Разработка и применение программных модулей для мониторинга защищенности IP-телефонных сетей и оценки качества связи в условиях кибератак

А. А. Привалов[3], Д. Д. Титов[1,2], В. И. Веремьёв[4]

[1]*Петербургский государственный университет путей сообщения Императора Александра I*

[2]*ОАО «СУПЕРТЕЛ», г. Санкт-Петербург, Российская Федерация*

[3]*Академия войск национальной гвардии, г. Санкт-Петербург, Российская Федерация*

[4]*НИИ «Прогноз»*

E-mail: titovdd178@gmail.com, aprivalov@inbox.ru, viveremyev@etu.ru

Аннотация. **Целью работы является разработка программных средств для комплексного мониторинга защищённости и имитационного моделирования функционирования IP-телефонных сетей в условиях кибератак с оценкой ключевых показателей качества обслуживания. Применяются математические и стохастические методы, включая графо-аналитические модели (GERT-сети), вероятностный анализ и топологические преобразования сетей. В моделях учитываются приоритеты трафика, а также используются функции распределения Парето, Вейбулла и гамма-распределения, что позволяет описывать самоподобие трафика и «тяжёлые хвосты» задержек. Результаты показывают, что разработанные инструменты позволяют количественно оценивать влияние различных кибератак (DDoS, комбинированные сценарии, сетевое сканирование) на время доставки, вероятность потерь и время восстановления маршрутов, а также выявлять уязвимые элементы сети и оптимизировать стратегии маршрутизации. Практическая значимость заключается в возможности интеграции решений в корпоративные и транспортные сети для упреждающего анализа устойчивости, моделирования последствий угроз и подготовки специалистов по сетевой безопасности.**

Ключевые слова: IP-телефонная сеть; кибератака; надёжность сети; устойчивость сети; приоритетный трафик; математическое моделирование; GERT-сеть; DDoS

I. Введение

Современные цифровые сети связи, включая телефонные IP-сети, всё чаще подвергаются целенаправленным кибератакам, способным дестабилизировать их работу. Распространённые угрозы включают распределённые атаки отказа в обслуживании (DDoS), перегрузку каналов, нарушения маршрутизации, атаки на протоколы аутентификации, компьютерную разведку и др.. Последствия подобных воздействий могут быть критичными: возрастание задержек и джиттера, деградация качества связи, потеря пакетов, сбои в работе узлов и даже отказ важных сервисов. Особенно опасны атаки на сети, обслуживающие критически важные объекты (транспорт, энергетика, медицина и т.п.), где кратковременное нарушение связи способно привести к цепочке сбоев и серьёзным материальным либо социальным потерям.

Несмотря на большое внимание к проблемам информационной безопасности сетей, большинство существующих средств мониторинга ориентированы на реактивный анализ, то есть отображение и расследование уже произошедших инцидентов или текущего состояния сети. Как правило, такие системы фиксируют факт атаки постфактум и дают статистику по имевшим место сбоям, но не позволяют заранее оценить потенциальные риски и спрогнозировать поведение сети при различных сценариях воздействия. Отсутствует также возможность проверки «что, если» – инженеры не могут на действующей инфраструктуре безопасно проигрывать разные варианты атак и защитных мер, поскольку это сопряжено с риском для реального трафика. В результате возникает объективная необходимость в прогностическом и имитационном инструменте, который, в отличие от пассивного мониторинга, предоставил бы средства для предварительного анализа устойчивости сети и поддержки принятия решений по её защите.

В данной работе представлены два программных модуля, разработанных для проактивного моделирования и оценки состояния IP-телефонных сетей в условиях кибератак. В основе инструментов лежат методы вероятностного и стохастического моделирования сетевых процессов, включая топологическое моделирование и графо-аналитические схемы типа GERT. Реализованная модель учитывает широкий спектр факторов: интенсивность фонового трафика и атак, вероятность отказов узлов, динамику изменения параметров сети при перегрузках. Важной особенностью является поддержка различных законов распределения времени обслуживания и межприбытия пакетов – помимо классического экспоненциального, используются распределения Вейбулла, Парето и гамма, что обеспечивает более реалистичное описание самоподобного телетрафика с «тяжёлыми хвостами» распределения задержек. Кроме того, учитывается приоритетность трафика: информационные потоки разделяются по категориям важности, влияющим на порядок и скорость обслуживания пакетов в условиях ограниченных ресурсов. Модули снабжены интерактивной системой визуализации, отображающей топологию сети, графики распределения времени доставки и текущие показатели качества, что даёт

инженеру наглядную картину развития ситуации и упрощает интерпретацию результатов моделирования.

Таким образом, разработанные программные средства направлены на повышение надежности и живучести IP-сетей за счёт имитации различных сценариев кибератак, выявления уязвимых узлов и оптимизации маршрутизации до наступления кризисной ситуации. В последующих разделах приведён обзор существующих методов анализа надёжности сетей, описаны научная новизна предложенного подхода, подробно изложена методология моделирования, рассмотрены реализованные функции программных модулей и проведён анализ результатов экспериментов.

II. Обзор литературы

Проблематика обеспечения живучести сетей связи в условиях кибератак широко освещена в отечественной и зарубежной научной литературе. Зарубежные исследования преимущественно базируются на математическом аппарате теории массового обслуживания, сетей Петри, Марковских моделей, а также на применении методов машинного обучения для выявления атак и аномалий трафика. Однако основной недостаток таких подходов заключается в их ориентации на обнаружение уже совершенных атак (IDS/IPS-системы) и недостаточной способности прогнозировать последствия атак в реальном времени.

В отечественных работах акцент делается на самоподобии и фрактальной природе телетрафика, что характеризуется высокой вариативностью и длинной памяти интервалов между пакетами. Показано, что игнорирование этих свойств приводит к значительным погрешностям при оценке вероятности перегрузок и отказов. Особое внимание уделяется также вопросам приоритетного обслуживания и резервирования.

Классические модели надёжности сетей чаще всего используют экспоненциальные законы распределения, не учитывающие реальных характеристик телетрафика, таких как «тяжёлые хвосты» распределения задержек и наличие длительных корреляций. В связи с этим современные подходы вводят усечённые распределения Парето, распределения Вейбулла и гамма-распределения, которые лучше отражают реалистичное поведение сетей, хотя и усложняют вычислительные процедуры. Разработанный подход интегрирует эти распределения, позволяя выбирать наиболее подходящие для эмпирических данных сети.

Анализ существующих решений выявил ряд ограничений: обычно рассматривается фиксированный характер трафика без учёта его динамических изменений, не учитывается адаптивная маршрутизация при ухудшении качества, анализируются изолированные атаки без комбинированных сценариев, отсутствуют средства интерактивного прогнозирования и визуализации. В предлагаемой разработке эти проблемы решаются комплексно.

Научная новизна предложенного подхода заключается в следующем:

1. Впервые для анализа устойчивости IP-телефонных сетей использованы графо-аналитические модели GERT, позволяющие моделировать вероятностные прохождения трафика по альтернативным маршрутам и учитывать циклы повторных передач при потерях пакетов.
2. Реализована гибкая поддержка различных законов распределения времени обслуживания и межприбытия пакетов (гамма, Парето, Вейбулла), что обеспечивает реалистичность имитационного моделирования.
3. Введено приоритетное обслуживание трафика с разделением потоков на классы важности, что позволяет количественно оценить эффективность механизмов QoS при атаках.
4. Моделируются сложные комбинированные атаки (сканирование сети с последующими DDoS-атаками), отражающие реальный характер многофазных кибервоздействий.
5. Предлагается интерактивная визуализация в реальном времени, отображающая текущие вероятностные характеристики сети и позволяющая инженерам оперативно принимать решения на основе изменяющихся условий.

Методология и математический аппарат моделирования включают в себя стохастический подход, характеризуемый параметрами восстановления маршрутов (T_{res}), пропускной способностью каналов (C), интенсивностью фонового и атакующего трафика, объемом буферной памяти и статистическими характеристиками пакетов. При расчёте ключевых показателей (время доставки, вероятность потерь и задержек) используются формулы для вычисления моментов и коэффициентов вариации с учётом выбранных распределений (Парето, Вейбулла, гамма). Для оценки устойчивости сети применяется коэффициент загрузки сети (ρ), критическое значение которого приближается к единице при потере устойчивости системы.

Численное решение реализовано через сочетание дискретно-событийного моделирования и метода Монте-Карло, что позволяет получить точные оценки интересующих показателей даже при сложных условиях эксплуатации. Это обеспечивает возможность точного прогнозирования состояния сети в условиях различных атак и выбора оптимальных стратегий маршрутизации и защиты.

III. Анализ результатов моделирования, заключение и перспективы

Проведённая серия экспериментов с использованием предложенных инструментов подтвердила их эффективность в условиях различных кибератак. Моделирование воздействия DDoS-атак продемонстрировало, что сеть способна нормально функционировать при низкой интенсивности атак, однако при превышении определённого порога нагрузки ($\rho \sim 1$) вероятность своевременной доставки резко снижается, буферы переполняются, и сеть теряет устойчивость. Критическое значение нагрузки проявляется как «фазовый переход», при котором задержки значительно превышают допустимые пределы. Важным параметром является среднее время восстановления (T_{res}), напрямую влияющее на быстроту восстановления работоспособности после прекращения атаки.

Эксперименты с приоритетным обслуживанием показали, что внедрение политики QoS позволяет эффективно поддерживать качество критически важных сервисов при перегрузках, вызванных высокой интенсивностью трафика. При этом низкоприоритетные потоки данных испытывают задержки и потери, что подтверждает ожидаемую эффективность дифференцированного обслуживания. Практическая проверка управленческих решений (например, временное отключение второстепенных потоков) продемонстрировала возможность оперативного улучшения характеристик сети, что подтверждает соответствие модели реальным условиям эксплуатации.

Особый интерес представляют результаты моделирования комбинированных атак, состоящих из разведки и последующих DDoS-атак. Инструмент выявил наиболее уязвимые компоненты сетевой инфраструктуры, отказ которых приводит к наибольшему ущербу. Благодаря моделированию оператор может заранее определить критические узлы и принять меры по их укреплению или оптимизации маршрутизации, что существенно повышает устойчивость сети.

Таким образом, предложенные модули обеспечивают не только мониторинг текущего состояния сети, но и дают возможность проактивного анализа и прогнозирования развития событий. Оператор сети получает возможность заранее оценить последствия атак, выбрать оптимальные стратегии реагирования и минимизировать возможные риски.

IV. Заключение и перспективы

Предложенный комплекс программных средств существенно повышает возможности прогнозирования и обеспечения устойчивости телефонных IP-сетей в условиях современных киберугроз. В отличие от традиционных подходов, ориентированных на пассивный мониторинг, созданные решения позволяют активно моделировать различные сценарии воздействия и оптимизировать защитные меры до наступления реальной угрозы.

Теоретическая значимость работы заключается в успешном объединении аналитических и имитационных методов, учёте сложных законов распределения и дифференцированном обслуживании трафика. Практическая значимость подтверждается возможностью применения разработанных решений для повышения надёжности транспортных, энергетических и корпоративных сетей, где бесперебойная работа является критически важной задачей. Модули могут быть интегрированы в существующие системы мониторинга и использоваться для подготовки специалистов в области информационной безопасности.

Перспективы развития включают интеграцию модулей с реальными системами мониторинга, автоматическое обновление параметров модели по текущим данным сети и внедрение методов машинного обучения для выявления новых типов атак и выработки рекомендаций оператору. В дальнейшем предполагается расширить спектр моделируемых сценариев и адаптировать подход для других типов сетей связи, что сделает его универсальным инструментом для обеспечения надёжности и безопасности сетевой инфраструктуры.

Список литературы

[1] Privalov A., Kotenko I., Saenko I., Evglevskaya N., Titov D. Evaluating the functioning quality of data transmission networks in the context of cyberattacks // *Energies*. 2021. Vol. 14, No. 16. DOI: 10.3390/en14164755.

[2] Шелухин О.И. Причины самоподобия телетрафика и методы оценки показателя Херста // *Электротехнические и информационные комплексы и системы*. 2007. Т. 3, № 1. С. 5–14.

[3] Назаров А.Н. Модели и методы расчета показателей качества функционирования узлового оборудования и структурно-сетевых параметров сетей связи следующего поколения. 2-е изд., доп. и перераб. Красноярск: ООО «Поликом», 2011. 491 с.

[4] Привалов А.А., Титов Д.Д. Модель процесса работы узла коммутации технологической IP-сети при обслуживании приоритетного многопродуктового потока в условиях DDoS-атак нарушителя // *Фундаментальные и прикладные научные исследования: сб. тр. X Междунар. конкурса науч.-исслед. работ*. Уфа, 2022.

[5] Привалов А.А., Титов Д.Д. Модель процесса передачи приоритетного многопродуктового потока по каналу телефонной IP-сети в условиях компьютерных атак // *Инновационные научные исследования в современном мире: сб. тр. X Всерос. конкурса науч.-исслед. работ*. Уфа, 2022.

[6] Привалов А.А., Титов Д.Д. Модель процесса функционирования узла коммутации технологической сети передачи данных в условиях DDoS-атак // *Информация и космос*. 2021.

[7] Привалов А.А., Титов Д.Д., Лукичева В.Л. Модель процесса доставки пакетов по каналу передачи данных в условиях компьютерных атак нарушителя // *Известия Петербургского университета путей сообщения*. 2021.

[8] Кравцов А.О., Привалов А.А., Матвейкин Г.В., Титов Д.Д. Структура транспортной сети связи ОАО «РЖД» и возникновение фазового перехода // *Материалы конф. ELTRANS-2019*. СПб.: ИПК «НП-Принт», 2023. С. 190–196.

[9] Lee J., Kim H., Park S. Security analysis of IP networks using Petri nets and Markov chains // *Journal of Network and Computer Applications*. 2020. Vol. 158. P. 102580. DOI: 10.1016/j.jnca.2020.102580.

[10] Zhang Y., Li P., Wang X. Network intrusion detection based on deep learning algorithms // *Future Generation Computer Systems.* 2019. Vol. 93. P. 572–583. – DOI: 10.1016/j.future.2018.10.039.

[11] Иванов А.И., Колесников В.П. Моделирование приоритетного обслуживания трафика в сетях передачи данных при кибератаках // *Информационные технологии и вычислительные системы*. 2022. № 3. С. 45–52.

[12] Васильев Д.Н., Соколов А.В., Семёнова Ю.А. Анализ перегрузок IP-сетей с использованием самоподобных моделей трафика // *Вестник связи*. 2021. № 4. С. 12–19.