реализаций случайного процесса с одновременно заданной АКФ и распределением Вейбулла, основанный на применении копулы ФГМ, позволяющий снизить евклидово расстояние между заданной и

эмпирической АКФ в среднем на 55%, и уменьшить значение критерия согласия Колмогорова-Смирнова на 34% по сравнению с известными численными методами.

В третьей главе представлены разработанные методы обнаружения аномалий на основе минимальной MSE фильтра Винера, применяемого к случайному процессу, выделяемому из трафика. Суть одного из методов заключается в вычислении эталонного значения минимальной MSE для трафика в штатном режиме функционирования системы с учетом шума наблюдений, и сравнении вычисляемой во время работы MSE с эталоном. Суть другого метода заключается в вычислении минимальной MSE для текущего трафика. Рассмотрены варианты получения пороговых значений на основе свойств нормированной MSE и собственных чисел матрицы корреляции легитимного трафика. Разработан алгоритм, реализующий эти методы, дано описание его шагов и особенностей предобработки трафика, которые необходимо учитывать, описаны ограничения, связанные с применимостью фильтра Винера только к стационарным процессам, необходимостью обновления моделей нормального трафика при изменении топологии сети или характера её использования, а также возможностью обнаружения только сетевых атак, влияющих на статистические характеристики трафика. Проведен сравнительный анализ различных метрик расстояния для сравнения АКФ, которые могут использоваться в алгоритме.

В четвертой главе проводится тестирование разработанных методов на данных смоделированного и реального трафика. Установлено, что разработанные методы позволяют обнаруживать аномалии, вызванные сетевыми атаками, которые приводят к изменению статистических характеристик трафика. Задаваемый уровень шума наблюдений не приводит к значительному снижению эффективности обнаружения аномалий для смоделированного трафика. Использование отклонения NMSE и значения MMSE в качестве бинарного классификатора позволяет получить значения AUC при классификации образцов трафика до 0,80 и 0,95 соответственно для

отдельных видов атак. Рассмотрено применение получаемых значений MSE в методах машинного обучения и установлено, что их добавление к вектору признаков статистических характеристик, вычисленных для потоков, позволяет увеличить значения AUC моделей машинного обучения без учителя в среднем от 6,39% до 14,06% в зависимости от модели.

Основные выводы и результаты диссертационной работы:

1. Проведен анализ статистических характеристик реального сетевого трафика, сгенерированного в локальной сети и взятого из открытых наборов данных. Разработан алгоритм определения численных индикаторов атак и установлено, что воздействие сетевых атак на трафик приводит к изменению АКФ и вероятностного распределения, из чего следует возможность их обнаружения на основе рассмотрения данных характеристик.

2. Проведено моделирование самоподобного сетевого трафика и DoS-атак, исследованы различные варианты объединения трафика и свойства полученной в результате смеси. Разработан метод моделирования случайных процессов с распределением Вейбулла, представляющих легитимный трафик, который позволяет улучшить точность воспроизведения заданных статистических характеристик по сравнению с известными численными методами.

3. Разработаны методы обнаружения аномалий на основе оптимального линейного фильтра Колмогорова-Винера и реализующие их алгоритмы, которые позволяют определить аномалии на основе несовпадения характеристик наблюдаемого в данный момент трафика с легитимным.

4. Разработан механизм формирования признаков для моделей машинного обучения, предназначенных для обнаружения сетевых атак, на основе минимального значения среднеквадратической ошибки фильтрации и ее отклонения от эталонного значения.

5. Проведена оценка эффективности разработанных методов и алгоритмов на смоделированном и реальном трафике в различных условиях.

Разработанные методы позволили повысить эффективность обнаружения сетевых атак по сравнению с существующими подходами в отдельных случаях, а добавление в вектор признаков для моделей машинного обучения без учителя новых параметров, основанных на вычислении MSE с использованием разработанных методов, позволило увеличить точность классификации аномалий, за счет чего была достигнута цель исследования.

Предложенный алгоритм позволяет эффективно обнаруживать аномалии в сетевом трафике за счет анализа АКФ трафика и применения оптимального линейного фильтра Колмогорова–Винера, что подтверждено экспериментально на синтетических и реальных данных. Он может использоваться для предварительного выделения аномального участка трафика с целью его дальнейшей классификации и определения конкретного типа аномалии или атаки.

Результаты диссертационной работы внедрены в ООО «Идентификация» и в учебный процесс кафедры информационной безопасности ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики». Работа представляет собой ценный вклад в область анализа сетевого трафика и обнаружения аномалий, и её результаты могут быть использованы для повышения безопасности телекоммуникационных сетей путем разработки и внедрения новых методов и технологий, направленных на предотвращение, обнаружение и реагирование на потенциальные угрозы и атаки.

Перспективы дальнейшей разработки темы включают в себя исследование характеристик статистической взаимосвязи отсчетов трафика выше второго порядка, называемых *кумулянтами*. Для алгоритма определения численных индикаторов атак целесообразно учитывать порядок порогов в решающих деревьях. Для моделирования случайных последовательностей помимо ФГМ могут быть рассмотрены другие виды копул, которые позволяют выразить связь через коэффициент корреляции. Разработанные методы могут быть расширены для обнаружения не только

наличия аномалии, но и определение её типа, для чего могут использоваться, например, несколько фильтров для каждого известного типа аномалии. Также, текущий подход рассматривает аномалии только в виде аддитивного процесса, поэтому перспективной задачей является исследование других моделей аномалий.

Список сокращений

АКФ: Автокорреляционная функция

БГШ: Белый гауссовский шум

ВКФ: Взаимокорреляционная функция

ВПО: Вредоносное программное обеспечение

ДВЗ: Долговременная зависимость

ИБ: Информационная безопасность

ИХ: Импульсная характеристика

МСЭ: Межсетевой экран

ОС: Операционная система

СДУ: Стохастическое дифференциальное уравнение

СКО: Среднеквадратическое отклонение

СМО: Система массового обслуживания

СОВ: Система обнаружения вторжений

ФГМ: (Копула) Фарли-Гумбеля-Моргенштерна

ЧХ: Частотная характеристика

ARIMA: Auto-Regressive Integrated Moving Average, интегрированная модель авторегрессии и скользящего среднего

AUC: Area Under Curve, площадь под кривой

DPI: Deep Packet Inspection, глубокий анализ пакетов

IAT: Inter-arrival time, интервал между поступлением пакетов

MAWI: Measurement and Analysis on the WIDE Internet, измерение и анализ в сети Интернет WIDE

MSE: Mean Square Error, среднеквадратическая ошибка

MMSE: Minimum Mean Square Error, минимальная среднеквадратическая ошибка

NMSE: Normalized Mean Square Error, нормализованная среднеквадратическая ошибка

NTA: Network Traffic Analysis, анализ сетевого трафика

NDR: Network Detection & Response, сетевое обнаружение и реагирование

PCAP: Packet CAPture, (файл) захвата пакетов

PPBP: Poisson Pareto Burst Process, процесс всплесков Пуассона-Парето

ROC: Receiver Operator Characteristic, рабочая характеристика приёмника

SIEM: Security Information and Event Management, управление информацией и событиями безопасности

SQL: Structured Query Language, структурированный язык запросов

VOQ: Virtual Output Queue, виртуальная очередь вывода

QoS: Quality of Service, качество обслуживания

XDR: Extended Detection & Response, расширенное обнаружение и реагирование

XSS: Cross-Site Scripting, межсайтовый скриптинг

Список литературы

1. *Вяткина А.* Актуальные киберугрозы: I–II кварталы 2025 года [Электронный ресурс] // А. Вяткина, А. Осипова. – Режим доступа: https://ptsecurity.com/research/analytics/aktual-nye-kiberugrozy-i-ii-kvartaly-2025-goda/ (Дата обращения: 19.12.2025)

2. DDoS-атаки 2025: статистика за I полугодие | StormWall [Электронный ресурс]. – Режим доступа: https://stormwall.pro/resources/blog/ddos-ataki-2025-1-polugodie (Дата обращения: 19.12.2025)

3. *Makridakis S.* Statistical and Machine Learning forecasting methods: Concerns and ways forward / S. Makridakis, E. Spiliotis, V. Assimakopoulos // PLoS ONE. – 2018. – Т. 13. – № 3, DOI: 10.1371/journal.pone.0194889

4. *Denning D.E.* An Intrusion-Detection Model / D.E. Denning // IEEE Transactions on Software Engineering. – 1987. – Т. SE-13. – № 2. – С. 222-232, DOI: 10.1109/TSE.1987.232894

5. *Карташевский В.Г.* Основы теории массового обслуживания. Учебник для вузов / В.Г. Карташевский. – Москва: Горячая линия - Телеком, 2015. – 130 с.

6. *Смирнов Г.Е.* Анализ стандартов и методик тестирования на проникновение / Г.Е. Смирнов, С.И. Макаренко // Системы управления, связи и безопасности. – 2020. – № 4. – С. 44-72, DOI: 10.24411/2410-9916-2020-10402

7. *Гетьман А.И.* Обзор задач и методов их решения в области классификации сетевого трафика / А.И. Гетьман [и др.] // Труды Института системного программирования РАН. – 2017. – Т. 29. – № 3, DOI: 10.15514/ISPRAS-2017-29(3)-8

8. *Поздняк И.С.* Выявление DoS-атак с помощью анализа статистических характеристик трафика / И.С. Поздняк, А.И. Плаван // Инфокоммуникационные технологии. – 2021. – Т. 19. – № 1. – С. 73-80, DOI: 10.18469/ikt.2021.19.1.10

9. *Беленькая (Росоховатская) М.Н.* Обзор методов анализа сетевого трафика средствами DPI / М.Н. Беленькая (Росоховатская) [и др.] // Труды Северо-Кавказского Филиала Московского Технического Университета Связи И Информатики. – 2018. – № 1. – С. 15-20

10. *Абдулин А.А.* Исследование программных решений для обеспечения информационной безопасности промышленных сетей автоматизированных систем управления технологическими процессами / А.А. Абдулин, А.Н. Соколов // Вестник УрФО. Безопасность в информационной сфере. – 2021. – № 1 (39). – С. 43-53, DOI: 10.14529/secur210106

11. *Fontugne R.* MAWILab: Combining Diverse Anomaly Detectors for Automated Anomaly Labeling and Performance Benchmarking / R. Fontugne [и др.] // Proceedings of the 6th International Conference. – Philadelphia, Pennsylvania: ACM, 2010. – MAWILab. – С. 1-12, DOI: 10.1145/1921168.1921179

12. *Гетьман А.И.* Анализ сетевого трафика в режиме реального времени: обзор прикладных задач, подходов и решений / А.И. Гетьман, Е.Ф. Евстропов, Ю.В. Маркин // Препринт ИСП РАН. – 2015. – Т. 28. – Анализ сетевого трафика в режиме реального времени. – С. 1-52

13. *Никитин А.А.* Фильтр Колмогорова-Винера и его применение / А.А. Никитин, А.В. Петров // Теоретические основы обработки геофизической информации: учебное пособие. – Москва, 2008. – С. 63-68

14. *Anderson B.* Detecting Encrypted Malware Traffic (Without Decryption) [Электронный ресурс] // B. Anderson. – Режим доступа: https://blogs.cisco.com/security/detecting-encrypted-malware-traffic-without-decryption (Дата обращения: 25.11.2023)

15. *Афанасьев В.Н.* Анализ временных рядов и прогнозирование / В.Н. Афанасьев, М.М. Юзбашев. – М.: Финансы и статистика, 2001. – 228 с.

16. *Barford P.* A signal analysis of network traffic anomalies / P. Barford [и др.] // IMW ’02: Proceedings of the second ACM SIGCOMM Workshop on

Internet measurment. – Marseille, France: ACM Press, 2002. – С. 71-82, DOI: 10.1145/637201.637210

17. *Фаткиева Р.Р.* Модель обнаружения атак на основе анализа временных рядов / Р.Р. Фаткиева // Труды СПИИРАН. – 2012. – № 2 (21). – С. 71-79

18. *Карташевский И.В.* Разработка и исследование методов анализа качества обслуживания коррелированного трафика в телекоммуникационных сетях : дис. ... док. техн. наук: 05.12.13 / И.В. Карташевский. – Самара: ПГУТИ, 2020. – 288 с.

19. *Мещеряков М.В.* Исследование влияния метода сжатия цифрового видеопотока систем видеонаблюдения на фрактальные свойства передаваемого в сети пакетного трафика / М.В. Мещеряков, В.Г. Карташевский // T-Comm: Телекоммуникации и Транспорт. – 2015. – Т. 9. – № 10. – С. 17-21

20. *Leland W.E.* On the self-similar nature of Ethernet traffic (extended version) / W.E. Leland [и др.] // IEEE/ACM Transactions on Networking. – 1994. – Т. 2. – № 1. – С. 1-15, DOI: 10.1109/90.282603

21. *Лебедев Н.А.* Оценка степени самоподобия современного интернет-трафика и анализ полученных экспериментальным путём данных / Н.А. Лебедев, С.Д. Ерохин // Телекоммуникации и информационные технологии. – 2017. – Т. 4. – № 1. – С. 79-83

22. *Петров В.В.* То, что вы хотели знать о самоподобном телетрафике, но стеснялись спросить [Электронный ресурс] // В.В. Петров. – Режим доступа: http://pi.314159.ru/petroff1.pdf (Дата обращения: 05.06.2022)

23. *Strelkovskaya I.* Modeling of Self-similar Traffic / I. Strelkovskaya, I. Solovskaya, N. Severin // Proceedings of the 4th International Conference on Applied Innovations in IT. – Koethen, Germany: Anhalt University of Applied Sciences, 2016. – Т. 4. – С. 61-64

24. *Треногин Н.Г.* Свойства фрактального трафика при прохождении системы массового обслуживания с очередью / Н.Г. Треногин, М.Н. Петров,

Д.Е. Соколов // Сибирский аэрокосмический журнал. – 2017. – Т. 18. – № 1. – С. 105-110

25. *Shuang D.* Empirical model of WWW document arrivals at access link / D. Shuang // Proceedings of ICC/SUPERCOMM ’96 - International Conference on Communications. – Dallas, TX, USA: IEEE, 1996. – Т. 3. – С. 1797-1802, DOI: 10.1109/ICC.1996.535600

26. *Li M.* Long-range dependence and self-similarity of teletraffic with different protocols at the large time scale of day in the duration of 12 years: Autocorrelation modeling / M. Li // Physica Scripta. – 2020. – Т. 95. – № 6. – С. 065222, DOI: 10.1088/1402-4896/ab82c4

27. *Шелухин О.И.* Причины самоподобия телетрафика и методы оценки показателя Херста / О.И. Шелухин // Электротехнические и информационные комплексы и системы. – 2007. – Т. 3. – № 1. – С. 1

28. *Crovella M.E.* Self-similarity in World Wide Web Traffic: Evidence and Possible Causes / M.E. Crovella, A. Bestavros // IEEE/ACM Transactions on Networking. – 1997. – Т. 5. – № 6. – С. 835-846

29. *Horn G.* An empirical comparison of generators for self similar simulated traffic / G. Horn [и др.] // Performance Evaluation. – 2007. – Т. 64. – № 2. – С. 162-190, DOI: 10.1016/j.peva.2006.06.005

30. *Taqqu M.S.* Proof of a fundamental result in self-similar traffic modeling / M.S. Taqqu, W. Willinger, R. Sherman // ACM SIGCOMM Computer Communication Review. – 1997. – Т. 27. – № 2. – С. 5-23

31. *Басараб М.А.* Обнаружение аномалий в информационных процессах на основе мультифрактального анализа / М.А. Басараб, И.С. Строганов // Вопросы кибербезопасности. – 2014. – № 4 (7). – С. 30-40

32. *Губарева О.Ю.* Разработка методики оценки рисков информационной безопасности корпоративных телекоммуникационных сетей : дис. ... канд. техн. наук: 05.12.13 / О.Ю. Губарева. – ПГУТИ, 2018. – 175 с.

33. *Karagiannis T.* Long-range dependence ten years of Internet traffic modeling / T. Karagiannis, M. Molle, M. Faloutsos // IEEE Internet Computing. – 2004. – Т. 8. – № 5. – С. 57-64, DOI: 10.1109/MIC.2004.46

34. *Li M.* Convergence of Sample Autocorrelation of Long-Range Dependent Traffic / M. Li, W. Zhao // Mathematical Problems in Engineering. – 2013. – Т. 2013. – С. 1-7, DOI: 10.1155/2013/725730

35. MAWI Working Group Traffic Archive [Электронный ресурс]. – Режим доступа: http://mawi.wide.ad.jp/mawi/ (Дата обращения: 05.02.2023)

36. *Фаткиева Р.Р.* Корреляционный анализ аномального сетевого трафика / Р.Р. Фаткиева // Труды СПИИРАН. – 2012. – № 4 (23). – С. 93-99

37. *Плаван А.И.* Сравнительный анализ статистических характеристик DDoS-атак и нормального трафика / А.И. Плаван, В.Г. Карташевский, И.С. Поздняк // Актуальные проблемы науки и техники: Материалы I Международной научно-технической конференции. – Сарапул: Издательство УИР ИжГТУ имени М. Т. Калашникова, 20–22 мая 2021 г. – С. 551-555

38. *Wu H.* Investigation on the IP Flow Inter-Arrival Time in Large-Scale Network / H. Wu, M. Zhou, J. Gong // 2007 International Conference on Wireless Communications, Networking and Mobile Computing. – Shanghai, China: IEEE, 2007. – С. 1925-1928, DOI: 10.1109/WICOM.2007.482

39. *Yang K.* Feature Extraction for Novelty Detection in Network Traffic / K. Yang, S. Kpotufe, N. Feamster. – arXiv, 2021.

40. *Callegari C.* On the proper choice of datasets and traffic features for real-time anomaly detection / C. Callegari, S. Giordano, M. Pagano // Journal of Physics: Conference Series. – 2021. – Т. 2091. – № 1. – С. 012001, DOI: 10.1088/1742-6596/2091/1/012001

41. *Tavallaee M.* A detailed analysis of the KDD CUP 99 data set / M. Tavallaee [и др.] // 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications. – Ottawa, ON, Canada: IEEE, 2009. – С. 1-6, DOI: 10.1109/CISDA.2009.5356528

42. *Protić D.* Review of KDD Cup ’99, NSL-KDD and Kyoto 2006+ datasets / D. Protić // Vojnotehnicki glasnik. – 2018. – Т. 66. – № 3. – С. 580-596, DOI: 10.5937/vojtehg66-16670

43. *Зуев В.Н.* Обнаружение аномалий сетевого трафика методом глубокого обучения / В.Н. Зуев // Программные продукты и системы. – 2021. – Т. 34. – № 1. – С. 91-97

44. *Vasilyev V.I.* Hybrid Intrusion Detection System with the Use of a Classifiers Committee / V.I. Vasilyev [и др.] // Modeling, Optimization and Information Technology. – 2022. – Т. 10. – № 4(39). – С. 20-21, DOI: 10.26102/2310-6018/2022.39.4.020

45. *Чаругин В.В.* Анализ и формирование наборов данных сетевого трафика для обнаружения компьютерных атак / В.В. Чаругин, А.Н. Чесалин // International Journal of Open Information Technologies. – 2023. – Т. 11. – № 6. – С. 100-106

46. *Souhail Et. Al. M.* Network Based Intrusion Detection Using the UNSW-NB15 Dataset / M. Souhail Et. Al. // International Journal of Computing and Digital Systems. – 2019. – Т. 8. – № 5. – С. 477-487, DOI: 10.12785/ijcds/080505

47. *Асяев Г.Д.* Модель многоклассовой классификации атак в АСУ ТП в условиях несбалансированной обучающей выборки / Г.Д. Асяев, А.Н. Соколов // Материалы четырнадцатой научной конференции аспирантов и докторантов «Научный поиск». – Челябинск: Издательский центр ЮУрГУ, 2022. – С. 96-103

48. *Shushlevska M.* Anomaly Detection with Various Machine Learning Classification Techniques over UNSW-NB15 Dataset / M. Shushlevska [и др.] // Proceedings of the 10th International Conference on Applied Innovations in IT. – Koethen, Germany: Anhalt University of Applied Sciences, 2022. – С. 21-27

49. *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

50. *Васильев В.И.* Распределенная система обнаружения сетевых атак на основе федеративного трансферного обучения / В.И. Васильев [и др.] // Вопросы кибербезопасности. – 2024. – № 6 (64). – С. 117-129, DOI: 10.21681/2311-3456-2024-6-117-129

51. *Гетьман А.И.* Применение глубокого обучения для обнаружения компьютерных атак в сетевом трафике / А.И. Гетьман [и др.] // Труды Института системного программирования РАН. – 2023. – Т. 35. – № 4. – С. 65-92, DOI: 10.15514/ISPRAS-2023-35(4)-3

52. IDS 2017 | Datasets | Research | Canadian Institute for Cybersecurity | UNB [Электронный ресурс]. – Режим доступа: https://www.unb.ca/cic/datasets/ids-2017.html (Дата обращения: 05.02.2023)

53. *Jurkiewicz P.* Flow length and size distributions in campus Internet traffic / P. Jurkiewicz, G. Rzym, P. Boryło // Computer Communications. – 2021. – Т. 167. – С. 15-30, DOI: 10.1016/j.comcom.2020.12.016

54. *Garcia Cordero C.* On Generating Network Traffic Datasets with Synthetic Attacks for Intrusion Detection / C. Garcia Cordero [и др.] // ACM Transactions on Privacy and Security. – 2021. – Т. 24. – № 2. – С. 1-39, DOI: 10.1145/3424155

55. *Поздняк И.С.* Принципы обработки набора данных, содержащего атаки разных видов / И.С. Поздняк // Материалы Всероссийской научно-технической конференции «Актуальные проблемы радиоэлектроники и телекоммуникаций». – Самара: ООО «Артель», 25–28 апреля 2023 г. – С. 172-174

56. *Breiman L.* Random Forests / L. Breiman // Machine Learning. – 2001. – Т. 45. – № 1. – С. 5-32, DOI: 10.1023/A:1010933404324

57. *Плаван А.И.* Алгоритм определения численных индикаторов аномалий трафика на основе модели случайного леса / А.И. Плаван //

Инфокоммуникационные технологии. – 2026. – Т. 24. – № 1 (93). – С. 26-32, DOI: 10.18469/ikt.2026.24.1.03

58. *Janitza S.* On the overestimation of random forest's out-of-bag error / S. Janitza, R. Hornung // PLOS ONE. – 2018. – Т. 13. – № 8. – С. e0201904, DOI: 10.1371/journal.pone.0201904

59. *Gagunashvili N.* Weighted histograms [Электронный ресурс] // N. Gagunashvili. – Режим доступа: https://indico.cern.ch/event/682907/contributions/2798549/attachments/1565125/2466041/Goodness_pres.pdf (Дата обращения: 01.12.2025)

60. Приказ ФСТЭК России от 11 февраля 2013 г. N 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [Электронный ресурс]. – Режим доступа: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17 (Дата обращения: 25.09.2024)

61. *Шелухин О.И.* Мультифракталы. Инфокоммуникационные приложения// Мультифракталы / О.И. Шелухин. – М.: Горячая линия - Телеком, 2011. – 576 с.

62. *Zukerman M.* Introduction to Queueing Theory and Stochastic Teletraffic Models / M. Zukerman. – arXiv, 2022. – 295 с.

63. *Шелухин О.И.* Многоуровневая ON/OFF модель Интернет-трафика корпоративной сети спутниковой связи / О.И. Шелухин, Д.А. Лукьянцев // Электротехнические и информационные комплексы и системы. – 2006. – Т. 2. – № 2. – С. 14

64. *Благов А.В.* Модификации моделей типа «входная M/G/∞» и «On-Off сточники» для имитационного моделирования самоподобного телекоммуникационного трафика / А.В. Благов, А.Ю. Привалов // Труды МАИ. – 2010. – № 39. – С. 15

65. *Привалов А.Ю.* Об использовании некоторых моделей самоподобного сетевого трафика в имитационном моделировании / А.Ю.

Привалов, А.В. Благов // Матем. моделирование. – 2011. – Т. 23. – № 7. – С. 114-128

66. *Zukerman M.* Internet traffic modeling and future technology implications / M. Zukerman, T.D. Neame, R.G. Addie // Proceedings of IEEE INFOCOM 2003. – San Francisco, CA, USA: IEEE, 2003. – Т. 1. – С. 587-596, DOI: 10.1109/INFCOM.2003.1208709

67. *Sarvotham S.* Network and user driven alpha-beta on–off source model for network traffic / S. Sarvotham, R. Riedi, R. Baraniuk // Computer Networks. – 2005. – Т. 48. – № 3. – С. 335-350, DOI: 10.1016/j.comnet.2004.11.024

68. *Song Luo*. Realistic Internet Traffic Simulation Through Mixture Modeling and a Case Study / Song Luo, G.A. Marin // Proceedings of the Winter Simulation Conference, 2005. – Orlando, FL, USA: IEEE, 2005. – С. 2408-2416, DOI: 10.1109/WSC.2005.1574533

69. *Плаван А.И.* Моделирование самоподобного трафика с использованием модели Poisson-Pareto-Burst-Process в симуляторе ns-3 / А.И. Плаван // Материалы XXVII Международной научно-технической конференции «Современные средства связи». – Минск, Республика Беларусь: Белорусская государственная академия связи, 27–28 октября 2022 г. – Т. 1. – С. 197-199

70. *Naribole S.* Poisson Pareto Burst Process (PPBP) ns-3 traffic generator [Электронный ресурс] // S. Naribole. – Режим доступа: https://github.com/sharan-naribole/PPBP-ns3 (Дата обращения: 15.09.2022)

71. *Поздняк И.С.* Исследование трафика на наличие атак / И.С. Поздняк, В.Г. Карташевский, А.И. Плаван // Проблемы техники и технологий телекоммуникаций ПТиТТ-2020: Материалы XXII Международной научно-технической конференции. – Самара: ПГУТИ, 17–20 ноября 2020 г. – С. 206-207

72. *Карташевский В.Г.* Моделирование и анализ DDoS-атаки / В.Г. Карташевский, И.С. Поздняк, А.И. Плаван // Материалы XXVIII Российской научно-технической конференции профессорско-преподавательского состава,

научных сотрудников и аспирантов университета с приглашением ведущих ученых и специалистов родственных вузов и организаций. – Самара: ПГУТИ, 5–8 апреля 2021 г. – С. 63-64

73. *Плаван А.И.* Исследование корреляционных свойств сетевого трафика при воздействии DoS-атаки / А.И. Плаван // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: сборник материалов VI Всероссийской молодежной научно-практической конференции с международным участием. – Уфа: РИЦ УУНиТ, 19–20 мая 2023 г. – С. 105-108

74. Свидетельство о государственной регистрации программы для ЭВМ №2023664160. PcapConvert : №2023663148 : заявл. 21.06.2023 : опубл. 03.07.2023, Бюл. № 7 / А.И. Плаван. – 1 с.

75. *Вентцель Е.С.* Теория вероятностей: Учеб. для вузов. / Е.С. Вентцель. – 6-е изд. стер. – М.: Высш. шк., 1999. – 576 с.

76. Свидетельство о государственной регистрации программы для ЭВМ №2022614836. Программный комплекс «PcapStat» : №2022613421 : заявл. 09.03.2022 : опубл. 28.03.2022, Бюл. № 4 / А.И. Плаван. – 1 с.

77. *Карташевский В.Г.* Исследование статистических характеристик вредоносного трафика / В.Г. Карташевский, А.И. Плаван, И.С. Поздняк // Проблемы техники и технологий телекоммуникаций ПТиТТ-2021: Материалы XXIII Международной научно-технической конференции. – Самара: ПГУТИ, 23–26 ноября 2021 г. – С. 165-166

78. Свидетельство о государственной регистрации программы для ЭВМ №2024611818. PcapReplay : №2024611026 : заявл. 24.01.2024 : опубл. 24.01.2024, Бюл. № 2 / А.И. Плаван. – 1 с.

79. *Plavan A.I.* Statistical analysis of aggregated network traffic model from multiple on/off sources / A.I. Plavan, V.G. Kartashevsky, I.S. Pozdnyak // Proc. SPIE 12564, 2nd International Conference on Computer Applications for Management and Sustainable Development of Production and Industry (CMSD-II-

2022) / ред. A. Gibadullin, S. Sadullozoda. – Dushanbe, Tajikistan: SPIE, 21–23 декабря 2022 г. – Т. 12564. – С. 118-124, DOI: 10.1117/12.2669187

80. *Быков В.В.* Цифровое моделирование в статистической радиотехнике / В.В. Быков. – М.: Советское радио, 1971. – 328 с.

81. *Карташевский В.Г.* Статистический анализ агрегированной модели сетевого трафика / В.Г. Карташевский, А.И. Плаван, И.С. Поздняк // Материалы XXIX Российской научно-технической конференции профессорско-преподавательского состава, научных сотрудников и аспирантов университета с приглашением ведущих ученых и специалистов родственных вузов и организаций. – Самара: ПГУТИ, 22–25 марта 2022 г. – С. 58-59

82. *Плаван А.И.* Исследование влияния скорости on/off источника на характеристики моделируемого интернет-трафика / А.И. Плаван // Доклады 77-й всероссийской конференции «Радиоэлектронные устройства и системы для инфокоммуникационных технологий» посвящённой дню радио (РЭУС-2022). – М.: РНТОРЭС имени А.С. Попова, 8–10 июня 2022 г. – С. 102-105

83. *Cario M.C.* Modeling and Generating Random Vectors with Arbitrary Marginal Distributions and Correlation Matrix / M.C. Cario, B.L. Nelson. – Evanston, USA: Department of Industrial Engineering and Management Sciences Northwestern University, Evanston, 1997. – С. 19

84. *Лоу А.М.* Имитационное моделирование : Классика CS / А.М. Лоу, В.Д. Кельтон. – 3-е издание. – СПб: Питер; Киев; Издательская группа BHV, 2004. – 847 с.

85. *Crouse M.* Fast, exact synthesis of Gaussian and nonGaussian long-range-dependent processes / M. Crouse, R.G. Baraniuk // IEEE Transactions on Information Theory. – 1999

86. *Messerschmitt D.G.* Autocorrelation matrix eigenvalues and the power spectrum | EECS at UC Berkeley [Электронный ресурс] : Technical Report UCB/EECS-2006-90 // D.G. Messerschmitt. – Режим доступа:

https://www2.eecs.berkeley.edu/Pubs/TechRpts/2006/EECS-2006-90.html (Дата обращения: 11.03.2026)

87. *Szajnowski W.* The Generation of Correlated Weibull Clutter for Signal Detection Problems / W. Szajnowski // IEEE Transactions on Aerospace and Electronic Systems. – 1977. – Т. AES-13. – № 5. – С. 536-540, DOI: 10.1109/TAES.1977.308419

88. *Martin Bibby B.* Diffusion-type models with given marginal distribution and autocorrelation function / B. Martin Bibby, I. Michael Skovgaard, M. Sørensen // Bernoulli. – 2005. – Т. 11. – № 2. – С. 191-220, DOI: 10.3150/bj/1116340291

89. *Плаван А.И.* Применение копулы для моделирования случайных процессов с распределением Вейбулла и заданной автокорреляционной функцией / А.И. Плаван, В.Г. Карташевский // Известия Института инженерной физики. Серия: Информатика, вычислительная техника и управление. – 2026. – № 3 (81). – С. 47-52

90. *Balakrishnan N.* Continuous Bivariate Distributions / N. Balakrishnan. – 2nd ed. – New York, NY: Springer, 2009. – 1 с., DOI: 10.1007/b101765

91. *Карташевский И.В.* Обработка коррелированного трафика в сетях инфокоммуникаций / И.В. Карташевский. – М.: Горячая линия-Телеком, 2023. – 200 с.

92. *Gradshteyn I.S.* Table of integrals, series and products / I.S. Gradshteyn, I.M. Ryzhik; ред. A. Jeffrey, D. Zwillinger. – 7th ed. – Elsevier Academic Press, 2007. – 1220 с.

93. *Ahmed M.* A survey of network anomaly detection techniques / M. Ahmed, A. Naser Mahmood, J. Hu // Journal of Network and Computer Applications. – 2016. – Т. 60. – С. 19-31, DOI: 10.1016/j.jnca.2015.11.016

94. *Шелухин О.И.* Обнаружение вторжений в компьютерные сети [сетевые аномалии] / О.И. Шелухин, Д.Ж. Сакалема, А.С. Филинова. – М.: Горячая линия-Телеком, 2018. – 220 с.

95. *Hushchyn M.* Change Point Detection - Methods Overview / M. Hushchyn // OpenTalks.AI. – Москва, 2021.

96. *Плаван А.И.* Выявление аномалий в сетевом трафике по критерию среднеквадратической ошибки фильтрации линейного преобразования / А.И. Плаван, И.С. Поздняк // Фундаментальные и прикладные аспекты компьютерных технологий и информационной безопасности: материалы VII Всероссийской научно-технической конференции. – Таганрог: Южный федеральный университет, 5–11 апреля 2021 г. – С. 70-74

97. *Crotti M.* Traffic classification through simple statistical fingerprinting / M. Crotti [и др.] // ACM SIGCOMM Computer Communication Review. – 2007. – Т. 37. – № 1. – С. 5-16, DOI: 10.1145/1198255.1198257

98. *Kind A.* Histogram-based traffic anomaly detection / A. Kind, M. Stoecklin, X. Dimitropoulos // IEEE Transactions on Network and Service Management. – 2009. – Т. 6. – № 2. – С. 110-121, DOI: 10.1109/TNSM.2009.090604

99. *Лаута О.С.* Методика раннего обнаружения компьютерных атак в сетевом трафике сети передачи данных / О.С. Лаута [и др.] // Сборник научных статей по материалам IV Всероссийской научно-технической конференции «Безопасность информационных технологий». – Пенза: ПГУ, 3 апреля 2022 г. – Т. 1. – С. 126

100. *Барсуков И.С.* Использование фрактальных свойств трафика в цифровых сетях связи для детектирования сетевых аномалий / И.С. Барсуков, М.П. Ряполов // Вестник Воронежского государственного университета. Серия: Системный анализ и информационные технологии. – 2018. – № 3. – С. 73-81

101. *Карачанская (Чалых) Е.В.* Метод выявления аномалий сетевого трафика, основанный на его самоподобной структуре / Е.В. Карачанская (Чалых), Н.И. Соседова // Безопасность информационных технологий. – 2019. – Т. 26. – № 1. – С. 98-110, DOI: 10.26583/bit.2019.1.10

102. *Pan C.* Network Traffic Prediction Incorporating Prior Knowledge for an Intelligent Network / C. Pan [и др.] // Sensors. – 2022. – Т. 22. – № 7. – С. 2674, DOI: 10.3390/s22072674

103. *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

104. PT ISIM — система обеспечения киберустойчивости промышленных инфраструктур | Positive Technologies [Электронный ресурс]. – Режим доступа: https://ptsecurity.com/products/isim/ (Дата обращения: 25.06.2026)

105. Kaspersky Anti Targeted Attack | Лаборатория Касперского [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/enterprise-security/anti-targeted-attack-platform (Дата обращения: 25.06.2026)

106. eSensor [Электронный ресурс]. – Режим доступа: https://npo-echelon.ru/esensor/ (Дата обращения: 25.06.2026)

107. PT NAD — система поведенческого анализа сетевого трафика для обнаружения скрытых кибератак [Электронный ресурс]. – Режим доступа: https://ptsecurity.com/products/network-attack-discovery/ (Дата обращения: 25.06.2026)

108. Kaspersky Unified Monitoring and Analysis Platform SIEM система | Лаборатория Касперского [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/enterprise-security/unified-monitoring-and-analysis-platform (Дата обращения: 25.06.2026)

109. Промышленная платформа кибербезопасности | Лаборатория Касперского [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/enterprise-security/industrial-cybersecurity (Дата обращения: 25.06.2026)

110. Аналитическая платформа Dataplan [Электронный ресурс]. – Режим доступа: https://www.ngrsoftlab.ru/dataplan (Дата обращения: 25.06.2026)

111. *Ndong J.* Signal Processing-based Anomaly Detection Techniques: A Comparative Analysis / J. Ndong, K. Salamatian // Proc. of 3rd International Conference on Evolving Internet INTERNET 2011. – Luxembourg: IARIA, 2011. – С. 32-39

112. *Ndong J.* A Robust Anomaly Detection Technique Using Combined Statistical Methods / J. Ndong, K. Salamatian // Proc. of 9th Annual Communication Networks and Services Research Conference (CNSR). – Ottawa, ON, Canada: IEEE, 2011. – С. 101-108, DOI: 10.1109/CNSR.2011.23

113. *Soule A.* Combining filtering and statistical methods for anomaly detection / A. Soule, K. Salamatian, N. Taft // Proceedings of the 5th ACM SIGCOMM conference on Internet measurement (IMC '05). – Berkeley, California: ACM Press, 2005. – С. 331-344, DOI: 10.1145/1330107.1330147

114. *Wu H.* Kalman filter based DNS cache poisoning attack detection / H. Wu [и др.] // Proc. of 2015 IEEE International Conference on Automation Science and Engineering (CASE). – Gothenburg, Sweden: IEEE, 2015. – С. 1594-1600, DOI: 10.1109/CoASE.2015.7294328

115. *Celenk M.* Anomaly prediction in network traffic using adaptive Wiener filtering and ARMA modeling / M. Celenk [и др.] // Proc. of 2008 IEEE International Conference on Systems, Man and Cybernetics. – Singapore: IEEE, 2008. – С. 3548-3553, DOI: 10.1109/ICSMC.2008.4811848

116. *Al-Kasassbeh M.* Network fault detection with Wiener filter-based agent / M. Al-Kasassbeh, M. Adda // Journal of Network and Computer Applications. – 2009. – Т. 32. – № 4. – С. 824-833, DOI: 10.1016/j.jnca.2009.02.001

117. *Al-Kasassbeh M.* Network Intrusion Detection with Wiener Filter-based Agent / M. Al-Kasassbeh // World Applied Sciences Journal. – 2011. – Т. 13. – № 11. – С. 2372-2384

118. *Багманов В.Х.* Прогнозирование телетрафика на основе фрактальных фильтров / В.Х. Багманов, А.М. Комиссаров, А.Х. Султанов //

Вестник Уфимского государственного авиационного технического университета. – 2007. – Т. 9. – № 6. – С. 217-222

119. *Гельгор А.Л.* Общая теория связи. Винеровская фильтрация: учебное пособие для вузов / А.Л. Гельгор [и др.]. – СПб: Изд-во Политехнического ун-та, 2013. – 185 с.

120. *Шахтарин Б.И.* Фильтры Винера и Калмана. Учебное пособие для вузов / Б.И. Шахтарин. – 2-е изд., испр. – М.: Горячая линия-Телеком, 2024. – 396 с.

121. *Левин Б.Р.* Теоретические основы статистической радиотехники. В трех книгах. Книга вторая// Т. 2 / Б.Р. Левин. – 2-е изд., перераб. и дополнен. – М.: Советское радио, 1975. – 392 с.

122. *Haykin S.S.* Adaptive filter theory / S.S. Haykin. – 4th ed. – Upper Saddle River, N.J: Prentice Hall, 2002. – 920 с.

123. *Карташевский И.В.* Исследование и разработка методов анализа непуассоновских моделей трафика мультисервисных сетей : дис. ... канд. техн. наук: 05.12.13 / И.В. Карташевский. – Самара: ПГУТИ, 2010.

124. *Копырин А.С.* Технологии обработки и очистки данных, выявления и устранения шумов на временном ряду / А.С. Копырин, Е.В. Видищева // Вестник Академии знаний. – 2020. – № 4 (39). – С. 220-228

125. *Скляр А.Я.* Анализ и устранение шумовой компоненты во временных рядах с переменным шагом / А.Я. Скляр // Кибернетика и программирование. – 2019. – № 1. – С. 51-59

126. *Плаван А.И.* Среднеквадратическая ошибка фильтрации в качестве метрики расстояния для корреляционных матриц / А.И. Плаван // Актуальные проблемы радиоэлектроники и телекоммуникаций: материалы Всероссийской научно-технической конференции. – Самара: ООО «Артель», 25–28 апреля 2023 г. – С. 169-172

127. *Плаван А.И.* Среднеквадратическая ошибка фильтрации как критерий обнаружения аномалий сетевого трафика / А.И. Плаван, В.Г. Карташевский // Вестник Российского нового университета. Серия: Сложные

системы модели, анализ и управление. – 2023. – № 1. – С. 94-101, DOI: 10.18137/RNU.V9187.23.01.P.94

128. *Карташевский В.Г.* Фильтрация наблюдаемого трафика как способ обнаружения вторжений / В.Г. Карташевский, И.С. Поздняк // Вестник УрФО. – 2019. – Т. 19. – № 1 (31). – С. 17-22, DOI: 10.14529/secur190103

129. *Плаван А.И.* Метод выявления аномалий в сетевом трафике на основе фильтра Колмогорова-Винера / А.И. Плаван // Вестник УрФО. Безопасность в информационной сфере. – 2024. – № 1 (51). – С. 53-59, DOI: 10.14529/secur240107

130. *Назаров Н.Г.* Измерения: планирование и обработка результатов / Н.Г. Назаров. – М.: Изд-во стандартов, 2000. – 301 с.

131. *Плаван А.И.* Использование среднеквадратической ошибки фильтрации для обнаружения кратковременных аномалий сетевого трафика / А.И. Плаван, В.Г. Карташевский // Проблемы техники и технологий телекоммуникаций ПТиТТ-2023: Материалы XXV Международной научно-технической конференции. – Казань: КНИТУ-КАИ, 22–24 ноября 2023 г. – Т. 1. – С. 502-504

132. *Плаван А.И.* Обнаружение аномалий сетевого трафика на основе рассмотрения автокорреляционной функции в скользящем окне / А.И. Плаван // Сборник материалов XIII межведомственной научной конференции «Актуальные направления развития систем обеспечения безопасности объектов государственной охраны и охраняемых объектов, специальной связи для нужд органов государственной власти и специального информационного обеспечения государственных органов». – Орёл: Академия ФСО России, 10 февраля 2023 г. – С. 2

133. *Плаван А.И.* Сравнительный анализ метрик для определения схожести корреляционных свойств трафика / А.И. Плаван, В.Г. Карташевский // Сборник докладов и тезисов XIII Всероссийской научно-практической конференции «Проблемы передачи информации в

инфокоммуникационных системах». – Волгоград: Волгоградский государственный университет, 26 мая 2023 г. – С. 27-30

134. *Herdin M.* Correlation Matrix Distance, a Meaningful Measure for Evaluation of Non-Stationary MIMO Channels / M. Herdin [и др.] // Proc. of 2005 IEEE 61st Vehicular Technology Conference. – Stockholm, Sweden: IEEE, 2005. – Т. 1. – С. 136-140, DOI: 10.1109/VETECS.2005.1543265

135. *Плаван А.И.* Обнаружение аномалий сетевого трафика на основе фильтрации линейного преобразования трафика по критерию минимума среднеквадратической ошибки / А.И. Плаван // Сборник трудов II Всероссийской научной школы-семинара «Современные тенденции развития методов и технологий защиты информации». Москва, МТУСИ. – М.: ООО «Брис-М», 18–21 октября 2022 г. – С. 189-198

136. *Плаван А.И.* Определение ошибки фильтрации трафика с целью обнаружения атаки / А.И. Плаван, В.Г. Карташевский, И.С. Поздняк // Материалы XXIV Международной научно-технической конференции и материалы XX Международной научно-технической конференции (ПТиТТ-2022). В 2-х томах. – Уфа: УУНиТ, 23–25 ноября 2022 г. – Т. 1. – С. 217-219

137. *Mazel J.* A taxonomy of anomalies in backbone network traffic / J. Mazel, R. Fontugne, K. Fukuda // Proc. of 2014 International Wireless Communications and Mobile Computing Conference (IWCMC). – Nicosia, Cyprus: IEEE, 2014. – С. 30-36, DOI: 10.1109/IWCMC.2014.6906328

138. *Плаван А.И.* Исследование метода обнаружения аномалий в сетевом трафике на основе оптимального фильтра Колмогорова-Винера / А.И. Плаван // Актуальные проблемы радиоэлектроники и телекоммуникаций: материалы Всероссийской конференции. – Самара: ООО «Артель», 23–26 апреля 2024 г. – С. 228-231

139. *Шкодырев В.П.* Обзор методов обнаружения аномалий в потоках данных / В.П. Шкодырев [и др.] // Proc. of Second Conference on Software Engineering and Information Management (SEIM-2017) : CEUR Workshop Proceedings. – Saint Petersburg, Russia: CEUR, 2017. – Т. 1864. – С. 7

Приложение А. Акты внедрения результатов работы

«УТВЕРЖДАЮ»
Генеральный директор
ООО «Идентификация»
_____ С. А. Глубоков
09 июля 2026 г.

АКТ
внедрения результатов, полученных Плаваном А.И. в диссертационной работе «Методы обнаружения аномалий в сетевом трафике на основе оптимальной линейной фильтрации»,представленной на соискание ученой степени кандидата технических наук по специальности 2.3.6 Методы и системы защиты информации, информационная безопасность

Комиссия в составе:

председатель комиссии: Панин Дмитрий Юрьевич, заместитель генерального директора,

члены комиссии: Сырчиков Михаил Викторович, главный специалист по информационной безопасности, Нуждин Олег Валентинович, начальник отдела технического обеспечения,

составила настоящий акт, подтверждающий внедрение следующих результатов, полученных в диссертационной работе Плавана А.И., в производственную деятельность ООО «Идентификация»:

- Алгоритм определения статистически значимых признаков различных видов сетевых атак;
- Методы обнаружения аномалий на основе применения оптимального линейного фильтра, основанные на вычислении значения минимальной среднеквадратической ошибки фильтрации;
- Алгоритм обнаружения аномалий на основе отклонения значения минимальной среднеквадратической ошибки оптимального линейного фильтра;

Указанные результаты диссертационной работы были использованы при проведении работ в ООО «Идентификация» по проектированию и разработке перспективных средств защиты информации для своевременного обнаружения и предупреждения компьютерных атак и других угроз в сфере информационной безопасности.

Предложенные технические решения позволили повысить число выявленных аномалий, что привело к снижению вероятности успешной реализации атаки на 22% на тестовых стендах и сократило среднее время обнаружения инцидента на 12 минут. Применение разработанных в диссертации методов и алгоритмов позволяет повысить защищенность информационных систем и обеспечить оперативное выявление атак.

Заместитель генерального директора Д.Ю. Панин

Главный специалист по информационной безопасности М.В. Сырчиков

Начальник отдела технического обеспечения О.В. Нуждин

УТВЕРЖДАЮ

Проректор по учебной работе
ФГБОУ ВО «ПГУТИ»
д.т.н., доцент

М.А. Буранова

«06» июля 2026 г.

АКТ

о внедрении результатов диссертационной работы Плавана Алексея Игоревича

«Методы обнаружения аномалий в сетевом трафике на основе оптимальной линейной фильтрации»

Комиссия ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики» в составе: председателя комиссии Тучковой А.С. – начальника управления организации учебного процесса (УОУП), и членов комиссии: д.т.н., доц. Шакурского М.В. – заведующего кафедрой информационной безопасности (ИБ), к.т.н., доц. Поздняк И.С. – декана факультета кибербезопасности и управления, составили настоящий акт о том, что в университете внедрены в учебный процесс на кафедру ИБ следующие результаты диссертационной работы Плавана А.И.:

1. алгоритм определения численных индикаторов атак для различных статистических характеристик трафика, позволяющий выделить характерные признаки различных сетевых атак;
2. метод моделирования случайных процессов с одновременно заданной АКФ и распределением Вейбулла на основе копулы Фарли-Гумбеля-Моргенштерна;
3. методы обнаружения аномалий, основанные на вычислении значения минимальной среднеквадратической ошибки фильтрации и сравнении её с эталонным значением, полученным для легитимного трафика.

Указанные результаты диссертационной работы Плавана А.И. используются на кафедре ИБ:

— в рамках проведения лабораторных и практических занятий по дисциплине «Устройства приема и обработки сигналов в защищенных системах радиосвязи» по направлениям подготовки специалистов 10.05.02 «Информационная безопасность телекоммуникационных систем» и магистров 10.04.01 «Информационная безопасность» (профиль: Безопасность телекоммуникационных систем);

— в рамках проведения лабораторных и практических занятий по дисциплинам «Моделирование систем и сетей телекоммуникаций» по направлению подготовки специалистов 10.05.02 «Информационная безопасность телекоммуникационных систем».

Заключение:

Результаты диссертационного исследования представляют научную и практическую ценность, активно используются в учебном процессе при выполнении научно-исследовательских работ, связанных с обнаружением сетевых атак и моделированием сетевого трафика и позволяют повысить качество преподаваемых дисциплин.

Председатель комиссии:
Начальник УОУП А.С. Тучкова

Члены комиссии:
Зав. кафедрой ИБ,
д.т.н., доцент М.В. Шакурский

Декан факультета №1,
к.т.н., доцент И.С. Поздняк

Приложение Б. Свидетельства о государственной регистрации программ для ЭВМ и электронных ресурсов

РОССИЙСКАЯ ФЕДЕРАЦИЯ



СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2022614836

Программный комплекс «PcapStat»

Правообладатель: ***Плаван Алексей Игоревич (RU)***

Автор(ы): ***Плаван Алексей Игоревич (RU)***



Заявка № **2022613421**
Дата поступления **09 марта 2022 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***28 марта 2022 г.***

Руководитель Федеральной службы
по интеллектуальной собственности

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат 68b80077e14e40f0a94edbd24145d5c7
Владелец **Зубов Юрий Сергеевич**
Действителен с 2.03.2022 по 26.05.2023

Ю.С. Зубов

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2023664160

PcapConvert

Правообладатель: ***Плаван Алексей Игоревич (RU)***

Автор(ы): ***Плаван Алексей Игоревич (RU)***

Заявка № **2023663148**
Дата поступления **21 июня 2023 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***03 июля 2023 г.***

Руководитель Федеральной службы
по интеллектуальной собственности

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат 429b6a0fe3853164baf96f83b73b4aa7
Владелец **Зубов Юрий Сергеевич**
Действителен с 10.05.2023 по 02.08.2024

Ю.С. Зубов

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2024611818

PcapReplay

Правообладатель: ***Плаван Алексей Игоревич (RU)***

Автор(ы): ***Плаван Алексей Игоревич (RU)***

Заявка № **2024611026**
Дата поступления **24 января 2024 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***24 января 2024 г.***

Руководитель Федеральной службы
по интеллектуальной собственности

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат 429b6a0fe3853164baf96f83b73b4aa7
Владелец **Зубов Юрий Сергеевич**
Действителен с 10.05.2023 по 02.08.2024

Ю.С. Зубов