ЛЕКАРЬ ЛЮДМИЛА АНТОНОВНА[1]

antonna47@bk.ru

КУБАСОВ ИГОРЬ АНАТОЛЬЕВИЧ[2]

igorak@list.ru

[1,2] Академия управления МВД России (Москва, Россия)

Системный подход к поиску и регулированию меш-сетей в целях охраны общественного порядка и обеспечения общественной безопасности

Аннотация. Меш-сети, развертываемые с помощью различных меш-мессенджеров (зарубежных разработчиков) без подключения пользователей к Wi-Fi или сотовой связи, могут использоваться отдельными лицами или сообществами для осуществления противоправной деятельности. Однако анализ информации о пользователях и блокирование таких меш-сетей затруднены из-за их децентрализованного характера и сосредоточенности на конфиденциальности. А применяемый в настоящее время правоохранительными органами метод радиоэлектронной борьбы с помощью блокираторов, излучающих мощность в широкой полосе частот, подавляет в заданной территории все источники излучения, как те, которые являются целью, так и базовые станции сотовой связи, сети Wi-Fi и др. Обоснована необходимость применения системного подхода в борьбе с незаконной деятельностью в меш-сетях в целях повышения эффективности охраны общественного порядка и обеспечения общественной безопасности. На основе анализа результатов выполнения научно-исследовательской работы (шифр «Отвертка») сделан вывод о том, что выбраны эффективные техники и методы, затрудняющие и блокирующие обмен в меш-сетях.

Ключевые слова и словосочетания: охрана общественного порядка и обеспечение общественной безопасности, поиск и регулирование меш-сетей, меш-мессенджер

Для цитирования: *Лекарь Л.А., Кубасов И. А. Системный подход к поиску и регулированию меш-сетей в целях охраны общественного порядка и обеспечения общественной безопасности // Вестник ВИПК МВД России. – 2023. – № 4(68). – С. 90-96; doi: 10.29039/2312-7937-2023-4-90-96*

LEKAR LYUDMILA A.[1],
KUBASOV IGOR A.[2]
[1,2] Academy of Management of the Ministry of Internal Affairs of Russia (Moscow, Russia)

A SYSTEMATIC APPROACH TO SEARCH AND REGULATION MESH NETWORKS IN ORDER TO PROTECT PUBLIC ORDER AND ENSURE PUBLIC SAFETY

Annotation. Mesh networks deployed using various mesh messengers (foreign developers) without connecting users to Wi-Fi or cellular communications can be used by individuals or communities to carry out illegal activities. However, analyzing user information and blocking such mesh networks is difficult due to their decentralized nature and focus on privacy. And the method of electronic warfare currently used by law enforcement agencies with the help of blockers emitting power in a wide frequency band suppresses all radiation sources in a given territory, both those that are the target and cellular base stations, Wi-Fi networks, etc. The necessity of applying a systematic approach in the fight against illegal activities in mesh networks in order to increase the effectiveness of public order protection and public safety is substantiated. Based on the analysis of the results of the research work (cipher "Screwdriver"), it is concluded that effective techniques and methods have been selected that complicate and block the exchange in mesh networks.

Key words and word combinations: protection of public order and ensuring public safety, search and regulation of mesh networks, mesh messenger

For citation: *Lekar L.A., Kubasov I. A. A systematic approach to search and regulation Mesh networks in order to protect public order and ensure public safety // Vestnik Advanced Training Institute of the MIA of Russia. – 2023. – № 4(68). – P. 90-96; doi: 10.29039/2312-7937-2023-4-90-96*

Меш-сеть (mesh network – ячеистая сеть, анонимная сеть обмена информацией)[1] – это децентрализованный тип сети, в котором несколько устройств, называемых узлами, работают вместе для связи и передачи данных другим узлам сети. В традиционной сети устройства подключаются к центральной точке доступа, например маршрутизатору, для доступа в Интернет. Однако в меш-сети каждый узел действует как клиент и маршрутизатор, позволяя устройствам напрямую подключаться друг к другу.

Устраняя необходимость в централизованном маршрутизаторе, меш-сети имеют несколько преимуществ:

1. Повышенная надежность. Благодаря множеству путей передачи данных меш-сети обладают высокой отказоустойчивостью. Если узел выходит из строя или отключается, сеть может автоматически перенаправить данные по альтернативным путям, обеспечивая непрерывное соединение.

2. Расширенное покрытие. Меш-сети могут покрывать большие территории благодаря расширению диапазона сети за счет добавления большего количества узлов. Каждый новый узел действует как расширение, увеличивая охват сети без ущерба для производительности.

3. Улучшенная масштабируемость. Добавление узлов в меш-сеть относительно простое, что позволяет легко расширять и адаптировать сеть по мере необходимости. Такая масштабируемость обеспечивает быстрое развертывание как в жилых, так и в коммерческих помещениях.

4. Повышенная производительность. Меш-сети часто используют интеллектуальные алгоритмы маршрутизации, которые оптимизируют пути передачи данных. Эти алгоритмы учитывают такие факторы, как уровень сигнала и перегруженность трафика, чтобы обеспечить эффективную и быструю доставку данных.

5. Гибкость и мобильность. Меш-сети могут быть очень гибкими, позволяя устройствам беспрепятственно перемещаться внутри сети без потери возможности подключения. Каждый узел может действовать как точка доступа, позволяя устройствам переключаться между узлами по мере необходимости.

6. Избыточность и отказоустойчивость. Поскольку каждый узел меш-сети может взаимодействовать с несколькими соседними узлами, сеть имеет встроенную избыточность. Если один узел выходит из строя или возникают проблемы, соседние узлы могут вмешаться и поддержать функциональность сети.

7. Безопасность. В меш-сети данные могут шифроваться и аутентифицироваться на каждом узле, обеспечивая дополнительный уровень безопасности. Такой распределенный подход к безопасности снижает риск возникновения единой точки отказа или несанкционированного доступа [1-5].

---

[1] *Mesh-сеть* – это распределенная, одноранговая, самоорганизующаяся сеть с ячеистой топологией.

Благодаря своим преимуществам меш-сети, создаваемые с использованием различных меш-месенджеров[2], становятся все более популярными в применении, в том числе и для совершения противоправной деятельности. Например, Firechat[3] с успехом применяли протестующие в Гонг-Конге, Алжире, Зимбабве (власти этих стран выключали Интернет, чтобы помешать протестам). Сейчас Firechat, наравне с приложениями по обходу блокировок, на первом месте по скачиванию в Венесуэле [4].

Актуальность поиска и регулирования меш-сетей правоохранительными органами является сложной и развивающейся проблемой. Способность правоохранительных органов выявлять и регулировать меш-сети имеет важное значение для охраны общественного порядка и обеспечения общественной безопасности. Как и в любой сети связи, существует вероятность неправомерного использования, включая распространение незаконного контента, киберпреступность, терроризм и другую незаконную деятельность [6, с. 11-16, 7, с. 436-442]. Правоохранительные органы должны иметь средства для расследования и задержания лиц, причастных к такой деятельности.

Системный подход в борьбе с незаконной деятельностью в меш-сетях. Для борьбы с незаконной деятельностью в меш-сетях необходим системный подход с упором на технологические, юридические и совместные усилия.

Технологические решения могут сыграть жизненно важную роль в пресечении незаконной деятельности в меш-сетях. Исследования и разработки должны быть сосредоточены на расширении возможностей сетевого мониторинга для выявления и отслеживания вредоносных действий. Это включает в себя разработку передовых систем обнаружения вторжений, которые могут обнаруживать модели незаконного поведения, такие как распространение незаконного контента или координация преступной деятельности. Совместные усилия сетевых провайдеров, производителей устройств и правоохранительных органов имеют решающее значение для разработки и обмена инструментами, которые могут помочь в выявлении и смягчении последствий незаконной деятельности.

Правоохранительные органы должны адаптировать свои методы расследования, чтобы идти в ногу с технологическим прогрессом. Это включает в себя развитие опыта в анализе ячеистых сетевых инфраструктур, выявлении ключевых узлов или лиц, вовлеченных в преступную деятельность, а также поиске способов перехвата или мониторинга коммуникаций внутри этих сетей, соблюдая при этом конфиденциальность и правовые границы. Учитывая децентрализованный характер меш-сетей, традиционные методы мониторинга и перехвата могут оказаться не столь эффективными, что требует разработки новых методов и технологий, а также формирования у сотрудников навыков по применению специальной техники в едином цифровом пространстве [8, с. 96-101].

Необходимо также обновить правовую базу для борьбы с незаконной деятельностью в меш-сетях. Следует работать над принятием нормативных правовых актов, которые конкретно направлены на пресечение противоправного применения этих сетей, гарантируя, что правоохранительные органы имеют необходимые инструменты для расследования и преследования лиц, причастных к незаконной деятельности. Однако важно найти баланс между противодействием незаконной деятельности и сохранением конфиденциальности и свободы людей, использующих меш-сети в законных целях.

Сотрудничество между заинтересованными сторонами имеет решающее значение для эффективной борьбы с незаконной деятельностью в меш-сетях. Правоохранительные органы, сетевые операторы, производители устройств и организации гражданского общества должны установить партнерские отношения и обмениваться информацией, чтобы опережать развивающиеся угрозы. Сотрудничество между правоохранительными органами и технологическими экспертами имеет

[2]*Меш-месенджеры* – это мобильные приложения (как правило, зарубежных производителей), которые применяют в местах массового скопления людей, где по каким-то причинам наблюдаются проблемы с Интернетом и сотовой связью.

[3]*Firechat* – это инновационное Android-приложение, работает путем передачи сигналов от одного устройства к другому.

решающее значение в решении проблем регулирования меш-сетей. Кампании по информированию общественности могут уведомить пользователей о потенциальных рисках участия в незаконной деятельности в меш-сетях и способствовать ответственному использованию.

Кроме того, международное сотрудничество имеет важное значение для борьбы с трансграничной незаконной деятельностью в меш-сетях. Поскольку эти сети могут пересекать географические границы, правоохранительные органы должны работать вместе, чтобы обмениваться информацией, разведданными и передовым опытом регулирования и расследования преступной деятельности. Это сотрудничество может помочь в разработке общих стандартов, правовых рамок и технических решений для обеспечения эффективного регулирования меш-сетей при соблюдении границ юрисдикции и прав человека.

При этом важно признать, что полное искоренение незаконной деятельности в меш-сетях может оказаться недостижимым. Как и в случае с любой технологией, всегда найдутся люди, которые будут использовать ее в незаконных целях. Поэтому усилия также должны быть сосредоточены на смягчении последствий незаконной деятельности путем создания устойчивых сетей, способных противостоять атакам и быстро восстанавливаться после сбоев.

Методы поиска, регулирования и деструктивного воздействия на меш-сети. Применяемые в настоящее время методы поиска, регулирования и деструктивного воздействия на меш-сети не являются высокоэффективными, т.к. меш-сети обладают свойствами повышенной конфиденциальности и улучшенной связью в отдаленных районах.

Так, например, для контроля анонимных сетей обмена информации используются методы радиоэлектронной борьбы с помощью блокираторов, излучающих мощность в широкой полосе частот. Однако на заданной территории подавляются все источники излучения, как те, которые являются целью, так и любые другие (базовые станции сотовой связи, сети Wi-Fi и т.д.). При этом сам факт деструктивного воздействия обнаруживается сразу.

Методы поиска применительно к меш-сетям могут включать обнаружение и идентификацию конкретных узлов или пользователей, вовлеченных в незаконную деятельность. Поскольку меш-сети распределяют данные по нескольким узлам, традиционные методы поиска, такие как отслеживание IP-адресов или мониторинг централизованных серверов, могут оказаться неэффективными. Правоохранительным органам требуется адаптировать методы для решения этих проблем. Один из подходов – сосредоточиться на конечных точках меш-сети, пытаясь перехватить сообщения в тех точках, где данные входят или выходят из децентрализованной системы. Это может включать мониторинг провайдеров интернет-услуг или развертывание инструментов наблюдения вблизи стратегически важных мест.

Регулирование меш-сетей – еще одна проблема, с которой сталкиваются правоохранительные органы. В отличие от традиционных сетей, которые работают под контролем центрального органа, меш-сети децентрализованы и часто действуют в «серых» правовых зонах. Это затрудняет обеспечение соблюдения существующих правил или введение новых. Правоохранительные органы борются с этими сетями, сохраняя при этом баланс между такими проблемами, как конфиденциальность, безопасность и необходимость предотвращения преступной деятельности.

Влияние деятельности правоохранительных органов на меш-сети может быть как конструктивным, так и деструктивным.

С одной стороны, правоохранительные органы играют решающую роль в обеспечении общественной безопасности, используя свои полномочия для выявления и предотвращения преступной деятельности. Они могут использовать свои ресурсы для мониторинга и пресечения незаконной деятельности, осуществляемой через меш-сети. Это может помочь защитить людей от вреда и предотвратить превращение сетей в прибежище для преступных предприятий.

С другой стороны, интрузивные методы, используемые правоохранительными органами, могут подорвать те самые принципы, которые делают меш-сети ценными. Чрезмерное наблюдение, неизбирательный сбор данных или ослабление протоколов

шифрования могут подорвать конфиденциальность пользователей и ущемить гражданские свободы. Кроме того, неумелые попытки регулирования меш-сетей могут задушить инновации и помешать развитию альтернативных коммуникационных инфраструктур [9, с. 83-89].

Чтобы найти баланс между потребностями правоохранительных органов и преимуществами меш-сетей, необходимы сотрудничество и диалог между заинтересованными сторонами. Взаимодействие с экспертами в области сетевых технологий и юристами может помочь разработать эффективные и соразмерные стратегии.

Результаты научно-исследовательской работы «Обоснование и выбор методов контроля анонимных сетей обмена информацией». Особо следует отметить технические решения, выработанные и экспериментально исследованные ФКУ НПО «СТиС» МВД России в результате выполнения научно-исследовательской работы «Обоснование и выбор методов контроля анонимных сетей обмена информацией», шифр «Отвертка» [10]. Данные решения реализованы в макете программно-аппаратного комплекса (далее – ПАК «Отвертка»), осуществляющего мониторинг активности, протоколирования действий и регулирования доступа пользователей к анонимным меш-мессенджерам, в том числе: Signal Offline, Briar, Bridgefy, включая деструктивное воздействие. При этом сам факт воздействия ПАК «Отвертка» не обнаруживается пользователями сети.

Экспериментально подтвержден широкий набор функциональных возможностей: в части сети меш-мессенджера Bridgefy – полная блокировка доступа к приложению, подмена личных сообщений, разовое отключение пользователей; в части, касающейся сети меш-мессенджера Briar, – принудительная деаутентификация пользователя, принудительная дизассоциация пользователя, перевод пользователя на другой канал, блокирование создания новых контактов, перехват подключения к целевому пользователю; в части, касающейся сети меш-мессенджера Signal Offline, – принудительная деаутентификация пользователя, принудительная дизассоциация пользователя, перевод пользователя на другой канал.

На рис. 1 представлена модель применения ПАК «Отвертка».

Для сбора данных с приемо-передающих устройств (ППУ) создается общая локальная Wi-Fi-сеть, обеспечивающая беспроводное подключение между всеми ППУ и пультом оператора на базе электронно-вычислительной машины типа ноутбук (ПуО) в радиусе действия беспроводных Wi-Fi-адаптеров данных устройств. Таким образом, все ППУ в радиусе действия друг друга создают собственную сеть для передачи данных друг другу и ПуО.

Отправка данных на ПуО и ППУ при этом возможна только по прямому запросу с ПуО или другого ППУ, входящего в состав комплекса, заведомо сконфигурированного на работу с другими ППУ.

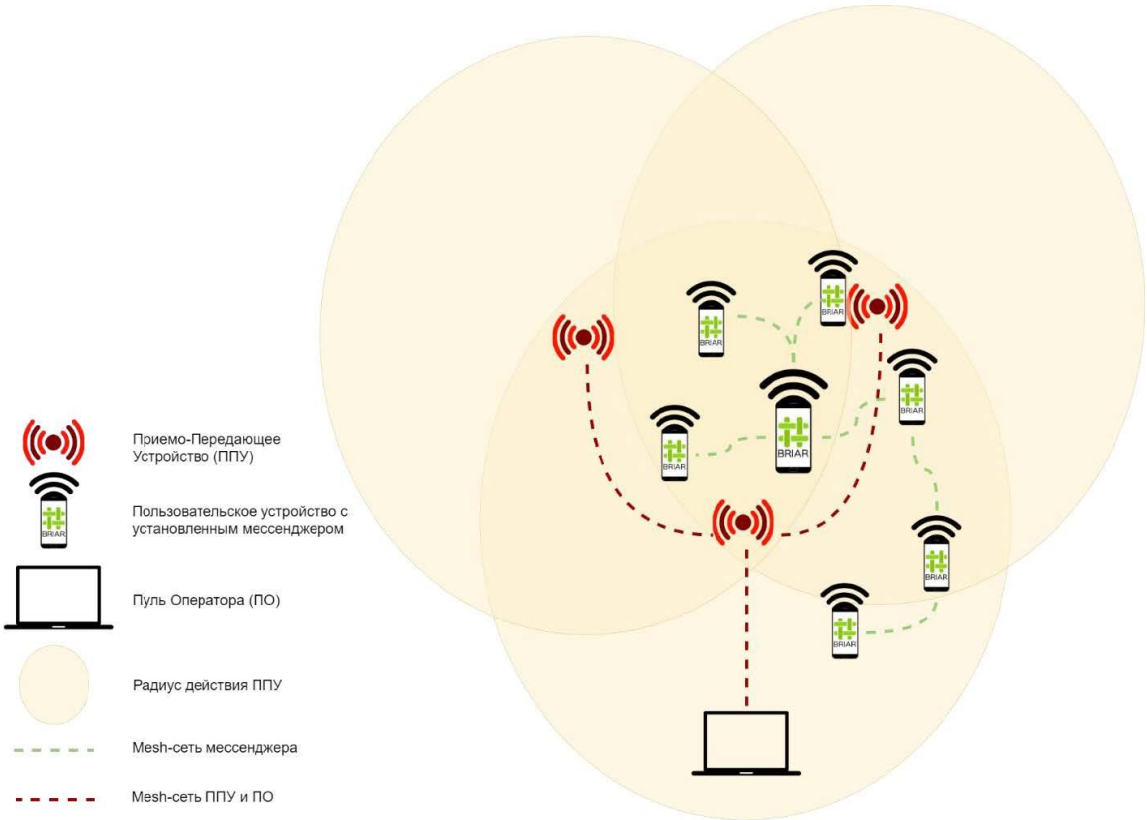

рис. 1. *Модель применения ПАК «Отвертка»*

На рис. 2 представлена архитектура данного комплекса.

рис. 2. *Архитектура ПАК «Отвертка»*ППУ содержит 4 основных компонента, необходимых для его работы:

- управляющий модуль ППУ;
- мобильное устройство;
- локальную базу данных;
- беспроводной Wi-Fi/Bluetooth-модуль.

Управляющий модуль ППУ отвечает за прием команд управления с ПуО и ППУ, а также отправку результатов выполнения полученных команд.

Локальная база данных ППУ используется для накопления и первичного анализа информации, поступающей с беспроводных Wi-Fi/Bluetooth-модулей ППУ, а также для фиксации результатов выполненных команд.

Беспроводной Wi-Fi/Bluetooth-модуль используется ППУ для отправки сетевых пакетов определенной структуры в зависимости от поступившей команды.

Мобильное устройство необходимо для взаимодействия с меш-приложениями, в том числе для регулирования доступа сторонних устройств.

ПуО содержит 2 основных компонента, необходимых для его работы:

- графическая оболочка оператора ПуО;
- глобальная база данных.

Графическая оболочка оператора ПуО используется для отображения всей агрегированной и обработанной информации, полученной от нескольких ППУ и отправки команд на ППУ.

Глобальная база данных представляет собой совокупность всех локальных баз данных ППУ, а также результатов анализа и поиска корреляций, проведенных над полученной с ППУ информацией.

Таким образом, выбраны эффективные техники и методы, затрудняющие и блокирующие обмен в меш-сетях, а именно приводящие к отказу в обслуживании пользователей из-за невозможности подключения к точке доступа, к созданию условий для постоянного процесса смены каналов пользователей, что приводит к DoS-атаке, а также к осуществлению многократной отправки широковещательных кадров с командой диассоциации пользователей от точки доступа. Также применена техника засорения рекламными кадрами BR/EDR эфира Bluetooth со случайным аппаратным адресом. Обмен становится невозможен, так как абонент не успевает подключиться.

Меш-сети привлекают внимание пользователей различных меш-мессенджеров как децентрализованная форма связи, позволяющая напрямую соединяться друг с другом, не полагаясь на традиционную интернет-инфраструктуру. Эти сети могут использоваться отдельными лицами или сообществами для создания анонимных сетей связи, особенно в районах с ограниченным доступом в Интернет или без него, для осуществления противоправной деятельности.

Пресечение незаконной деятельности, совершаемой с использованием меш-сетей, требует системного подхода, включающего технологические достижения, нормативно-правовую базу, совместные усилия, осведомленность общественности и международное сотрудничество. Крайне важно найти правильный баланс между противодействием незаконной деятельности и сохранением прав на неприкосновенность частной жизни. Хотя полное искоренение может быть сложной задачей, согласованные усилия могут значительно смягчить воздействие незаконной деятельности на меш-сети и способствовать созданию безопасной и защищенной цифровой среды.

Технические решения, выработанные и экспериментально исследованные в результате выполнения научно-исследовательской работы «Обоснование и выбор методов контроля анонимных сетей обмена информацией», шифр «Отвертка», выступают научно обоснованным фундаментом разработки программно-аппаратного комплекса для регулирования работы пользователей меш-мессенджеров, использующих технологии Bluetooth и Wi-Fi, а также мониторинга активности пользователей меш-мессенджеров и сбора статистической информации о пользователях и их устройствах.

1. Security and Privacy Issues in Wireless Mesh Networks: A Survey [Электронный ресурс] – Режим доступа: https://arxiv.org/ftp/arxiv/papers/1302/1302.0939.pdf
2. Common Security Issues and Challenges in Wireless Sensor Networks and IEEE 802.11 Wireless Mesh Networks [Электронный ресурс] – Режим доступа: https://core.ac.uk/download/pdf/336226.pdf

3. Analysis of Denial of Service Attacks in IEEE 802.11s Wireless Mesh Networks [Электронный ресурс] – Режим доступа: https://eudl.eu/pdf/10.1007/978-3-642-11530-1_1
4. 6 лучших мессенджеров, которые работают без сотовой связи и Интернета [Электронный ресурс] – Режим доступа: https://rusmonitor.com
5. Bluetooth Low Energy Mesh Networks: Survey of Communication and Security Protocols [Электронный ресурс] – Режим доступа: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349184/
6. Кубасов И.А., Лекарь Л.А. Перспективы организации обмена оперативно значимой информацией с использованием транспортного уровня пиринговых сетей // Оперативно-розыскной портал: право и технологии. 2023. № 1 (3).
7. Кубасов И.А., Лекарь Л.А., Кондрущенков О.М. Перспективные направления применения методов анализа больших данных в информационно-аналитическом обеспечении оперативно-разыскной деятельности // Стратегическое развитие системы МВД России: состояние, тенденции, перспективы: сб. ст. междунар. науч.-практ. конф. (Москва, 23 октября 2020 г.) / под общ. ред. И.Г. Чистобородова, А.Л. Ситковского, В.О. Лапина. – М.: Академия управления Министерства внутренних дел Российской Федерации, 2020.
8. Конуров А.Г., Кубасов И.А., Синютин Ю.В. О необходимости формирования у сотрудников органов внутренних дел Российской Федерации навыков по применению специальной техники в едином цифровом пространстве МВД России // Вестник Всероссийского института повышения квалификации сотрудников Министерства внутренних дел Российской Федерации. 2021. № 4 (60).
9. Кубасов И.А. Промышленный Интернет вещей как революционный скачок развития // Надежность и качество сложных систем. 2023. № 2 (42). DOI 10.21685/2307-4205-2023-2-9.
10. Отчет о научно-исследовательской работе «Обоснование и выбор методов контроля анонимных сетей обмена информацией» (заключительный). Шифр «Отвертка». – М.: ФКУ НПО «СТиС» МВД России, 2022. Рег. № НИОКТР 01220005.

Информация об авторе:

Л.А. Лекарь, *доцент кафедры информационных технологий, кандидат технических наук*
И.А. Кубасов, *доктор технических наук, доцент, профессор кафедры информационных технологий*

About the author:

L.A. Lekar, *Associate professor of Department of Information Technology, Candidate of Technical Sciences*
I.A. Kubasov, *Professor of the Department of Information technologies, doctor of technical sciences, associate professor*

Статья поступила в редакцию 2.10.2023