АКАДЕМИЯ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ОХРАНЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

На правах рукописи

Маркин Дмитрий Олегович

УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ МОБИЛЬНЫХ АБОНЕНТСКИХ УСТРОЙСТВ В КОРПОРАТИВНЫХ СЕТЯХ

Специальность 05.13.19 – Методы и системы защиты информации, информационная безопасность

Диссертация на соискание ученой степени
кандидата технических наук

Научный руководитель:
кандидат технических наук, доцент
Комашинский Владимир Владимирович

Орёл 2017

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность темы. Развитие современных многофункциональных мобильных абонентских устройств (МАУ) [69] и информационных технологий, пропускной способности каналов связи, в том числе беспроводных, приводят к постоянному росту потребности в доступе к информации [71], причем независимо от того, где находится пользователь. В этом отношении не являются исключением и корпоративные сети, в том числе, защищенные (ЗКС), предоставляющие доступ к инфокоммуникационным услугам и ресурсам с разными требованиями по защищенности. К таким сетям относятся, в том числе, информационные системы общего пользования, информационные системы, обрабатывающие персональные данные, а также геоинформационные системы.

Удаленный доступ с использованием МАУ к корпоративным сетям с разными требованиями по защищенности подразумевает применение соответствующих систем защиты безопасности, позволяющих обеспечить требуемый уровень обеспечения безопасности информации независимо от уровня защищенности сегмента защищенной корпоративной сети. При этом принципиальным требованием является использовании сотрудниками (пользователями) ЗКС единого мобильного устройства для осуществления такого доступа. Различие по требованиям защищенности в ЗКС, как правило, делит такую сеть на контуры обработки информации, которые, в свою очередь, обычно ограничены специализированными помещениями с известным расположением на объектах организации.

Однако использование современных МАУ, обладающих значительными вычислительными и коммуникационными ресурсами, для обработки конфиденциальной информации ограничено в связи с рядом существенных особенностей, касающихся их эксплуатации: размерами, мобильностью пользователей, многофункциональностью.

Указанные особенности определяют совершенно иной спектр угроз информационной безопасности при работе с МАУ по сравнению со стационарными средствами вычислительной техники (СВТ). Постоянная смена местоположения

пользователей МАУ, беспроводный удаленный доступ к сетям с разными требованиями по защищенности, ограниченные вычислительные возможности с одной стороны и высокоскоростные коммуникационные с другой создают большое количество угроз информационной безопасности, связанных в первую очередь с угрозами нарушения конфиденциальности информации [17].

С другой стороны перспективным направлением совершенствования современных корпоративных сетей является обеспечение предоставления защищенного доступа абонентам к информации и услугам с разными требованиями по защищенности при использовании единого МАУ [10, 30, 58]. При этом к предоставляемым услугам в соответствие относятся:

– телефонная и видеосвязь с дополнительными видами обслуживания;

– защищенный электронный почтовый обмен с элементами учета входящих и исходящих документов;

– видеоконференцсвязь;

– доступ к базам и банкам данных, сетевым приложениям и информационным ресурсам.

Необходимость предоставления указанного перечня услуг с использованием одного универсального абонентского устройства пользователям, учитывая, что услуги могут предоставляться сетями с разными требованиями по защищенности, позволяет говорить о том, что существует объективная потребность в разработке универсального МАУ и системы защиты информации (СЗИ), позволяющей обеспечить конфиденциальность информации [17] при своевременном [18] предоставлении доступа к указанному перечню услуг с использованием одного МАУ. Задачей СЗИ будет являться обеспечение безопасности информации при доступе к услугам сетей с разными требованиями по защищенности с использованием МАУ, путем управления безопасностью МАУ с помощью адаптивного изменения его программно-аппаратной конфигурации, позволяющего согласовывать состояние МАУ с условиями (атрибутами) доступа, требованиям безопасности корпоративной сети, а также требованиями по качеству предоставляемых услуг.

Анализ существующих научных исследований [47], технических и программно-аппаратных решений, а также нормативно-правовой базы в области защиты информации при работе с МАУ показал, что в настоящее время:

1) существующие технические решения, позволяющие управлять функциональностью (конфигурацией) МАУ, не предполагают определения вероятности нахождения пользователя МАУ в специальных помещениях, к которым предъявляются повышенные требования по обеспечению информационной безопасности (ИБ) в корпоративной сети, и не позволяют заблаговременно предотвращать работу МАУ тех режимах, которые при текущем местоположении МАУ запрещены;

2) доступ к сетям с разными требованиями по защищенности осуществляется либо с использованием нескольких зарегистрированных в корпоративной сети МАУ, соответствующих необходимому уровню защиты либо с использованием автоматизированного переключения режимов работы; отсутствует автоматическое управление МАУ в зависимости от требований защищенности сети, к которой предоставляется доступ, а также местоположения МАУ; в случае доступа к информационным ресурсам сторонней организации с использованием личных или корпоративных МАУ в настоящее время действуют организационно-технические ограничения.

В данном направлении исследований существенные результаты в области изучения моделей безопасности управления доступом в отечественных и зарубежных научных трудах получены под руководством Девянина П. Н., Зегжды Д. П., Гайдамакина Н. А., Бочкова М. В., Герасименко В. А., Бородакий Ю. В., Маклина Дж., Самарати П., Сандху Р. Исследования проблем защиты информации, в том числе и проблем анализа защищенности информации проводились под руководством Ломако А. Г., Молдовяна А. А., Стародубцева Ю. И., Окова И. Н., Остапенко А. Г., Шелупанова А. А., Котенко И. В. В области вопросов мобильной радиосвязи и радиодоступа, средств широкополосного доступа, безопасности беспроводных сетей доступа известны работы Челышева В. Д., Кловского Д. Д., Коржика В. И., Вишневского В. М., Шахновича И. В., Баскакова С.И., Зюко А. Г. и других. В области защиты информации при эксплуатации

МАУ известны работы Гузаирова М. В., Машкиной И. В., Бабикова А. Ю., Десницкого В. А. и Карпеева Д. О.. Однако вопросы управления безопасностью МАУ для обеспечения доступа к услугам корпоративных сетей с разными требованиями по защищенности рассмотрены недостаточно полно.

На основе анализа тенденций и перспектив развития современных корпоративных сетей выявлено **противоречие** между требованиями, предъявляемыми к безопасности информации [18] при доступе к защищенным услугам и информации с использованием универсальных МАУ, и техническими возможностями СЗИ, позволяющих обеспечить безопасность информации при осуществлении такого доступа в корпоративных сетях с разными требованиями по защищенности.

На основании этого выдвинута **гипотеза исследования**, заключающаяся в том, что для повышения вероятности обеспечения безопасности информации при эксплуатации МАУ и обеспечении безопасного доступа к услугам корпоративных сетей с разными требованиями по защищенности необходимо разработать модель безопасности МАУ и алгоритм, позволяющий управлять безопасностью (программно-аппаратной конфигурацией) МАУ, согласовывая его с требованиями по ИБ и качеству предоставляемых услуг, в зависимости от условий предоставления доступа к услугам и ресурсам, в которых находится МАУ, а также научно-технические предложения по реализации системы управления безопасностью МАУ в корпоративных сетях с разными требованиями по защищенности.

Перечисленные факторы обусловливают **актуальность темы** диссертационного исследования: "Управление безопасностью мобильных абонентских устройств в корпоративных сетях".

Объект исследования: система управления безопасностью МАУ в корпоративных сетях с разными требованиями по защищенности.

Предмет исследования: модели и алгоритмы управления безопасностью МАУ.

Цель исследования: повышение вероятности обеспечения безопасности информации при доступе к инфокоммуникационным услугам и информации в

корпоративных сетях с разными требованиями по защищенности при использовании единого МАУ.

Научная задача исследования: на основе формальной модели безопасности МАУ разработать алгоритм управления безопасностью МАУ, учитывающий атрибуты доступа пользователей и МАУ, включая его местоположение, требования по качеству предоставляемых услуг, а также научно-технические предложения по реализации системы управления безопасностью МАУ, позволяющие повысить вероятность обеспечения безопасности информации при доступе к инфокоммуникационным услугам и информации корпоративных сетей с разными требованиями по защищенности при использовании единого МАУ.

Частные научные задачи исследования:

1) провести анализ существующих научных исследований и технических решений по защите информации в МАУ, а также способов построения систем защиты информации при доступе к сетям с разными требованиями по защищенности с использованием единого устройства; разработать систему показателей качества, позволяющую оценить эффективность процесса защиты информации при эксплуатации системы управления безопасностью МАУ в корпоративных сетях с разными требованиями по защищенности;

2) разработать формальную модель безопасности МАУ, отличающуюся от известных учетом местонахождения МАУ в специальных помещениях, к которым предъявляются повышенные требования по ИБ, обосновать ее корректность;

3) разработать алгоритм управления безопасностью МАУ, учитывающий атрибуты доступа пользователей МАУ, включающие в себя, в том числе, вероятность нахождения МАУ в специальном помещении, а также требования по качеству предоставляемых услуг; разработать моделирующий алгоритм и осуществить имитационное моделирование функционирования системы управления безопасностью МАУ для получения оценки эффективности предложенных технических решений;

4) сформировать научно-технические предложения по практической реализации системы управления безопасностью МАУ в корпоративных сетях, а также

рекомендации по выбору параметров алгоритмов определения местоположения МАУ в помещениях корпоративной сети и алгоритма вычисления вероятности нахождения МАУ в специальном помещении.

Решение научной задачи основывается на использовании теории машинного обучения, теории вероятности и математической статистики, аппарата скрытых марковских моделей, теории алгоритмов, теории управления, теории множеств, теории оптимизации, численных методов и методов математического и имитационного моделирования.

Основные положения, выносимые на защиту:

1. **Модель безопасности мобильного абонентского устройства** в корпоративных сетях с разными требованиями по защищенности [39, 46, 50, 43, 51, 76, 79].

2. **Алгоритм управления безопасностью мобильного абонентского устройства**, позволяющий определить оптимальную программно-аппаратную конфигурацию устройства с учетом атрибутов доступа и требований по безопасности и качеству услуг [41, 48, 49, 77].

3. **Система управления безопасностью мобильных абонентских устройств**, обеспечивающая повышение вероятности обеспечения безопасности информации при доступе к инфокоммуникационным услугам и информации корпоративных сетей с разными требованиями по защищенности при использовании единого МАУ [40, 45, 47, 60, 61, 62, 75, 78, 80].

Научная новизна диссертационной работы заключается:

– в разработке и обосновании корректности новой формальной модели безопасности МАУ, отличающейся от известных учетом оценки его местонахождения в специальном помещении, других атрибутов доступа, а также реализацией требований мандатной и ролевой политик безопасности в корпоративных сетях с разными требованиями в отношении единого МАУ;

– в разработке нового алгоритма управления безопасностью МАУ, отличающегося от известных определением оптимальной, с точки зрения обеспечения конфиденциальности информации и качества предоставляемых пользователю

услуг, программно-аппаратной конфигурации МАУ с учетом вероятности его нахождения в специальных помещениях и других атрибутов доступа;

– в разработке системы управления безопасностью мобильных абонентских устройств, отличающейся возможностью удаленного управления программно-аппаратными конфигурациями МАУ в зависимости от условий доступа, требований политик безопасности и качества предоставляемых услуг для обеспечения защищенного доступа к инфокоммуникационным услугам и информации корпоративных сетей с разными требованиями по защищенности.

Практическая новизна диссертационной работы заключается:

– в разработке научно-технических предложений по практической реализации системы управления безопасностью МАУ в корпоративных сетях, позволяющих повысить вероятность обеспечения безопасности информации при удаленном доступе к инфокоммуникационным услугам и ресурсам в сетях с разными требованиями по защищенности при использовании единого МАУ;

– в разработке рекомендаций по формированию оптимальных параметров системы определения местоположения МАУ, позволяющих повысить достоверность вычисления его местонахождения в специальных помещениях.

Теоретическая значимость выполненных в диссертации исследований состоит в разработке формального аппарата моделирования безопасности МАУ в корпоративных сетях с учетом его местоположения в специальных помещениях, а также разработке алгоритма оптимизации программно-аппаратной конфигурации (безопасности) МАУ, позволяющего повысить вероятность обеспечения безопасности информации при доступе к инфокоммуникационным услугам и информации корпоративных сетей с разными требованиями по защищенности при использовании единого МАУ за счет учета требований по ИБ и качеству предоставляемых услуг в корпоративной сети.

Практическая значимость работы заключается:

1) в исследовании эффективности известных способов и систем определения местоположения МАУ при их использовании внутри здания в заданных помещениях и обосновании оптимальных параметров алгоритмов определения ме-

стоположения МАУ, позволяющих повысить достоверность определения местонахождения МАУ в специальных помещениях;

2) в реализации предложенных алгоритмов в виде комплекса программ для ЭВМ и проверке возможности их применения в корпоративной сети;

3) в разработке научно-технических предложений по практической реализации системы управления безопасностью МАУ, повысить вероятность обеспечения безопасности информации при доступе к инфокоммуникационным услугам и информации корпоративных сетей с разными требованиями по защищенности при использовании единого МАУ.

Структурно диссертационная работа состоит из введения, четырех разделов, заключения, библиографического списка, включающего 150 источник, 2 приложений. Текст диссертации изложен на 234 страницах, включая 52 рисунка и 31 таблицу.

В **первом разделе** проведен анализ состояния научных исследований в области защиты информации при использовании МАУ. Рассмотрены существующие формальные модели безопасности компьютерных систем, выделены их недостатки в случае их использования применительно к МАУ. Изучены отличительные особенности МАУ, влияющие на обеспечение безопасности информации. Выделены актуальные факторы, воздействующие на безопасность информации. На их основе разработана модель угроз информации в корпоративных сетях при доступе к ней пользователей МАУ. Проведен анализ современных технических решений по защите информации в МАУ. Проанализированы способы построения комплексных СЗИ при доступе к сетям с разными требованиями по защищенности. Сформулирована задача диссертационного исследования.

Во **втором разделе** предложена модель безопасности МАУ, отличающаяся от известных учетом его местонахождения в специальных помещениях, к которым предъявляются повышенные требования по ИБ. Показано, что основным параметром, вносящим неопределенность для определения условий предоставления доступа МАУ, является его местоположение. Исследованы современные подходы, используемые в технологиях определения местоположения пользователей МАУ в

помещениях внутри здания. В ходе исследований установлено, что для определения данного параметра необходимо использовать технологии определения местоположения пользователей МАУ в помещениях внутри здания с использованием сигналов беспроводных сетей передачи данных (БСПД) в диапазонах частот 2,4-5 ГГц (стандарт 802.11). Для обоснования алгоритмической разрешимости задачи определения местоположения и вычисления вероятности нахождения МАУ в специальном помещении на основе использования БСПД исследована эффективность технологий определения местоположения на основе методов трилатерации, k-ближайших соседей и байесовского подхода (скрытой марковской модели). Предложено использовать теорию машинного обучения и метод статистических испытаний (метод Монте-Карло) в качестве численного метода, позволяющего получить оценку вероятности нахождения МАУ в специальном помещении на основе известной карты помещений корпоративной сети и предварительных исследований статистики ошибок определения местоположения. Осуществлена оценка качества предложенной модели. Приведены результаты моделирования с численным примером расчета.

В **третьем разделе** представлено описание разработанного алгоритма управления безопасностью МАУ и входящих в его состав компонентов, включающих комплекс алгоритмов определения местоположения МАУ, в том числе, алгоритм вычисления вероятности нахождения МАУ в специальном помещении, а также алгоритм формирования конфигурации МАУ в зависимости от текущих атрибутов доступа и действующей в корпоративной сети политики безопасности МАУ и оценки информационной скорости передачи данных в БСПД. Осуществлена проверка основных свойств алгоритма. Получена оценка эффективности разработанного алгоритма.

В **четвертом разделе** описаны научно-технические предложения по практической реализации системы управления безопасностью МАУ в корпоративных сетях. Разработаны рекомендации по формированию оптимальных параметров системы определения местоположения. Проведено комплексное оценивание эффективности разработанных научно-технических предложений с расчетом показа-

телей эффективности системы управления безопасностью МАУ в корпоративных сетях.

В **заключении** перечислены полученные научные и практические результаты, раскрыта степень их новизны и значение для теории и практики, а также предложены перспективные направления дальнейших исследований, направленных на повышение вероятности обеспечения безопасности информации при эксплуатации МАУ в корпоративных сетях с разными требованиями по защищенности.

Апробация работы и ее основных результатов, полученных в ходе работы, была осуществлена на следующих конференциях:

– 6, 7-я Межрегиональные научно-практические конференции "Информационная безопасность и защита персональных данных: Проблемы и пути их решения" (г. Брянск, БГТУ, 2014, 2015, 2016 гг.) [39, 40, 42, 52];

– 12-е Всероссийское совещание по проблемам управления ВСПУ-2014 (Москва, ИПУ им. В. А. Трапезникова РАН, 16-19 июня 2014 г.) [49];

– Международной научно-технической конференции "Перспективные информационные технологии (ПИТ 2015)" (г. Самара, Самарский научный центр РАН, 2015, 2016 гг.) [50, 53].

Публикации по теме диссертационной работы включают в себя 6 статей, в том числе 5 статей в рецензируемых журналах, входящих в перечень ВАК Минобрнауки России, 7 тезисов докладов, 6 свидетельств об официальной регистрации программ для ЭВМ: № 2013612870 от 14.03.2013 г. "DNS-коммутатор" [74], № 2013615947 от 24.09.2013 г. "Автоматизированная система оценки вероятности отказа в обслуживании запросов пользователей при построении сети как системы массового обслуживания" [75], № 2013618388 от 06.09.2013 г. "Анализатор контекста доступа мобильного устройства" [76], № 2014617119 от 11.07.2014 г. "Автоматизированная система оценки параметров защищенности удаленного доступа к услугам защищенной корпоративной сети пользователя мобильного устройства" [77], № 2014617940 от 06.08.2014 г. "Автоматизированная система мониторинга и управления информационной безопасностью сетевого трафика при

доступе к услугам информационных сервисов, использующих систему доменных имен" [78], № 2015615631 "Автоматизированная система определения местоположения пользователей мобильных устройств внутри здания на основе сигналов беспроводной сети" [79], № 20166111210 "Программный агент удаленного управления функциональностью мобильного абонентского устройства" [80], 3 патента на изобретения: № 2503059 от 27.12.2013 г. "Способ удаленного мониторинга и управления информационной безопасностью сетевого взаимодействия на основе использования системы доменных имен" [60], № 2530691 от 10.10.2014 г. "Способ защищенного удаленного доступа к информационным ресурсам" [61], № 2546236 от 10.04.2015 г. "Способ анализа информационного потока и определения состояния защищенности сети на основе адаптивного прогнозирования и устройство для его осуществления" [62].

Акты внедрения научных результатов диссертационного исследования получены в Спецсвязи ФСО России, ФГУП "Государственный научно-исследовательский институт прикладных проблем" ФСТЭК России.

1. АНАЛИЗ СОСТОЯНИЯ НАУЧНЫХ ИССЛЕДОВАНИЙ И ТЕХНИЧЕСКИХ РЕШЕНИЙ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ИСПОЛЬЗОВАНИИ МОБИЛЬНЫХ АБОНЕНТСКИХ УСТРОЙСТВ

В данном разделе проведен анализ условий функционирования и требований, предъявляемых к МАУ в корпоративных сетях, недостатков существующих средств защиты информации и проблем, связанных с обеспечением безопасности информации при работе с МАУ. Дана характеристика существующим формальным моделям безопасности компьютерных систем и системам контроля доступа, построенным на их основе. Выделены недостатки существующих формальных моделей при использовании их в отношении современных МАУ. Исследованы критические с точки зрения обеспечения безопасности информации особенности современных МАУ. На основе анализа нормативно-правовых документов выделен перечень актуальных факторов, воздействующих на безопасность информации при эксплуатации МАУ, а также предложены модели угроз и нарушителя, отражающие состав угроз безопасности информации и возможности нарушителей безопасности при использовании МАУ в корпоративных сетях с разными требованиями по защищенности. Проведен анализ существующих защищенных МАУ, программных и программно-аппаратных мобильных технических решений, а также технических решений, позволяющих осуществлять доступ к сетям с разными требованиями по защищенности с использованием одного абонентского устройства. Описаны особенности эксплуатации МАУ в защищенных корпоративных сетях. Обоснована необходимость учета местоположения МАУ в корпоративной сети для обеспечения эффективной работы СЗИ. Проведен анализ способов и технических решений по определению местоположения МАУ в помещениях внутри здания, представлена их классификация, выделены их достоинства и недостатки. Обосновано использование БСПД для решения задачи вычисления вероятности нахождения МАУ в специальных помещениях. Сформулирована научная задача диссертационного исследования.

1.1. Условия функционирования и требования, предъявляемые к мобильным абонентским устройствам

В настоящее время использование современных МАУ в защищенных корпоративных сетях существенно ограниченно в связи с отсутствием эффективных СЗИ, гарантирующих обеспечение безопасности информации. Вместе с тем перспективным направлением совершенствования современных корпоративных сетей является обеспечение защищенного доступа абонентам к информации и услугам с разными требованиями по защищенности при использовании единого МАУ [10, 30, 58].

Современные корпоративные сети, в которых предусмотрено использовние МАУ, представляют собой аналоги структуры [30, 58], представленной на рисунке 1.1.

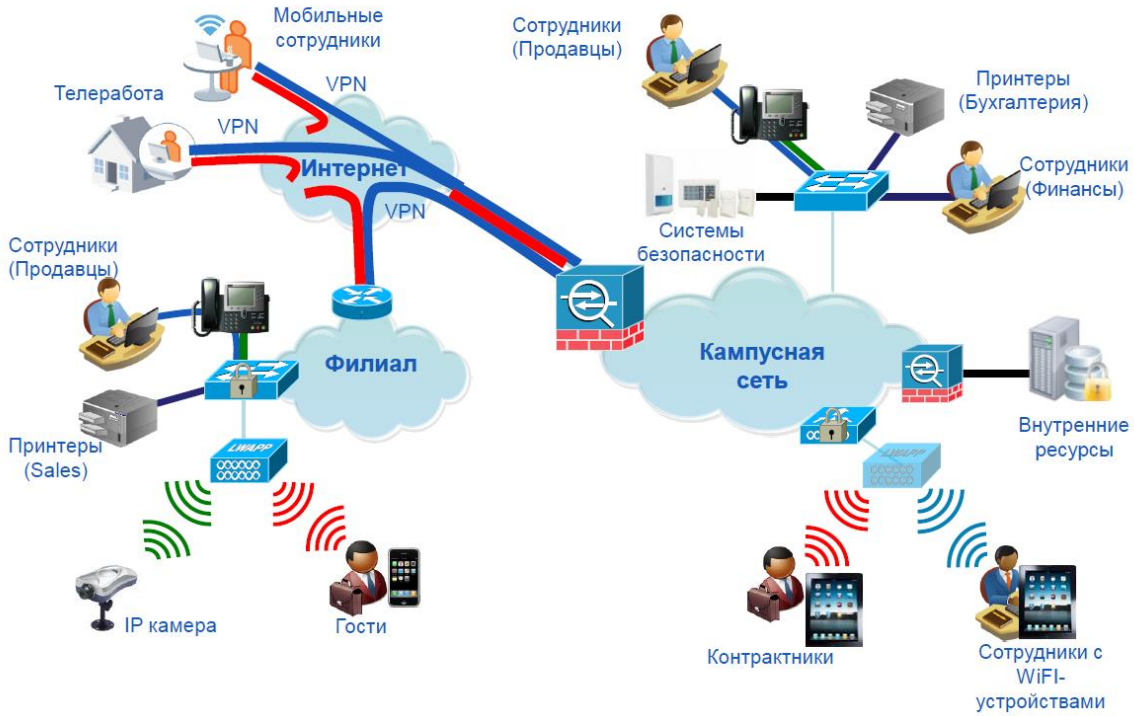


Рисунок 1.1 – Типовая структура корпоративных сетей с МАУ

При наличии в организации информации, требующей более высокого уровня защиты, внутри нее создаются несколько корпоративных сетей с разными требованиями по защищенности. Как правило, для получения доступа к ресурсам корпоративных сетей с разными требованиями по защищенности используются различные МАУ с необходимыми уровнями защищенности, что создается определенные неудобства. Для решения данной проблемы и обеспечения безопасности информации при работе на едином МАУ в настоящее время используется два подхода:

– установка специализированных СЗИ (MDM-решения) [3, 30, 55, 58] на личные МАУ сотрудников организации в рамках концепции BYOD (Bring Your Own Device);

– эксплуатация корпоративных защищенных МАУ [2, 35, 55, 83, 84, 85, 88].

Однако данные решения не обладают достаточной эффективностью с точки зрения защиты информации по различным причинам [3, 23, 25, 27, 41, 46]:

– отсутствуют обоснованные формальные модели безопасности компьютерных систем, в которых предусмотрена эксплуатация МАУ и учитывается мобильность пользователей;

– системы определения местоположения МАУ в помещениях на территории организации, как правило, строятся на основе БСПД стандарта 802.11 [43, 51] и обладают низкой точностью с ошибкой определения местоположения порядка 2 метров, что создается угрозу некорректного применения установленной в корпоративной сети политики безопасности МАУ;

– существующие MDM-решения [55, 58, 146] и корпоративные защищенные МАУ [2, 35, 84, 85] не предполагают аппаратной переконфигурации МАУ, что является причиной наличия технических каналов утечки информации внутри устройства за пределы контролируемой зоны;

– большинство современных МАУ построены на базе импортной электроники, которая не является доверенной [23], а существующие методики сертификации СЗИ не позволяют гарантировать отсутствие программных и аппаратных закладок.

Несмотря на наличие современных СЗИ, направленных на обеспечение безопасности информации при работе с МАУ, принципиальной проблемой является вопрос доверия к аппаратным платформам МАУ, которые реализуются, как правило, на базе импортной электроники и технологии SoC (System-on-Chip). Согласно исследованиям компании "Алладин Р. Д." [23] в большинстве современных МАУ используется архитектура ARM процессоров, в которых внедрена технология "TrustZone", разработанная английской компанией ARM. Сделано это для аппаратной изоляции (виртуализации) двух параллельных процессов – доверенного (безопасного) в рамках работы, так называемой ОС "Secure OS" и обычного (где работают приложения под управлением привычных операционных систем – Android, iOS, Linux, Tizen, Sailfish) – "RichOS" (гостевая ОС) [23]. Доверенные процессы в "TrustZone" обладают полным контролем над обычной ОС, включая полицейские функции и функции разведки. Приложения из "TrustZone" управляются доверенной операционной системой "Secure OS", которая внедряется в микросхему на этапе ее производства. При этом обычная ОС "RichOS", например, Android не имеет функциональных возможностей по определению наличия ОС "Secure OS". Данное исследование [23] также показало, что в более 95% современных процессорах с ARM-архитектурой внедрена технология "TrustZone", включая защищенные смартфоны типа "Коперник С1", Samsung Z3, YotaPhone, YotaPhone 2, а также сертифицированные ОС "Android 6.0 Marshmallow", ядро Astra Linux Special Edition 1.4 (релиз "Новороссийск" для ARM), ядро Linux 4.5.

Анализ нормативно-правовой базы и требований по обеспечению ИБ при использовании в защищенных корпоративных сетях [10, 18] показал, что:

– существуют особые требования системы ИБ в отношении эксплуатации МАУ в защищенных корпоративных сетях;

– использование личных МАУ в ЗКС запрещено либо существенно ограничено в рамках принципа BYOD с учетом выполнения требований системы ИБ;

– абонентские устройства (сотовые телефоны, смартфоны, планшетные компьютеры и т.п.) стандарта IEEE 802.11 должны отвечать требованиями корпоративной политике ИБ в ЗКС;

– оборудование сети Wi-Fi также должно отвечать требованиями корпоративной политике ИБ в ЗКС.

Очевидно, что доступность защищенных инфокоммуникационных услуг связи при использовании личных МАУ в ЗКС существенно ограничена. Открытые услуги, предоставляемые с использованием личных МАУ, могут быть и вовсе недоступны. Вместе с тем современные МАУ позволяют получать доступ к широкому перечню услуг. Сравнительный анализ количества представляемых различными МАУ [2, 27, 28, 35, 54, 55, 83, 84, 88] услуг представлен на рисунке 1.2.

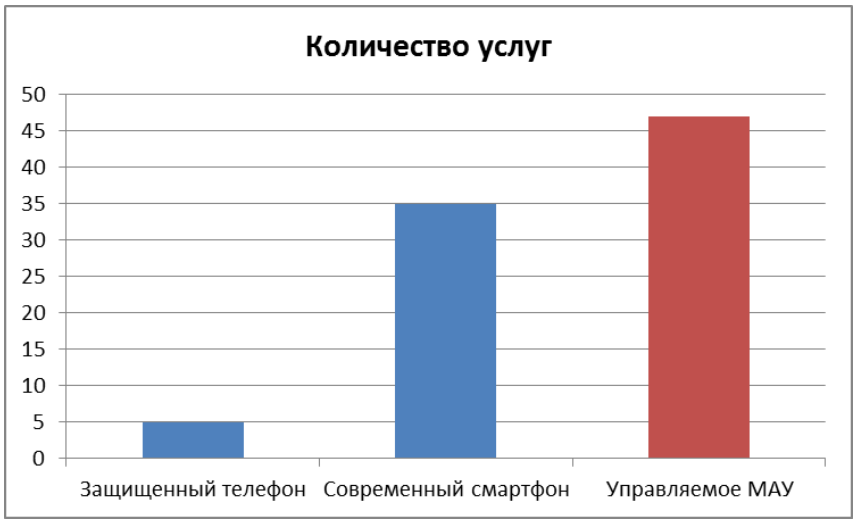


Рисунок 1.2 – Сравнительный анализ количества услуг, предоставляемых МАУ

В связи с отсутствием эффективных СЗИ, позволяющих обеспечить безопасность информации, эксплуатация МАУ для доступа к перечню услуг, включающих в себя, как защищенные, так и незащищенные, в ЗКС существенно ограничена. Повысить вероятность обеспечения безопасности информации при доступе к услугам и ресурсам ЗКС предлагается за счет использования управляемого МАУ, взаимодействующего с системой управления безопасностью МАУ, позволяющей управлять программно-аппаратной конфигурацией МАУ в зависимости от условий его эксплуатации (атрибутов доступа). Структура и топология системы управления безопасностью МАУ в корпоративной сети в этом случае может выглядеть так, как показано на рисунке 1.3 [30, 58].

Рисунок 1.3 – Структура и топология системы управления безопасностью МАУ в корпоративной сети

Основным недостатком подобной архитектуры системы управления безопасностью МАУ является отсутствие формальной модели безопасности МАУ, учитывающей при этом местоположение МАУ в корпоративной сети, доказательства ее корректности, а также недостаточно эффективные существующие технологии по определению местоположения МАУ в помещениях внутри здания. Указанные факторы свидетельствуют об актуальности рассматриваемой проблемы и необходимости решения поставленной научной задачи.

1.2. Модели безопасности компьютерных систем, включающих в свой состав мобильные абонентские устройства

Для формального описания процесса обеспечения безопасности информации в компьютерных системах и обоснования ее защищенности используют формальные модели безопасности, на основе которых строятся различные механизмы

защиты информации, включая систему контроля доступа. Основной задачей системы контроля доступа является предотвращение любой деятельности, которая может привести к *нарушению безопасности* компьютерной системы [25, 135]. Эта задача может решаться путем предотвращения действий или операций, которые могут выполнять в рамках системы пользователи или запущенные от имени пользователя процессы, а также путем ограничения доступных пользователю компьютерной системы действий.

Большинство современных систем управления доступом строится на основе модели Лэмпсона, описанной в работах [122, 123] и представленной на рисунке 1.4.

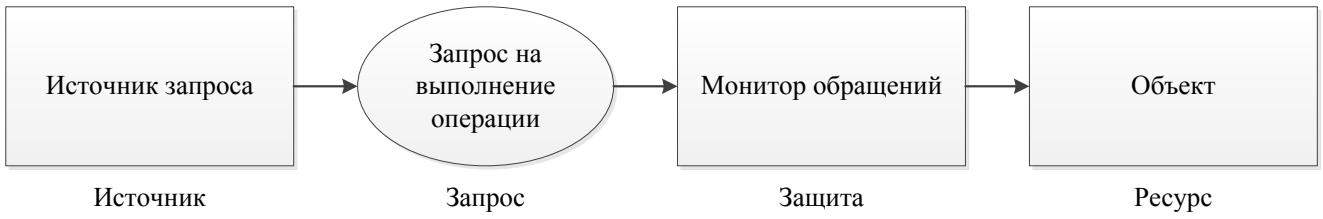


Рисунок 1.4 – Модель системы управления доступом Лэмпсона

В данной модели задача контроля доступа возлагается на монитор обращений, являющийся посредником при каждой попытке источника запроса обратиться к ресурсам системы (объектам доступа).

В существующей теории компьютерной безопасности для описания элементов компьютерной системы (КС) используется ряд понятий, таких как "сущность", "объект", "субъект", "доступ", "контейнер" [5]. В зависимости от текущих условий любая сущность КС может быть обозначена тем или иным понятием.

Для выполнения операций над сущностями КС субъекты осуществляют к ним доступы. В большинстве случаев рассматриваются:

– доступ на чтение из сущности;

– доступ на запись в сущность;

– доступ на запись в конец слова, описывающего состояние сущности;

– доступ на активизацию (исполнение) субъекта из сущности.

Остальные виды доступов, как правило, могут быть реализованы с использованием рассмотренных [25].

Система контроля доступа в КС создается как средство защиты от угроз безопасности информации. Согласно [26] при классификации угроз выделяют три основных свойства: конфиденциальность, целостность и доступность информации [18, 19, 72], которые и определяют три классических угрозы безопасности информации – угрозы конфиденциальности, целостности и доступности информации, а также еще одну – угрозу раскрытия параметров КС [25].

В соответствие с [19] управление доступом является одной из услуг защиты, входящих в общую архитектуру защиты информации наряду с такими услугами как аутентификация, конфиденциальность данных, целостность данных, безотказность. Для обеспечения тех или иных услуг защиты существуют специальные механизмы защиты [19], одним из которых является механизм управления доступом. В некоторых случаях для оказания ряда услуг защиты могут задействоваться несколько механизмов защиты.

В КС доступ субъекта к сущности разрешается системой управления доступом при наличии у субъекта соответствующего права доступа к сущности. Способ задания разрешенных прав доступа субъектов к сущностям КС регламентируется реализуемой в КС политикой управления доступом, являющейся составной частью политики безопасности КС [72].

Известны следующие виды политик управления доступом, определяющих способ задания разрешенных прав доступа субъекта к сущностям:

– дискреционная политика управления доступом [111];

– мандатная (полномочная) политика управления доступом [106];

– политика ролевого управления доступом [33, 139];

– политика безопасности информационных потоков [24];

– политика безопасности изолированной программной среды (ИПС) [97];

Формальные модели безопасности КС [25, с.25], описывающие порядок функционирования той или иной политики управления доступом, используются

для обоснования защищенности современных и перспективных КС. Очевидно, что технологическое развитие КС находится в постоянном движении и с появлением новых функциональных возможностей возникают и новые факторы, создающие угрозы безопасности информации, защита от которых в существующих формальных моделях безопасности не предусмотрена. Поэтому каждая новая формальная модель пытается учесть вновь возникающие факторы, приводящие к появлению новых угроз безопасности информации. Классификация и взаимосвязь ряда формальных моделей безопасности КС изображена на рисунке 1.5.

В настоящее время существуют и множество различных формальных моделей безопасности КС, ставящих перед собой цель с одной стороны осуществить более полный учет всех факторов, достижение которой позволить сделать модель безопасности КС более гибкой и адаптивной к условиям функционирования реальных КС, а с другой – использовать более совершенные механизмы управления доступом, упрощающие процедуры администрирования сложных КС.

К таким моделям безопасности КС можно отнести следующие:

– политика безопасности на основе решеток – LBAC (Lattice-Based Access Control) [136, 138];

– политика безопасности на основе местоположения – LBAC (Location-Based Access Control) [102, 110, 118, 129, 133];

– политика безопасности на основе контекста – CBAC (Context-Based Access Control) [100, 121, 141];

– атрибутная политика безопасности – ABAC (Attribute-Based Access Control) [94, 115, 148].

Помимо влияния допущений на безопасность КС при ее разработке серьезное влияние оказывает и невозможность учесть все возможные условия функционирования КС в реальной среде и, соответственно, выполнение требований безопасности КС.

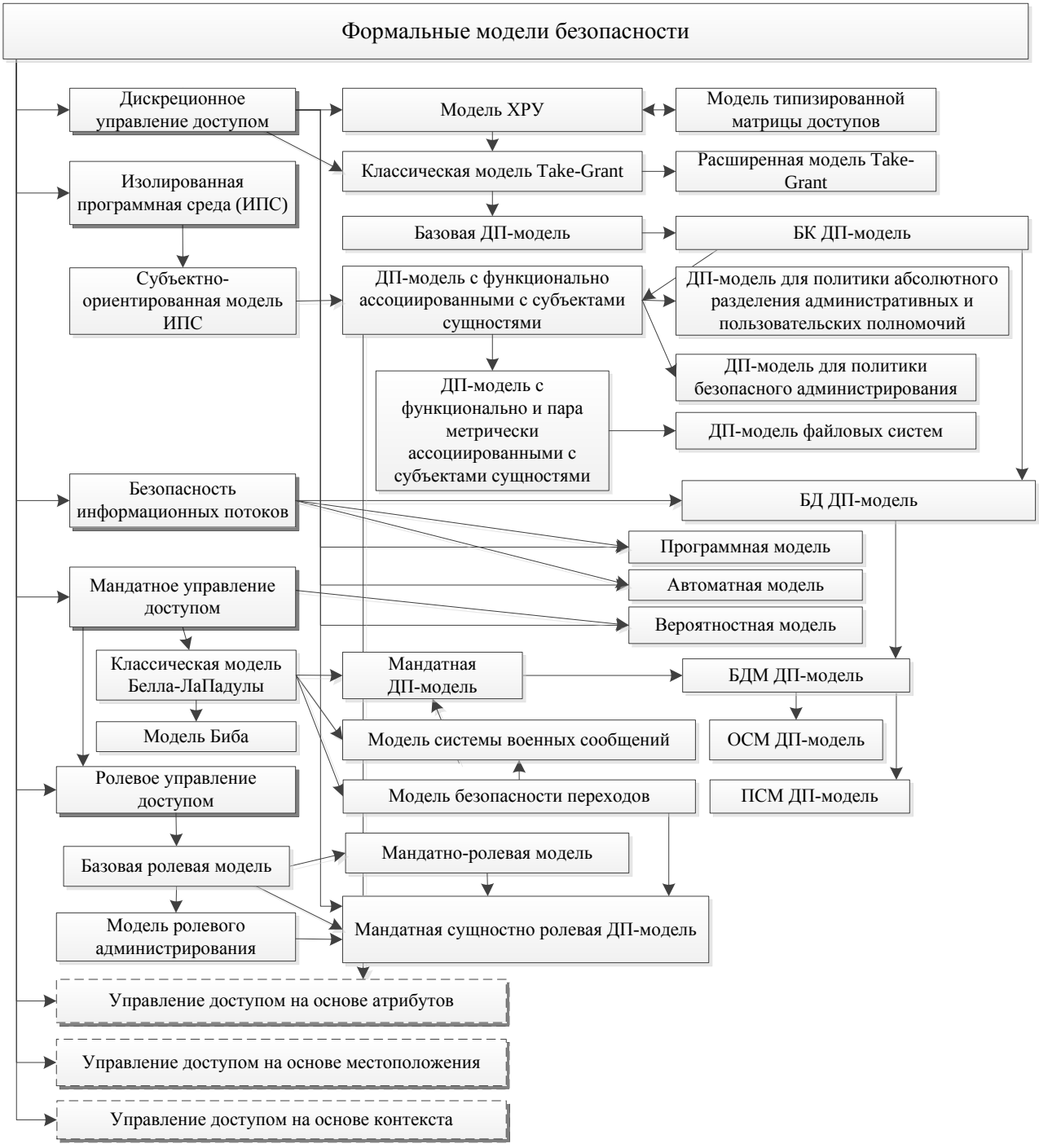


Рисунок 1.5 – Классификация и взаимосвязь отдельных формальных моделей безопасности КС

С точки зрения реализации формальных моделей безопасности для управления доступом пользователей МАУ возникает объективная потребность учитывать местоположение как фактор, влияющий на состояние безопасности информации в КС. В работах [102, 110, 118, 129, 133] приведено описание формальных

моделей безопасности КС, учитывающих местоположение пользователей и устройств. Однако при более детальном рассмотрении проблемы учета местоположения в данных моделях отчетливо виден ряд недостатков, серьезно влияющих на адекватность модели реальным КС и безопасность функционирования таких систем. К данным недостаткам относятся следующие:

– вопрос непосредственного определения местоположения как координат пользователей и устройств либо помещений, в которых находятся пользователи, выносится за рамки рассмотрения данных работ;

– не учитывается ошибка определения местоположения устройств, возникающая вследствие несовершенства современных способов определения местоположения МАУ, как на открытой местности, так и в помещениях внутри здания;

– не рассматривается вопрос оценки требований безопасности к устройствам, в зависимости от их местоположения и уровня требования по защищенности специальных помещений, в которых они находятся, а также уровня конфиденциальности информации и услуг, к которым запрашивается доступ;

– в качестве СЗИ в КС не используются возможности интеллектуального блокирования МАУ или их отдельных функциональных блоков, представляющих в определенных условиях доступа угрозу информационной безопасности в ЗКС.

Вывод: наличие указанных недостатков свидетельствует о том, что существующие модели безопасности КС, учитывающие такой фактор как местоположение устройств и пользователей, требуют серьезной доработки, поскольку не являются адекватными реальным КС и не гарантируют безопасность информации при использовании МАУ.

1.3. Модели угроз и нарушителя информационной безопасности при эксплуатации мобильных абонентских устройств и анализ технических решений для защиты от них

1.3.1. Характеристика и особенности современных мобильных абонентских устройств

Современные МАУ, обладающие и вычислительными и коммуникационными ресурсами, представляют собой многофункциональное медиаустройство, в котором функция телефонных переговоров не является первостепенно важной [93]. Для улучшения показателя экономичности основные узлы современных МАУ агрегированы в составе микросхемы класса SoC (System-on-Chip – системе на чипе), на которую возлагается весь перечень задач сбора, обработки, хранения и обмена пользовательской и служебной информацией [28]. Такая SoC зачастую объединяет на одном кристалле несколько ядер процессора, коммуникационный процессор, графический сопроцессор и др. Добавление при необходимости микроконтроллеров для кодирования речи, высокочастотных блоков для работы в различных стандартах сети сотовой связи, интерфейсных блоков Wi-Fi или иной беспроводной сети, модулей GPS/ГЛОНАСС/Galileo/Beidou, а также набор интерфейсов для взаимодействия с различными типами устройств (USB, SD, MMC, UART и др.) обеспечивает конфигурирование МАУ для решения различных задач и требований пользователей и обеспечивает многофункциональность современных МАУ.

При эксплуатации МАУ существует ряд важных особенностей, оказывающих существенное влияние на состояние защищенности информационного взаимодействия в рамках работы в ЗКС [49]. К ним относятся:

1. Миниатюрность МАУ. Данное свойство МАУ приводит к ограничению возможностей интерфейса взаимодействия с пользователем, влияет на вычислительные и функциональные возможности, повышает риск утраты МАУ и, соответственно, использование его неавторизованным пользователем.

2. Мобильность. Данное свойство МАУ позволяет использовать функциональные возможности МАУ независимо от местоположения пользователя, однако в сочетании с миниатюрностью позволяет незаметно осуществить пронос и использование МАУ внутри помещений с повышенными требованиями по защищенности.

3. Ограниченность вычислительных ресурсов МАУ. Данный фактор оказывает влияние на выполняемые в МАУ вычислительные процессы. Поскольку про-

цессы, отвечающие за функции защиты информации (ЗИ), как правило, должны выполняться в фоновом режиме и постоянно задействовать определенную часть вычислительных ресурсов, то в условиях ограниченности этих ресурсов в МАУ возникают и ограничения на функциональность и возможности таких процессов.

4. Мультифункциональность МАУ. К современным функциям МАУ можно отнести:

– использование МАУ в виде фото- и видеокамеры;

– использование МАУ как навигационного устройства;

– использование МАУ в качестве модема;

– использование МАУ в качестве переносной точки доступа;

– использование МАУ в качестве диктофона;

– использование МАУ в качестве съемного носителя информации.

5. Доступ к услугам корпоративной сети на основе использования принципа однократного входа SSO ("Single Sign-On"). Данная особенность является следствием миниатюрности МАУ и сложности человеко-машинного взаимодействия, характерного для МАУ. В сочетании с мобильностью и миниатюрностью МАУ использование режима SSO приводит к увеличению рисков использования МАУ неавторизованным пользователем.

6. Доступ к информационным ресурсам сетей с разными требованиями по защищенности. Использование МАУ для доступа к сетям с разными требованиями по защищенности в настоящее время ограничено, поскольку не существует эффективных СЗИ, обеспечивающих безопасность информации. Существующие подходы по ЗИ, используемые в стационарных СВТ, не применимы в полной мере к МАУ из-за ограниченности их вычислительных ресурсов, а также особенностей их программно-аппаратной архитектуры.

Указанные особенности увеличивают вероятность осуществления угроз ИБ при работе с МАУ в условиях ЗКС, поэтому необходимо учитывать факторы, влияющие на безопасность информации.

Существенное значение при разработке СЗИ для МАУ имеют вопросы их конфигурирования с учетом показателей ресурсопотребления [27], предусматри-

вающие выбор и разработку СЗИ путем комбинирования отдельных компонентов защиты с учетом их свойств, ограничений и требований к ним со стороны МАУ.

1.3.2. Актуальные факторы, воздействующие на безопасность информации при использовании мобильных абонентских устройств

На основе ГОСТ Р 51275-2006 [16] и с учетом того, что эксплуатация МАУ предполагается в сетях с разными требованиями по защищенности, а также учитывая указанные отличительные особенности МАУ по сравнению со стационарными СВТ, были выделены актуальные факторы, воздействующие на безопасность информации при использовании МАУ в ЗКС. Перечень указанных факторов представлен в таблице 1.1.

Анализ представленных факторов позволяет сделать следующие выводы:

1) значительная доля факторов, влияющих на ИБ при работе с МАУ, является субъективной, т.е. зависящей от пользователей;

2) большая часть выделенных объективных внутренних факторов, воздействующих на безопасность информации, является следствием наличия в составе МАУ функциональных блоков (модулей), создающих технические каналы утечки информации при их использовании внутри или вблизи специальных помещений ЗКС, а также при незащищенном доступе к конфиденциальной информации.

Проведенный анализ актуальных факторов, влияющих на безопасность информации при работе с МАУ, позволяет сформировать перечень угроз безопасности информации, а также модель нарушителя при эксплуатации МАУ в ЗКС.

Таблица 1.1 – Актуальные факторы, воздействующие на безопасность информации при эксплуатации МАУ

1. Объективные факторы	2. Субъективные факторы	
1.1. Внутренние факторы	2.1. Внутренние факторы	2.2. Внешние факторы
1.1.1. Передача сигналов в) в диапазоне радиоволн и в оптическом диапазоне длин волн (при передаче информационного сигнала с использованием модулей беспроводной связи Bluetooth, Wi-Fi, GSM, UMTS, LTE и т.п.;) 1.1.2. Излучения сигналов, функционально присущие техническим средствам (ТС) объекта информатизации: а) излучения акустических сигналов сопутствующие произносимой или воспроизводимой ТС речи (при функционировании динамика МАУ как в режиме телефона, так и в режиме громкой связи); б) электромагнитные излучения и поля (в радиодиапазоне при передаче информации с использованием модулей Bluetooth, Wi-Fi (802.11), GSM (2G), UMTS (3G), LTE (4G) и т.п.); 1.1.6 Наличие акустоэлектрических преобразователей в элементах ТС. 1.1.7. Дефекты, сбои и отказы, аварии ТС и систем. 1.1.8. Дефекты, сбои и отказы программного обеспечения (ПО)	2.1.1. Разглашение защищаемой информации имеющими к ней право доступа через б) передачу информации по открытым линиям связи; в) обработку информации на незащищенных ТС обработки информации; д) копирование информации на незарегистрированный носитель информации; ж) утрату носителя информации; 2.1.2. Неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации, путем: а) несанкционированное изменение информации; б) несанкционированное копирование защищаемой информации; 2.1.3. Несанкционированный доступ к информации путем: а) подключения к техническим средствам и системам объекта информатизации; б) использования закладочных средств (устройств); в) использования программного обеспечения технических средств объекта информатизации через 1) маскировку под зарегистрированного пользователя; 2) дефекты и уязвимости ПО объекта информатизации; 3) внесение программных закладок; 4) применение вирусов или другого вредоносного программного кода (троянские программы, клавиатурные шпионы, активное содержимое документов); г) хищения носителя защищаемой информации; д) нарушения функционирования ТС обработки информации; 2.1.5. Ошибки, обслуживающего персонала объекта информатизации при а) эксплуатации ТС; б) эксплуатации программных средств; в) эксплуатации средств и систем защиты информации;	2.2.2. Несанкционированный доступ к защищаемой информации путем: а) подключения к техническим средствам и системам объекта информатизации; б) использования закладочных средств (устройств); в) использования ПО технических средств объекта информатизации через: 1) маскировку под зарегистрированного пользователя; 2) дефекты и уязвимости ПО объекта информатизации; 3) внесение программных закладок; 4) применение вирусов или другого вредоносного программного кода (троянские программы, клавиатурные шпионы, активное содержимое документов); г) несанкционированного физического доступа к объекту информатизации; д) хищения носителя информации; 2.2.3. Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку; 2.2.5. Искажения, уничтожение или блокирование информации с применением технических средств путем: в) использования программных или программно-аппаратных средств при осуществлении: 1) компьютерной атаки; 2) сетевой атаки.

1.3.3. Модель угроз и нарушителя безопасности при использовании мобильных абонентских устройств в корпоративных сетях с разными требованиями по защищенности

Совокупность перечисленных актуальных факторов, воздействующих на безопасность информации при эксплуатации МАУ, позволяет сформировать модель угроз информации в ЗКС при доступе к ней пользователей МАУ. В ряде случаев информационный доступ может быть подвержен угрозам ИБ, возникающим вследствие использования сторонних приложений, а также устройств, взаимодействующих с МАУ в рамках информационного взаимодействия внутри ЗКС. В работах [44, 48, 75] приводится описание модели доступа к информационным сервисам, при которой возможна реализация атаки типа "отказ в обслуживании" в связи с наличием подобных сторонних приложений и информационного взаимодействия с ними, методика расчета оценки защищенности такой системы, а также методики обнаружения и противодействия данному виду атак.

При разработке модели угроз необходимо учитывать особенности МАУ, отличающие их от стационарных СВТ, а также принципы обеспечения ИБ в ЗКС с использованием МАУ [3]:

1. Принцип отсутствия доверия к импортной электронике на базе SoC, а также архитектуры наиболее распространенных процессоров с ARM-архитектурой с аппаратной виртуализацией основной ОС (например, Android) и закрытой доверенной ("Trusted OS"). Средствами защиты может выступать собственная доверенная ОС с доверенным начальным загрузчиком (аппаратно-программным модулем доверенной загрузки) для процессоров с ARM-архитектурой с контролем отсутствия скрытых аппаратных не декларируемых возможностей.

2. Принцип ненадежности МАУ. Требует наличия СЗИ, позволяющих гарантировать требуемый уровень защиты информации в ЗКС при условии отсутствия доверия к МАУ. Средствами защиты могут выступать:

– запрет или ограничение на использование личных МАУ;

– запуск корпоративных приложений в изолированных контейнерах;

– использование приложений, отслеживающих состояние МАУ;

– использование доверенной программно-аппаратной среды.

3. Принцип небезопасности беспроводных соединений, используемых МАУ. Требует наличия СЗИ, позволяющих гарантировать аутентичность сторон, участвующих в беспроводном сетевом взаимодействии, а также защищенность передаваемых данных. Средствами защиты могут выступать:

– применение шифрования при передаче данных;

– использование взаимной аутентификации на основе криптографических алгоритмов.

4. Принцип небезопасности сторонних приложений. Предполагается, что любые внешние приложения небезопасны и создают каналы утечки защищаемой информации с МАУ и из ЗКС. Требует наличия СЗИ, обеспечивающих доверенность используемых в МАУ приложений, а также отсутствие каналов утечки информации, возникающих в процессе запуска установленных в МАУ приложений. Средствами защиты могут выступать:

– изолированная программная среда (ИПС);

– безопасный изолированный контейнер для корпоративных приложений (например, средства программной или аппаратной виртуализации);

– терминальный доступ к приложениям, расположенным на удаленном защищенном корпоративном сервере;

– доверенные гипервизоры для запуска приложений в изолированной защищенной оболочке.

5. Принцип небезопасности устройств, взаимодействующих с МАУ. Современное МАУ является многофункциональным медиаустройством с различными коммуникационными функциями, способное взаимодействовать с большим количеством разнообразных устройств и носителей информации. Обеспечение требуемой защищенности подразумевает гарантированность того, что все подключае-

мые и взаимодействующие с МАУ устройства безопасны и являются доверенными. Средствами защиты могут быть:

– средства контроля подключаемых к МАУ устройств;

– средства контроля состояния и функциональных возможностей отдельных модулей МАУ;

– средства контроля передаваемых данных в процессе взаимодействия МАУ с другими устройствами.

С учетом данных принципов, а также на основе исследований [10, 81, 90] и проведенного анализа факторов, воздействующих на безопасности информации при эксплуатации МАУ, выделены актуальные угрозы ИБ. Угрозы ИБ при эксплуатации МАУ представлены в виде:

<угроза> := <источник угрозы>, <уязвимость>, <способ реализации угрозы>,<объект воздействия (программа, протокол, данные и т.д.>,<деструктивное воздействие>.

Описательная модель угроз и нарушителя ИБ при эксплуатации МАУ с учетом указанного представления изображена на рисунке 1.6.

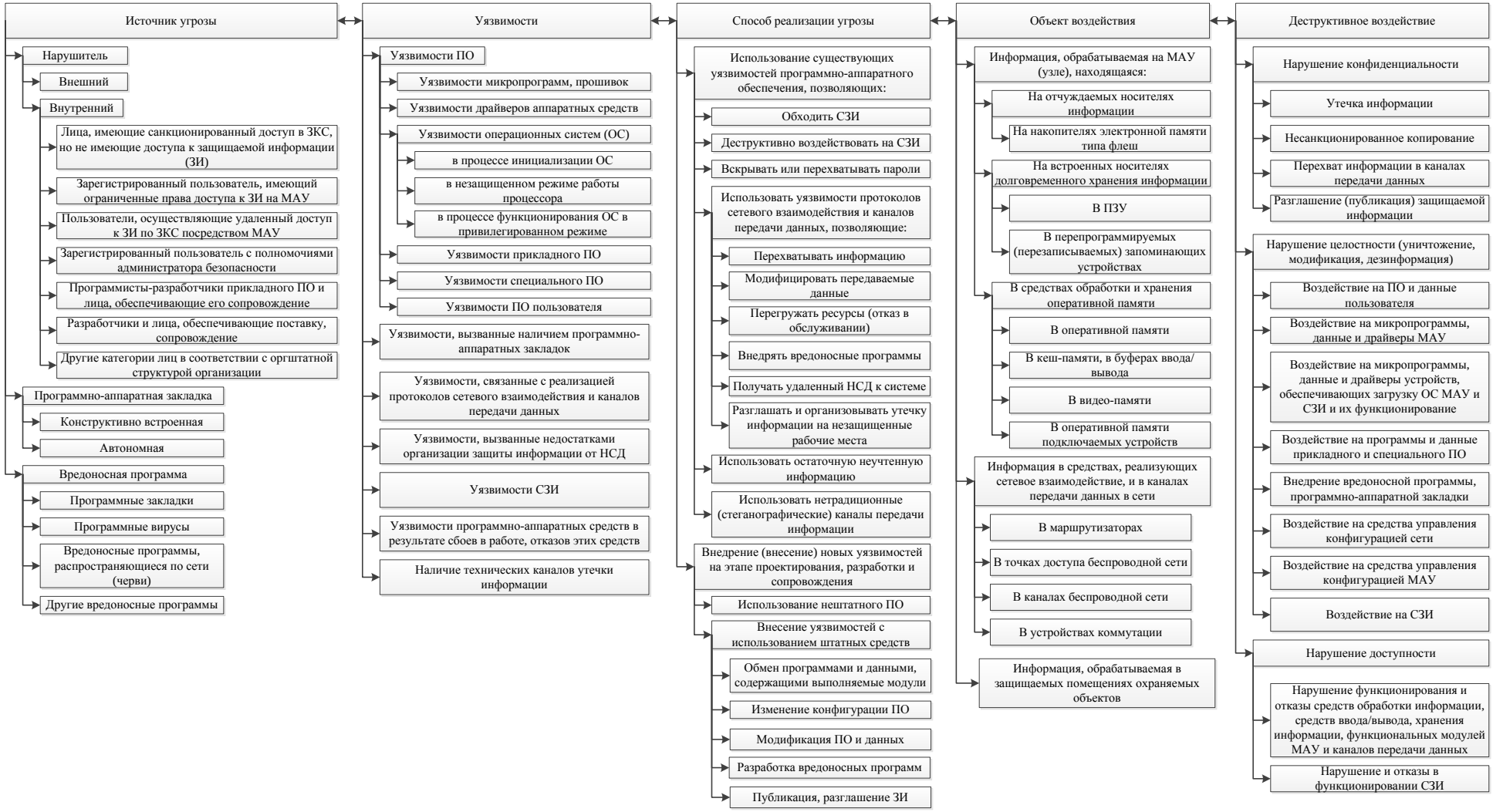


Рисунок 1.6 – Описательная модель угроз и модель нарушителя ИБ при эксплуатации МАУ в ЗКС

Основным источником угроз ИБ, рассматриваемым в данной работе, является *внутренний нарушитель*, поскольку для эффективной защиты от других источников пригодны имеющиеся СЗИ:

1) для защиты от внешнего нарушителя – комплекс организационно-технических мер по выполнению требований ИБ в ЗКС;

2) для защиты от программно-аппаратных закладок и вредоносных программ – комплекс мер по лицензированию и сертификации МАУ, а также применение изолированной программной среды в составе системного ПО МАУ, доверенной ОС и АПМДЗ.

Основными уязвимостями являются:

– уязвимости, связанные с недостатками организации ЗИ от НСД;

– наличие технических каналов утечки информации (ТКУИ) [91, 92] в МАУ в условиях эксплуатации МАУ в запрещенных режимах работы.

В связи с необходимостью использования единого МАУ для доступа к корпоративным сетям с разными требованиями по защищенности принципиальной задачей является создания условий для такого управления программно-аппаратной конфигурацией МАУ, при котором будет исключено наличие ТКУИ при доступе с использованием единого МАУ к ресурсам корпоративных сетей с разными требованиями по защищенности. Типовая схема ТКУИ в МАУ представлена на рисунке 1.7.

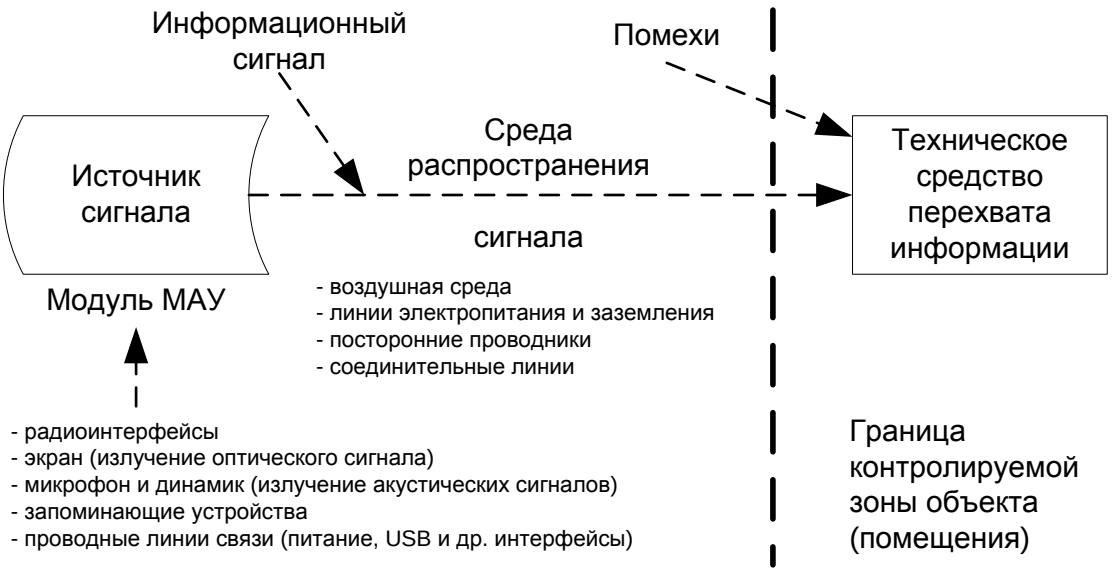


Рисунок 1.7 – Схема технического канала утечки информации, обрабатываемого средствами вычислительной техники

Одним из эффективных средств предотвращения утечки информации по ТКУИ может быть система управления программно-аппаратной конфигурацией МАУ, позволяющая отключать модули МАУ (например, микрофон, радиоинтерфейс, запоминающие устройства), создающие информационные источники сигнала, в зависимости от условий (атрибутов доступа), в которых находится МАУ и к которым можно отнести, в том числе, местоположение. При отсутствии такой системы внутренний нарушитель имеет техническую возможность использовать МАУ как средство связи независимо от условий доступа и своего местоположения в организации. Например, в случае несанкционированного или случайного проноса МАУ в специальное помещение, в котором запрещена обработка открытой информации и использование МАУ, данное устройство становится источником информационных сигналов, содержащих конфиденциальную информацию. Схема утечки информации представлена на рисунке 1.8.

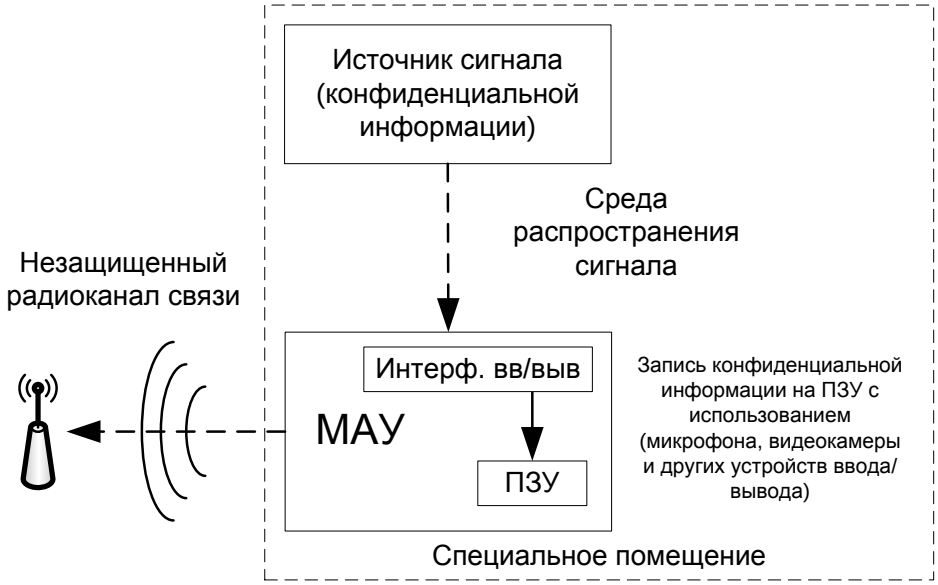


Рисунок 1.8 – Схема утечки информации при несанкционированном использовании МАУ в специальном помещении

В настоящее время существует ряд СЗИ в виде MDM-решений, позволяющих блокировать работу МАУ в запрещенных режимах. Данные решения не предполагают аппаратной переконфигурации устройства и работают на уровне приложений, что является существенным недостаткам с учетом принципов отсутствия доверия к импортной электроники, ненадежности МАУ и отсутствия доверия к сторонним приложениям.

Контроль вноса незащищенных МАУ осуществляется, как правило, организационно-техническими мерами, которые сравнительно легко преодолеваются при отсутствии эффективного контроля выполнения данных мер.

Таким образом, существует объективная потребность в разработке таких СЗИ, которые позволят в автоматическом режиме управлять не только программной, но и аппаратной конфигурацией МАУ, блокируя возможные каналы утечки информации при использовании устройства в организациях, в которых предусмотрена обработка конфиденциальной информации, независимо от местоположения МАУ на территории данной организации.

Разрабатываемая система управления безопасностью МАУ направлена в первую очередь на защиту от угроз, связанных с:

– обходом СЗИ;

– деструктивными воздействиями на СЗИ;

– перехватом и модификации передаваемой информации;

– разглашением и организации утечки информации в незащищенных местах доступа;

– использованием нештатного ПО;

– внесением уязвимостей с использованием штатных средств.

Основными объектами защиты информации при реализации разрабатываемой СЗИ является:

– информация, обрабатываемая МАУ;

– информация в средствах, реализующих сетевое взаимодействие, а также в каналах передачи данных в сети;

– информация, обрабатываемая в специальных помещениях ЗКС.

Указанные описательные модели угроз и нарушителя ИБ при использовании МАУ позволяют более детально сформировать требования к разрабатываемой системе управления безопасностью МАУ и реализуемых СЗИ для обеспечения безопасности информации в корпоративных сетях с разными требованиями по защищенности.

1.3.4. Технические решения для защиты информации при эксплуатации мобильных абонентских устройств

В настоящее время для защиты информации при эксплуатации МАУ в ЗКС разработано достаточно большое количество программных, программно-аппаратных решений, выполняющих функции СЗИ. Среди ПО для защиты информации в МАУ и управления доступом к услугам ЗКС известны такие продукты, как программные комплексы "ViPNet Client" [146], CISCO для управления до-

ступом Cisco Unified Access, Cisco Identity Services Engine [58], Cisco Secure ACS [30], "MobileIron", "Kaspersky Security 10" для мобильных устройств, "McAfee Enterprise Mobility Management", "Afaria", "SOTI Mobicontrol", "AirWatch MDM", "Samsung Enterprise Access Layer", "Juniper Junos Pulse MSS".

Данные решения представляют собой реализации технологии MDM (Mobile Device Management – управление МАУ), MAM (Mobile Application Management – управление корпоративными приложениями на МАУ) и MIM (Mobile Information Management – управление корпоративными документами с использованием МАУ), представляющие собой элементы комплексного ПО для работы с корпоративными системами при помощи МАУ, обеспечивающее безопасность, контроль и поддержку МАУ, используемых персоналом компаний. Как видно из названия технологии, управление МАУ осуществляется на уровне приложений и доступов к документам.

Существенным недостатком данных решений является использование только лишь программного управления МАУ, что не позволяет в полной мере гарантировать безопасность информации при доступе к защищенным услугам, а также отсутствие математически доказанного корректного формального аппарата моделирования безопасности МАУ в ЗКС.

К аппаратным и программно-аппаратным защищенным техническим решениям в настоящее время относятся [47]:

– защищенные мобильные телефоны;

– технические средства защищенного терминального доступа;

– защищенные планшетные компьютеры;

– защищенные мобильные компьютеры.

В настоящее время известны следующие решения в области защищенных мобильных телефонов:

1. Защищённый телефон стандарта GSM "Талисман 395" [88].

2. Специализированный терминал мобильной связи "Сапфир-К" [83].

3. Специальный сотовый телефон "SMP-АТЛАС/2" [85].

4. Аппаратура шифрования речевых сообщений "Аппаратура 605" [2].

5. Специальный микросотовый телефон "М-549М" [84].

К известным техническим средствам защищенного терминального доступа можно отнести:

1. Терминальный клиент "ViPNet Terminal" [147].

2. Терминальный клиент "КАМИ-Терминал" [32].

3. Терминальный клиент "HELIOS ProfyShield LT-A330–1s" [113].

Известен защищенный планшетный компьютер "Континент Т-10" [35], сертифицированный ФСТЭК и ФСБ, а также ряд таких защищенных мобильных компьютеров как:

1. Мобильное защищенное автоматизированное рабочее место доступа в сеть Интернет "МАРМ ДСИ" [54].

2. Мобильный вычислительный комплекс "ИНФОПРО" МВК-2 [55].

Большинство представленных технических решений позволяют обеспечивать защищенный доступ к конфиденциальной информации. Некоторые обеспечивают защищенный доступ к сведениям, содержащим информацию, отнесенную к государственной тайне. Однако на данный момент отсутствуют технические решения, позволяющие обеспечивать доступ к сетям с разными требованиями по защищенности с использованием одного МАУ. Другим недостатком является то, что не существуют эффективных СЗИ, учитывающих местоположение МАУ. Данные недостатки СЗИ в настоящее время устраняются путем применения организационных мер в отношении МАУ и их пользователей, включающих в себя, в том числе, запрет на пронос личных МАУ и их использования в ЗКС.

Существует ряд технических решений от иностранных производителей, таких как у компании CISCO [30, 58], позволяющих обеспечивать управление доступом пользователей МАУ в зависимости от их местоположения в ЗКС. Однако в данных решениях местоположение определяется лишь точкой подключения к БСПД ЗКС, при этом уровень конфиденциальности доступа определяется уровнем конфиденциальности точки доступа, а не реальным местоположением пользователя МАУ.

Одним из наиболее существенных недостатков современных защищенных МАУ является ограниченный перечень предоставляемых услуг. Отсутствие возможности совмещать функциональность современных смартфонов и защищенных технических мобильных решений, которые допустимо использовать в ЗКС при условии выполнения требований ИБ, сказывается на доступности и своевременности предоставления абонентам услуг. Это связано с отсутствием эффективных СЗИ, позволяющих гарантировано исключить работу МАУ в небезопасных режимах (конфигурациях), а также обеспечить отсутствие технических каналов утечки информации в период нахождения пользователя МАУ в зоне доступа ЗКС.

Таким образом, на основе проведенного анализа существующих защищенных технических мобильных решений выделены следующие недостатки:

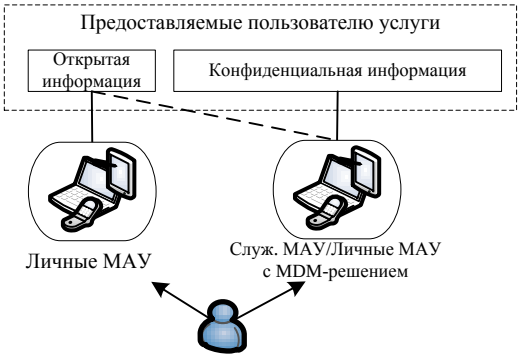
– отсутствие СЗИ, позволяющих обеспечить безопасный доступ к сетям с разными требованиями по защищенности с использованием одного устройства;

– отсутствие технических решений, позволяющих определять местоположение МАУ и учитывать требования ИБ к МАУ, предъявляемые к СВТ в данном местоположении в ЗКС;

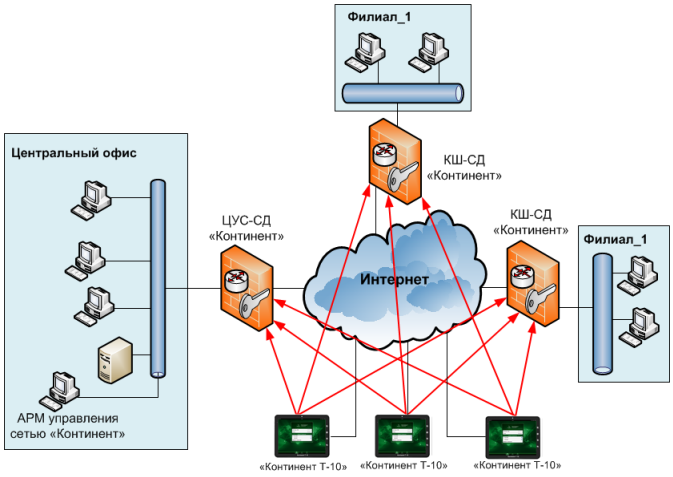
– ограниченное количество предоставляемых пользователям МАУ услуг в защищенных мобильных решениях.

1.4. Способы построения комплексной системы защиты информации при доступе к сетям с разными требованиями по защищенности

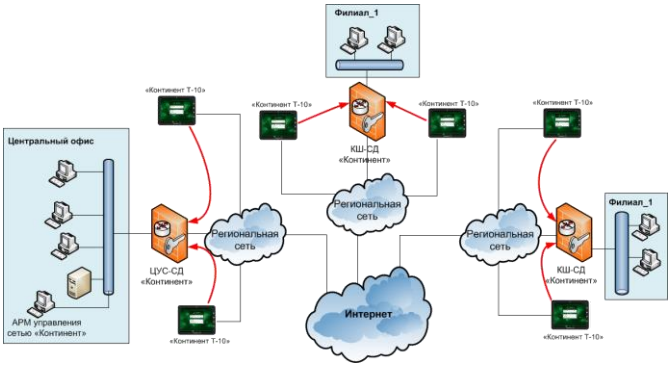
Для защиты информации, обрабатываемой в ЗКС, применяются СЗИ, параметры которых определяются политикой безопасности данной ЗКС на основании уровня конфиденциальности обрабатываемой информации и соответствующими нормативно-правовыми актами [56, 59]. При обеспечении доступа МАУ к конфиденциальной информации и сетям с разными требованиями по защищенности в настоящее время применяется схема, представленная на рисунке 1.9 [35].



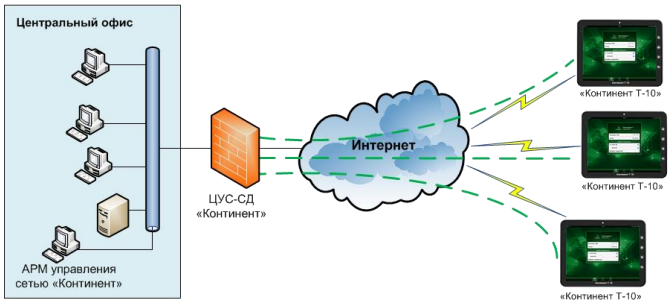
а)



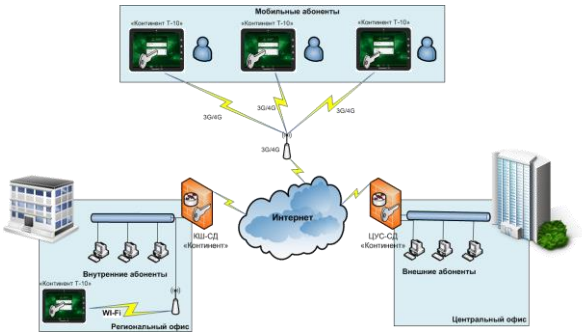
б)



в)



г)



д)

Рисунок 1.9 – Схема доступа в ЗКС к информации с разным уровнем защищенности при использовании МАУ: а) обобщенная; б-д) варианты подключения на примере защищенного планшета "Континент Т-10"

Порядок и режим доступа к конфиденциальной информации с использованием указанной схемы определяется, в том числе, и комплексом организационных и организационно-технических мер по ЗИ в ЗКС.

Как видно из рисунка 1.9 в настоящее время могут применяться несколько МАУ для работы в сетях с разными требованиями по защищенности. Однако в ряде случаев необходимо сопряжение данных сетей (контуров обработки информации с разными требованиями по защищенности). При этом выполнение требований по ИБ должно соответствовать уровню защиты, предъявляемому к контуру с более высокими требованиями по защищенности.

В настоящее время известны несколько подходов для сопряжения контуров обработки информации с разными требованиями по защищенности. К ним относятся:

1. Технологии однонаправленных шлюзов. Гарантируют передачу информации в одном направлении. В настоящее время известны такие технические решения как однонаправленный шлюз "Атликс-Шлюз-К" [57], система однонаправленной передачи данных "ДИОД" [82] и другие.

2. Технологии виртуализации. Использование доверенных гипервизоров, позволяющих в одном корпусе объединить несколько защищенных программно-аппаратных контейнеров, в которых допустимо обрабатывать информацию с разными требованиями по защищенности.

3. Технологическое объединение в едином корпусе программно-аппаратных платформ, выполненное с использованием оптоэлектронной, трансформаторной развязки, позволяющее разделить и изолировать тракты прохождения информации с разным требованиями по защищенности друг от друга.

4. Терминальный доступ. Реализация технологий тонкого клиента с использованием серверов приложений.

С точки зрения реализации сопряжения контуров обработки информации с разными требованиями по защищенности при эксплуатации МАУ технологии однонаправленных шлюзов применимы лишь как вспомогательные средства. Технологии виртуализации требуют серьезных вычислительных ресурсов, которыми обладают только планшетные и мобильные компьютеры и достаточно ограниченно – смартфоны.

Технологическое объединение в едином корпусе программно-аппаратных платформ, позволяющее разделить и изолировать тракты прохождения информации, к которым предъявляются разные требования по защищенности, друг от друга, в настоящее время реализовано только лишь для стационарных вычислительных систем. В то же время данное направление является перспективным для МАУ, поскольку технический уровень в настоящее время позволяет объединять в едином корпусе многопроцессорные системы, в том числе и в МАУ.

Терминальный доступ является наиболее оптимальным средством при доступе к информации с разными требованиями по защищенности. Однако реализация данных технологий не позволяет осуществлять управление функциональностью МАУ, исключая его работу и работу отдельных функциональных модулей МАУ в запрещенных режимах, а также не решает задачи определения местоположения МАУ.

Таким образом, для устранения проблемы реализации сопряжения контуров обработки информации с разными требованиями по защищенности в МАУ необходимо решение следующих задач:

1) разработка формальной модели безопасности МАУ, учитывающей программно-аппаратную конфигурацию МАУ и его местоположение;

2) разработка системы определения местоположения МАУ, позволяющей с требуемой достоверностью определять местонахождения МАУ в специальных помещениях ЗКС в режиме реального времени;

3) разработка системы управления безопасностью (программно-аппаратной конфигурации) МАУ в зависимости от его местоположения и других атрибутов доступа, а также требований по качеству предоставляемых услуг;

4) разработка технических предложений по реализации системы управления безопасностью МАУ, позволяющей функционировать данному устройству в сетях с разными требованиями по защищенности, с учетом местоположения МАУ и иных атрибутов доступа.

Решение данных задач возможно с помощью применения агентно-ориентированного подхода [34, 98, 114], являющегося элементом искусственного

интеллекта и построенного на основе классической клиент-серверной архитектуры. Обобщенная схема доступа в этом случае может иметь вид, представленный на рисунке 1.10.

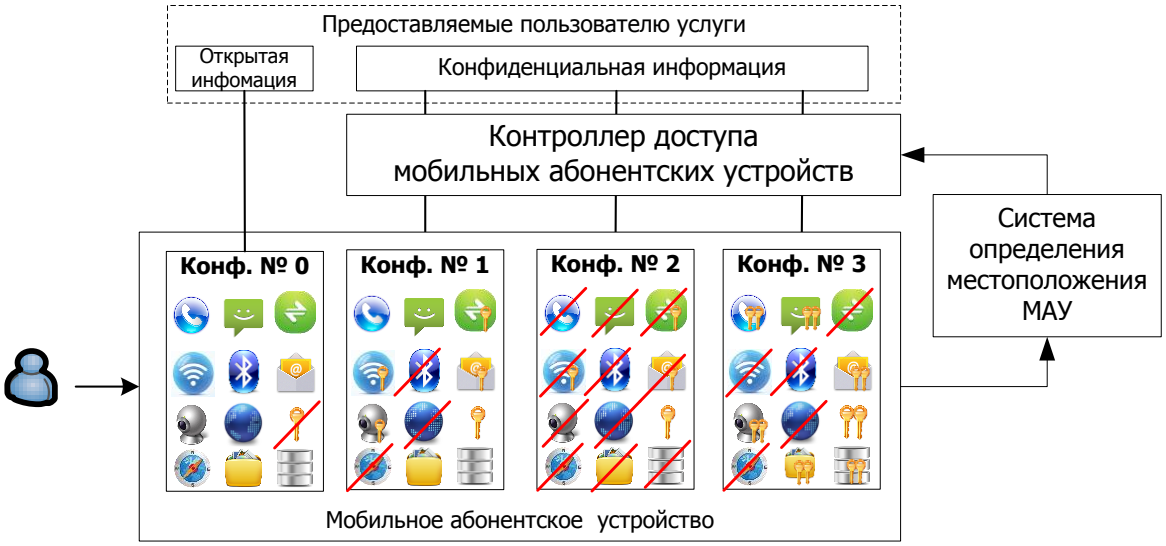


Рисунок 1.10 – Схема доступа к информации с использованием различных конфигураций МАУ

Для решения задачи определения местоположения МАУ в качестве агентов могут выступать точки доступа БСПД, собирающие сведения об уровне сигнала МАУ, на основе которого будет осуществляться расчет местоположения МАУ в пределах области покрытия БСПД. Данный расчет может осуществляться, как в контроллере беспроводной сети, так и централизованно в точке принятия решения по управлению конфигурацией МАУ. Прототип такой многоагентной системы представлен на рисунке 1.11.

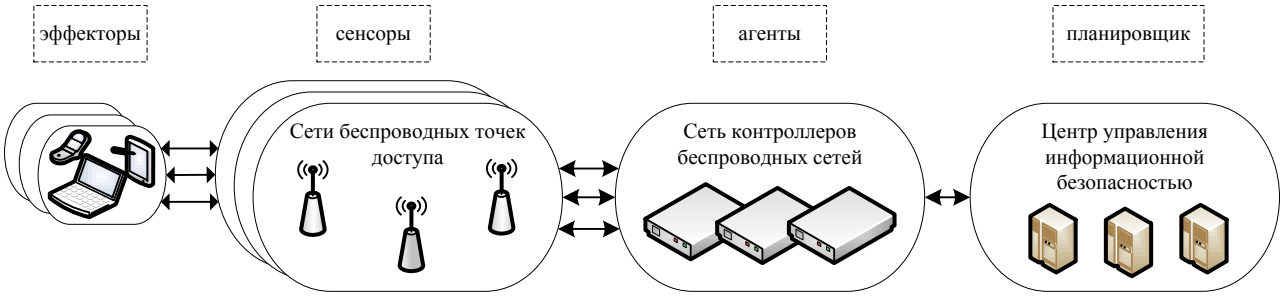


Рисунок 1.11 – Многоагентная система определения местоположения МАУ

Задача по управлению конфигурацией МАУ в зависимости от предъявляемых требований ИБ может решаться за счет внедрения в МАУ программно-аппаратного агента, например, на базе доверенного аппаратно-программного модуля доверенной загрузки (АПМДЗ), обменивающегося информацией по защищенному каналу управления через доверенную беспроводную сеть доступа с центром управления информационной безопасности (ЦУИБ) ЗКС. Схема такой системы управления конфигурацией МАУ представлена на рисунке 1.12.

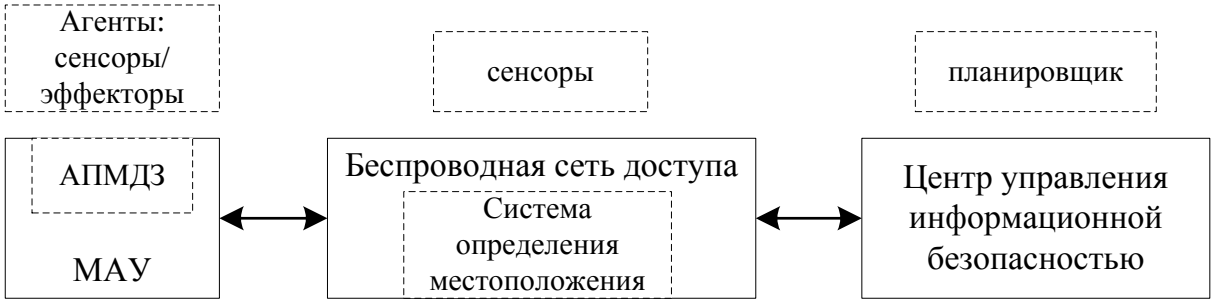


Рисунок 1.12 – Схема подсистемы управления конфигурацией МАУ

Реализация представленных систем совместно с использованием технологий терминального доступа, виртуализации или оптоэлектронной развязки объединенных программно-аппаратных платформ в едином корпусе позволит обеспечить защищенный удаленный доступ к сетям с разными требованиями по защищенности с использованием одного МАУ.

1.5. Постановка задачи диссертационного исследования

Для повышения вероятности обеспечения безопасности информации при доступе к инфокоммуникационным услугам и информации в корпоративных сетях с разными требованиями по защищенности, необходимо разработать систему управления безопасностью МАУ, позволяющую управлять программно-аппаратной конфигурацией МАУ и доступом мобильных пользователей к инфокоммуникационным услугами и ресурсам в зависимости от атрибутов доступа, включая местоположение устройства, а также требований по безопасности информации и качеству предоставляемых услуг.

Формальная постановка задачи диссертационного исследования: на основе теории машинного обучения, математический статистики и численных методов разработать модель безопасности МАУ и алгоритм управления безопасностью МАУ, учитывающий атрибуты доступа, включая местоположение устройства, требования по безопасности информации и качеству предоставляемых услуг.

Исходные данные:

1) универсальное мобильное абонентское устройство (МАУ) MD, его технические характеристики;

2) множество возможных конфигураций МАУ – $CONF$;

3) расположение и параметры помещений:

$$Rooms = \left\{ room_i = \left((x_{i1}, y_{i1}), (x_{i2}, y_{i2}), ..., (x_{in}, y_{in}), L_{Room_i} \right) \right\},\ i = \overline{1, N}_{Rooms}, \qquad (1.1)$$

где L_{Room_i} – уровень требований по защищенности помещения, $(x_{i1}, y_{i1}), (x_{i2}, y_{i2}), ..., (x_{in}, y_{in})$ – координаты n углов помещений, N_{Rooms} – количество помещений;

4) расположение точек доступа беспроводной сети $AP = \left\{ AP_j = \left(x_j, y_j \right) \right\}$, $j = \overline{1, N}_{AP}$, где (x_j, y_j) – координаты точек доступа, N_{AP} – количество точек доступа;

5) множество пороговых значений частных показателей эффективности $H = \left\{ P_{\beta}\left(\tilde{L}_{Room} > L_{Room} \right) \le P_{\beta}^{\text{треб}}, T_{RECONF} \le T_{\text{RECONF}}^{\text{доп}} \right\}$;

6) совокупность атрибутов доступа $A = \{a_i\}$, включающая:

– идентификационные данные о пользователе, МАУ, операционной системе (ОС) и приложениях МАУ;

– сетевая адресная информация;

– уровень конфиденциальности и идентификатор запрашиваемой услуги (ресурса).

Требуется:

1) разработать модель безопасности МАУ Z, учитывающую вероятность нахождения МАУ в специальных помещениях, обосновать ее корректность и оценить качество;

2) разработать алгоритм управления безопасностью МАУ путем реализации решающего правила F отнесения совокупности атрибутов доступа, включающих в себя, в том числе, вероятность нахождения МАУ в специальном помещении к разрешенной конфигурации (состоянию) МАУ, обеспечивающей безопасность информации при доступе к услугам корпоративных сетей с разными требованиями по защищенности и заданное качество предоставление услуг, оценить свойства алгоритма:

$$\begin{cases} Z \xrightarrow{F(MD, Rooms, AP, A)} \{CONF_i\}_{t+1}; \\ P_{\text{БИ}}(T) > P_{\text{БИ}}^{\text{треб}}(T) \end{cases} \quad (1.2)$$

3) разработать научно-технические предложения по практической реализации системы управления безопасностью МАУ, позволяющей повысить безопасность информации при эксплуатации МАУ в корпоративных сетях с разными требованиями по защищенности при следующих **ограничениях и допущениях**:

– в состав корпоративной сети входит доверенная беспроводная сеть передачи данных (БСПД);

– канал управления между доверенными точками доступа и МАУ защищен криптографическими средствами защиты информации;

– МАУ имеет возможность функционировать в различных программно-аппаратных конфигурациях;

– в составе МАУ функционирует аппаратно-программный модуль доверенной загрузки (АПМДЗ), являющийся программно-аппаратным агентом, управляющим конфигурацией (состоянием) МАУ;

– на МАУ функционирует доверенная операционная система (ДОС);

– в ДОС МАУ функционирует изолированная программная среда (ИПС);

– пользователь МАУ в корпоративной сети аутентифицирован;

4) оценить эффективность разработанной системы управления безопасностью МАУ.

Для получения оценки эффективности предложенной системы управления безопасностью МАУ, а также оценки степени достижения цели диссертационного исследования целесообразно воспользоваться критерием превосходства [64], исходя из специфики предъявляемых к системе требований.

Система показателей качества [45] построена из следующих соображений. Поскольку цель разрабатываемой системы – обеспечение безопасности информации (защиты информации) при эксплуатации МАУ в корпоративных сетях с разными требованиями по защищенности, то степень достижения данной цели согласно теории эффективности целенаправленных процессов [64] может быть представлена в виде выражения

$$\mathrm{P}_{\text{ЗИМАУ}} = P\left(REZ \geq REZ^{\text{тр}}\right) \cdot P\left(RES \leq RES^{\text{доп}}\right) \cdot P\left(OPR \leq OPR^{\text{доп}}\right), \qquad (1.3)$$

где REZ – результативность процесса защиты информации; $REZ^{\text{треб}}$ – требуемое значение результативности процесса защиты информации; RES – ресурсоемкость процесса защиты информации; $RES^{\text{доп}}$ – максимально допустимый расход ресурсов для процесса защиты информации; OPR – затраты операционного времени для достижения цели функционирования системы; $OPR^{\text{доп}}$ – максимально допустимое время для достижения цели функционирования системы.

В соответствие с [7, 15, 17, 26] безопасность информации является комплексным свойством и обеспечивается за счет выполнения требований по обеспе-

чению конфиденциальности, целостности и доступности информации. Исходя из этого, результативность процесса защиты информации при эксплуатации МАУ может быть представлена в виде выражения

$$P_{\text{БИ}}(T) = P_{\text{КИ}}(T) \cdot P_{\text{ЦИ}}(T) \cdot P_{\text{ДИ}}(T), \qquad (1.4)$$

где $P_{\text{КИ}}(T)$ – вероятность обеспечения конфиденциальности информации в течение времени T; $P_{\text{ЦИ}}(T)$ – вероятность обеспечения целостности информации; $P_{\text{ДИ}}(T)$ – вероятность обеспечения доступности информации.

Вопросы обеспечения целостности информации в работе не рассматриваются, поэтому показатель при расчетах принят равным единице: $P_{\text{ЦИ}}(T) = 1$.

Вероятность обеспечения доступности информации предлагается оценивать по своевременности обработки запросов на доступ к услугам [18] с учетом количества доступным услуг $N_{\text{ДУ}}$ относительно их общего числа $N_{\text{У}}$. Тогда вероятность предоставления информации или услуг $P_{\text{ДИ}}(T_{\text{ДИ}})$ за заданное время $T_{\text{ДИ}}^{\text{зад}}$ будет определяться с помощью табулированной неполной гамма-функции [18]:

$$P_{\text{ДИ}}(T_{\text{ДИ}}) = \frac{N_{\text{ДУ}}}{N_{\text{У}}} \cdot P_{\text{ДИ}}^{У}(T_{\text{ДИ}}) = \frac{N_{\text{ДУ}}}{N_{\text{У}}} \cdot \int_0^{\theta} exp(-\tau) \cdot \tau^{\gamma}\, d\tau / \Gamma(\gamma), \qquad (1.5)$$

где

$$\Gamma(\gamma) = \int_0^{\theta} exp(-\tau) \cdot \tau^{\gamma}\, d\tau / \Gamma(\gamma) \text{ - гамма функция, } \gamma = \frac{T_{\text{полн}}}{\sqrt{T_2 - T_{\text{полн}}^2}}, \theta = T_{\text{ДИ}}^{\text{зад}} \cdot \frac{\gamma}{T_{\text{полн}}}^2, \qquad (1.6)$$

где $T_{\text{полн}}$ и T_2 – рассчитываемые соответственно среднее время и 2-й момент времени реакции системы при обработке запросов системе (полного времени пребывания на обработке с учетом ожидания в очереди), $T_{\text{ДИ}}^{\text{зад}}$ – заданное время (предельно допустимое) для обработки запроса на доступ к информации (услугам).

Целью диссертационного исследования является повышение вероятности обеспечения безопасности информации при эксплуатации МАУ для доступа к инфокоммуникационным услугам и ресурсам корпоративных сетей с разными

требованиями по защищенности, соответственно, необходимо доказать, что показатель вероятности обеспечения конфиденциальности информации будет не хуже, чем в действующих прототипах. Для обеспечения конфиденциальности информации необходимо обеспечить защиту от несанкционированного доступа (НСД), а также обеспечить сохранение конфиденциальности на заданном периоде времени [7, 18]. Исходя из этих соображений, показатель вероятности обеспечения конфиденциальности может быть представлен в виде выражения

$$P_{\text{КИ}}(T) = \left(1 - P_{\text{НСД}}\right) \cdot P_{\text{СК}}\left(T\right), \tag{1.7}$$

где $P_{\text{НСД}}$ – вероятность НСД к информации; $P_{\text{СК}}\left(T\right)$ – вероятность сохранения конфиденциальности информации на заданном периоде времени.

Вероятность НСД при условии корректно заданной политики безопасности, будет определяться величиной вероятности ошибки 2-го рода при определении местоположения МАУ, которая будет оказывать непосредственное влияние на выбор конфигурации МАУ в системе управления безопасностью МАУ. Тогда показатель вероятности НСД можно представить в виде выражения

$$P_{\text{НСД}} = 1 - P\left(CONF \subset CONF^{\text{доп}}\right) = 1 - P\left[\beta\left(\tilde{L}_{Room} > L_{Room}\right) \le \beta^{\text{доп}}\right], \tag{1.8}$$

$$P\left(CONF \subset CONF^{\text{доп}}\right) = P\left[P_{\beta}\left(\tilde{L}_{Room} > L_{Room}\right) \le P_{\beta}^{\text{доп}}\right], \tag{1.9}$$

где $CONF$ – конфигурация МАУ, сформированная системой управления безопасностью МАУ; $CONF^{\text{доп}}$ – множество допустимых конфигураций МАУ при текущих условиях доступа.

Показатель вероятности сохранения конфиденциальности информации на заданном периоде времени определяется своевременностью переконфигурации МАУ при изменении атрибутов доступа и при условии назначения конфигурации из допустимого множества $P\left[\left(T_{RECONF} \le T_{RECONF}^{\text{доп}}\right) / \left(CONF \subset CONF^{\text{доп}}\right)\right]$, а также вероятностью преодоления СЗИ за данный период времени $P_{\text{Пр3}}$ [7, 18]. Данный показатель может быть представлен в виде выражения:

$$P_{\text{СК}}\left(T_{RECONF}\right) = P\left[\left(T_{RECONF} \le T_{RECONF}^{\text{доп}}\right) / \left(CONF \subset CONF^{\text{доп}}\right)\right] \cdot \left(1 - P_{\text{Пр3}}\right). \tag{1.10}$$

В соответствие с [18, с. 41-42] показатель $P_{\text{ПрЗ}}$ может быть рассчитан как

$$P_{\text{ПрЗ}} = 1 - \prod_{m=1}^{k} P_{\text{НСД}_m}, \tag{1.11}$$

где k – количество преград, которое необходимо преодолеть нарушителю, чтобы получить доступ к информационным и программным ресурсам, $P_{\text{НСД}_m}$ – вероятность преодоления нарушителем m-той преграды (средства защиты).

Для экспоненциальной аппроксимации распределений исходных характеристик при их независимости:

$$P_{НСД\,m} = \frac{f_m}{f_m + u_m}, \tag{1.12}$$

где f_m – среднее время между соседними изменениями параметров m-й преграды системы защиты (время между сменой конфигураций); u_m – среднее время расшифровки (вскрытия) значений параметров m-й преграды системы защиты. Показатель $P_{\text{ПрЗ}}$ в рамках работы вынесен в ограничения и принят равным нулю.

Ресурсоемкость процесса защиты информации [7] при эксплуатации МАУ может быть определена, исходя из выражения:

$$\begin{aligned} RES_{\text{ЗИМАУ}} &= K_{\text{ИВР}} \cdot C_{\text{ВР}} + K_{\text{ИТР}} \cdot C_{\text{ТР}} + K_{\text{ИСУ}} \cdot C_{\text{СУМАУ}} + \\ &+ K_{\text{ИСОМ}} \cdot C_{\text{СОМ}} + \left(\sum_{i=1}^{N_{\text{МАУ}}} C_{\text{МАУ}_i} \right) \cdot N_{\text{Польз}}, \end{aligned} \tag{1.13}$$

где $K_{\text{ИВР}}$ – коэффициент использования вычислительных ресурсов; $C_{\text{ВР}}$ – стоимость вычислительных ресурсов; $K_{\text{ИТР}}$ – коэффициент использования телекоммуникационных ресурсов; $C_{\text{ТР}}$ – стоимость телекоммуникационных ресурсов; $K_{\text{ИСУ}}$ – коэффициент использования системы управления безопасностью МАУ; $C_{\text{СУМАУ}}$ – стоимость системы управления безопасностью МАУ; $K_{\text{ИСОМ}}$ – коэффициент использования системы определения местоположения МАУ; $C_{\text{СОМ}}$ – стоимость системы определения местоположения МАУ; $C_{\text{МАУ}_i}$ – стоимость i-го МАУ,

необходимого для доступа к услугам; $N_{\text{МАУ}}$ – количеством МАУ, необходимых для доступа ко всему перечню услуг; $N_{\text{Польз}}$ – количество пользователей МАУ.

Решение научной задачи предполагается проводить в рамках структуры исследования, представленной на рисунке 1.13.

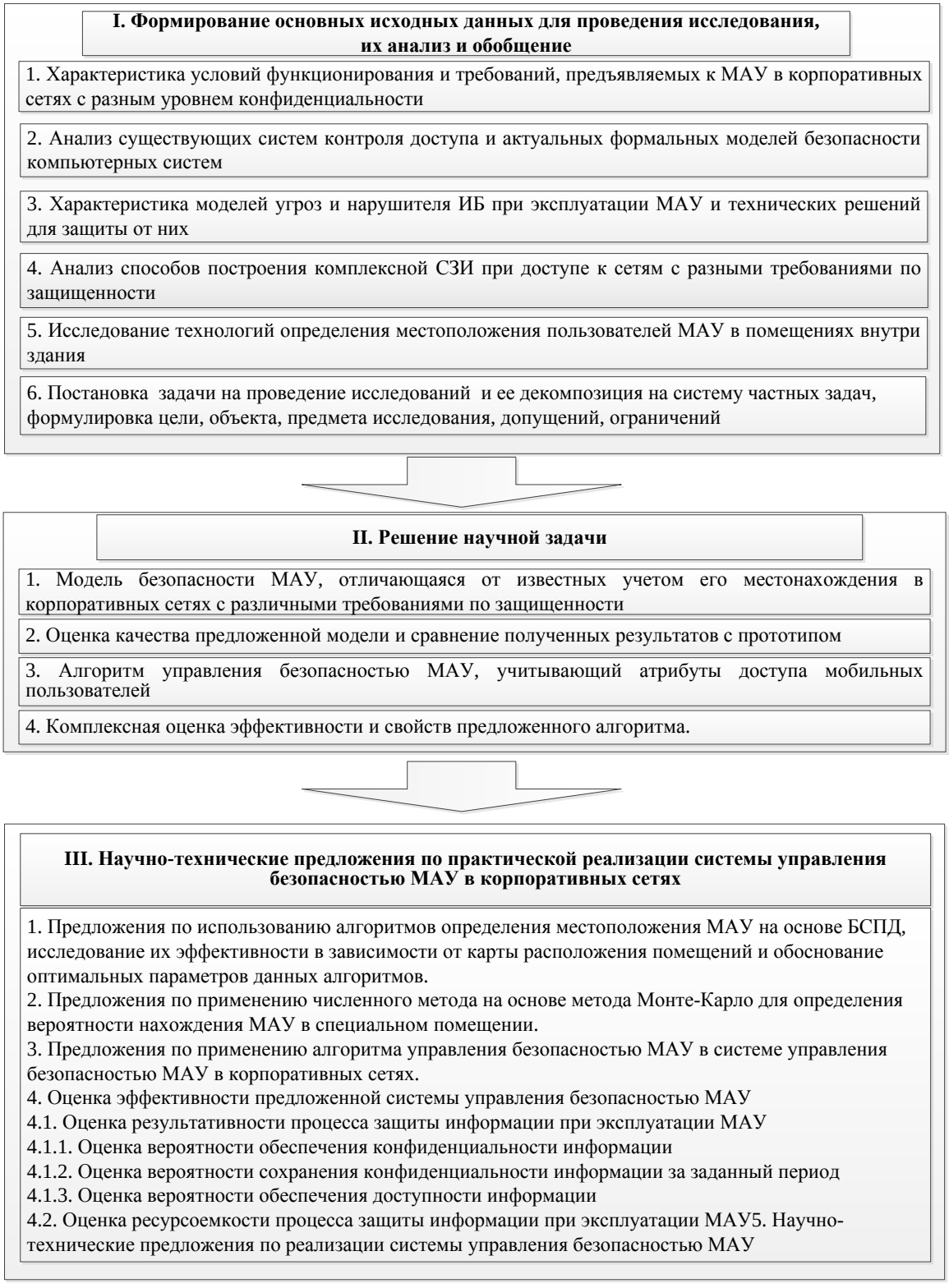


Рисунок 1.13 – Структурно-логическая схема исследования

Выводы по первому разделу

1. Использование вычислительных ресурсов современных МАУ в корпоративных сетях и обеспечение доступа к широкому перечню услуг корпоративных сетей, в том числе, защищенных является актуальной задачей. В настоящее время она не решена, поскольку отсутствуют эффективные СЗИ, нейтрализующие угрозы ИБ, связанные с использованием МАУ, в том числе при доступе к сетям с разными требованиями по защищенности.

2. Существует ряд недостатков современных формальных моделей безопасности компьютерных систем применительно к обеспечению безопасности информации при использовании МАУ, включая существующие технические и программно-аппаратные решения:

1) отсутствуют технические решения по определению местоположения МАУ, обладающие достаточной точностью;

2) отсутствует техническая возможность интеллектуального программно-аппаратного блокирования МАУ или их отдельных функциональных блоков, представляющих при определенных условиях угрозу ИБ в ЗКС;

3) доступ к сетям с разными требованиями по защищенности с использованием МАУ осуществляется либо с использованием разных МАУ соответствующих необходимому уровню защищенности либо с ручным переключением режимов работы; отсутствует автоматическое управление программно-аппаратной конфигурацией МАУ в зависимости от уровня конфиденциальности предоставляемых услуг, местоположения МАУ и других атрибутов доступа.

Наличие указанных недостатков свидетельствует о необходимости учета такого фактора как местоположение МАУ, а также доработки формальных моделей безопасности и обоснования их корректности. Необходима разработка новых технических предложений по реализации программно-аппаратной платформы универсального единого МАУ, позволяющего обеспечить защищенный доступ к услугам сетей с разными требованиями по защищенности.

3. Для решения задачи сопряжения контуров обработки информации с разными требованиями по защищенности в современных МАУ предлагается использовать агентно-ориентированный подход, являющийся элементом искусственного интеллекта и построенный на основе клиент-серверной архитектуры. Данный подход позволит применить технологию удаленного управления программно-аппаратной конфигурацией МАУ на основе информации о его местоположении на и других атрибутах доступа.

4. Постановка задачи диссертационного исследования сформулирована как задача автоматического управления с элементами машинного обучения. Для ее решения предлагается использовать теорию машинного обучения, теории вероятности и математической статистики, аппарат скрытых марковских моделей, теорию алгоритмов, теорию управления, теорию оптимизации, теорию множеств, численные методы и методы математического и имитационного моделирования.

2. МОДЕЛЬ БЕЗОПАСНОСТИ МОБИЛЬНОГО АБОНЕНТСКОГО УСТРОЙСТВА В КОРПОРАТИВНЫХ СЕТЯХ С РАЗНЫМИ ТРЕБОВАНИЯМИ ПО ЗАЩИЩЕННОСТИ

Данный раздел посвящен разработке формальной модели безопасности МАУ. Отличительной особенностью данной модели является учет атрибутов доступа, включая местонахождение МАУ в специальных помещениях здания, в котором развернуты корпоративные сети с разными требованиями по защищенности. Предложена модель безопасности МАУ, обоснована ее корректность. На основе анализа технологий определения местоположения МАУ в помещениях внутри зданий предложено технологическое решение, позволяющее повысить достоверность определения местоположения МАУ в помещениях с разными требованиями по защищенности за счет применения метода статистических испытаний. Обосновано применение предложенного технологического решения для оценивания местонахождения МАУ на территории помещений организации с заданной точностью. Разработана имитационная модель, позволяющая оценить оптимальные параметры алгоритмов определения местоположения, проведена оценка его качества. Представлены результаты моделирования.

2.1. Постановка задачи на разработку модели

Рассматриваемая в качестве объекта исследования в диссертационной работе система управления безопасностью МАУ в корпоративных сетях с разными требованиями по защищенности может быть отнесена к компьютерной системе (КС). В соответствии с [5] при анализе безопасности КС, которые должны обладать высоким уровнем доверия, начиная с оценочного уровня доверия 5, согласно классификации по [5], требуется, чтобы при разработке КС была использована формальная модель политики безопасности.

Для анализа безопасности предлагаемой в работе системы управления МАУ и достижения цели исследования, заключающейся в повышении вероятности обеспечения безопасности информации при эксплуатации МАУ необходимо разработать модель безопасности МАУ, отличающуюся от известных учетом его местонахождения в корпоративных сетях с разными требованиями по защищенности. Формальная постановка задачи на разработку модели: на основе теорий множеств, конечных автоматов, машинного обучения, математической статистики и численных методов разработать модель безопасности МАУ.

Предлагаемая в работе модель безопасности МАУ базируется на классической модели Белла-ЛаПадулы [106], элементах ролевой [135, 139] и атрибутной [115] моделях управления доступом, а также и моделях безопасности, учитывающих местоположение субъектов [100, 102, 118].

Исходные данные:

1) элементы классической модели Белла-ЛаПадулы:

S – множество субъектов системы;

MD – множество МАУ, при этом $MD \subseteq S$;

O – множество объектов системы, включая функциональные блоки МАУ;

$P = \{read, write, append, execute\}$ – множество видов доступа и видов прав доступа;

$B = \{b \subseteq S \times O \times P\}$ – множество возможных множеств текущих доступов в системе;

$(L, \leq)$ – решетка конфиденциальности, например, $L = \{\text{"ОИ","КИ"}\}$, где "ОИ" < "КИ";

$\text{M} = \{m_{|S|\times|O|}\}$ – множество возможных матриц доступов, где $m_{|S|\times|O|}$ – матрица доступов, $m[s,o] \subseteq P$ – права доступа субъекта s к объекту o;

$(f_s, f_o, f_c, f_{loc}) \in F = L^S \times L^O \times L^S$ – четверка функций (f_s, f_o, f_c, f_{loc}), задающих соответственно: $f_s : S \to L$ – уровень доступа субъектов; $f_o : O \to L$ – уровень конфиденциальности объектов; $f_c : S \to L$ – текущий уровень доступа субъектов,

при этом для любого $s \in S$, выполняется неравенство $f_c(s) \le f_s(s)$; $f_{LOC} : LOC \to L$ – функция, определяющая уровень конфиденциальности местоположения;

$V = B \times M \times F$ – множество состояний системы;

Q – множество запросов к системе;

D – множество ответов по запросам, например $\{yes, no, error\}$;

$W \subseteq Q \times D \times V \times V$ – множество действий системы, где четверка $(q, d, v^*, v) \in W$ означает, что система по запросу q с ответом d перешла из состояния v в состояние v^*;

$\mathbb{N}_0 = \{0,1,2,...\}$ – множество значений времени;

X – множества функций $x : \mathbb{N}_0 \to Q$, задающих все возможные последовательности запросов к системе;

Y – множество функций $y : \mathbb{N}_0 \to D$, задающих все возможные последовательности ответов системы по запросам;

Z – множество функций $z : \mathbb{N}_0 \to V$, задающих все возможные последовательности состояний системы;

2) элементы мандатно-ролевого управления доступом:

R – множество ролей;

$CONF$ – множество возможных конфигураций МАУ, при этом $CONF \subseteq R$;

SS – множество сессий пользователей (субъектов);

$PA : R \to 2^P$ – функция, задающая для каждой роли множество прав доступа; при этом для каждого права доступа $p \in P$ существует роль $r \in R$ такая, что $p \in PA(r)$;

$SA : S \to 2^R$ – функция, задающая для каждого субъекта множество ролей, на которые он может быть авторизован, при этом для $MD \subseteq S$ $SA : MD \to 2^{CONF}$;

$user : SS \to S$ –функция, задающая для каждой сессии субъекта (пользователя), от имени которого она активизирована;

$device: SS \to S$ –функция, задающая для каждой сессии субъекта (МАУ), от имени которого она активизирована, при этом MD – множество МАУ и $MD \subseteq S$;

$roles: SS \to 2^R$ – функция, задающая для субъекта (пользователя) множество ролей, на которые он авторизован в данной сессии, при этом в каждый момент времени для каждой сессии $ss \in SS$ выполняется условие $roles(ss) \subseteq SA(user(ss))$;

$confs: SS \to 2^R$ – функция, задающая для субъекта (МАУ) множество конфигураций, на которые он авторизован в данной сессии, при этом в каждый момент времени для каждой сессии $ss \in SS$ выполняется условие $confs(ss) \subseteq SA(device(ss))$;

3) элементы атрибутной политики безопасности, учитывающей особенности программно-аппаратных конфигураций МАУ и его местоположение:

A – множество оцениваемых атрибутов доступа, таких как, например, идентификационные данные о пользователе, МАУ, операционной системе (ОС) и приложениях МАУ, сетевая адресная информация, уровень конфиденциальности и идентификатор запрашиваемой услуги, время запроса на доступ;

LOC – множество возможных местоположений;

$\mathrm{MA} = \left\{ ma_{|CONF|\times|A|} \right\}$ – множество возможных матриц атрибутов доступа, где $ma_{|CONF|\times|A|}$ – матрица требуемых атрибутов доступа, $ma[conf, a] \subseteq A$ – множество требуемых значений атрибутов доступа для конфигурации $conf$;

расположение и другие параметры помещений:

$$Rooms = \left\{ room_i = \left((x_{i1}, y_{i1}), (x_{i2}, y_{i2}), ..., (x_{in}, y_{in}), L_{Room_i} \right) \right\},\ i = \overline{1, N}_{Rooms}, \quad (2.14)$$

где L_{Room_i} – уровень требований по защищенности помещения; $(x_{i1}, y_{i1}), (x_{i2}, y_{i2}), ..., (x_{in}, y_{in})$ – координаты n углов помещений; N_{Rooms} – количество помещений;

расположение точек доступа БСПД $AP = \left\{ AP_j = \left(x_j, y_j \right) \right\}$, $j = \overline{1, N_{AP}}$, где (x_j, y_j) – координаты точек доступа, N_{AP} – количество точек доступа.

Требуется:

1) разработать формальную модель безопасности МАУ Z, отличающуюся от известных учетом его местонахождения в корпоративных сетях с разными требованиями по защищенности;

2) провести анализ безопасности разработанной модели безопасности МАУ;

3) осуществить имитационное моделирование оценивания достоверности определения местоположения МАУ в специальных помещениях корпоративных сетей с разным уровнем защищенности и оценить качество имитационной модели.

В современной теории компьютерной безопасности наибольше развитие в области формального моделирования безопасности КС получил подход, заключающейся в представлении исследуемой КС в виде абстрактной системы (конечного автомата), каждое состояние которой описывается доступами, реализуемыми субъектами к сущностям, а переходы КС из состояния в состояние описываются командами или правилами преобразования состояний, выполнение которых, как правило, инициируется субъектами. В основе данного подхода используется аксиома [144], позволяющая выделить элементы КС, необходимые для анализа ее безопасности.

Основная аксиома компьютерной безопасности. В рамках субъект-сущностного подхода все вопросы безопасности информации в КС описываются доступами к сущностям.

Основные определения субъект-сущностного подхода, такие как "сущность", "объект", "субъект", "доступ" даны в [5]. Разработка формальной модели безопасности МАУ в данной работе базируется на приведенных определениях.

2.2. Разработка формальной модели безопасности мобильного абонентского устройства и доказательство отсутствия запрещенных информационных потоков в компьютерной системе с мобильными абонентскими устройствами

Безопасность системы защиты должна учитывать особенности и угрозы безопасности, появляющиеся в ней в связи с наличием в компьютерной системе МАУ. Учет данных особенностей позволит повысить адекватность формальной модели безопасности и построенной на ее основе СЗИ.

Типовой состав современного МАУ представлен на рисунке 2.1. Очевидно, что такое устройство способно работать в режимах, запрещенных политикой безопасности ЗКС. Для блокирования работы МАУ в запрещенных режимах необходим механизм управления программно-аппаратной конфигурацией МАУ, например, на основе АПМДЗ, позволяющий обеспечить выполнение требований политики безопасности, установленной в ЗКС.

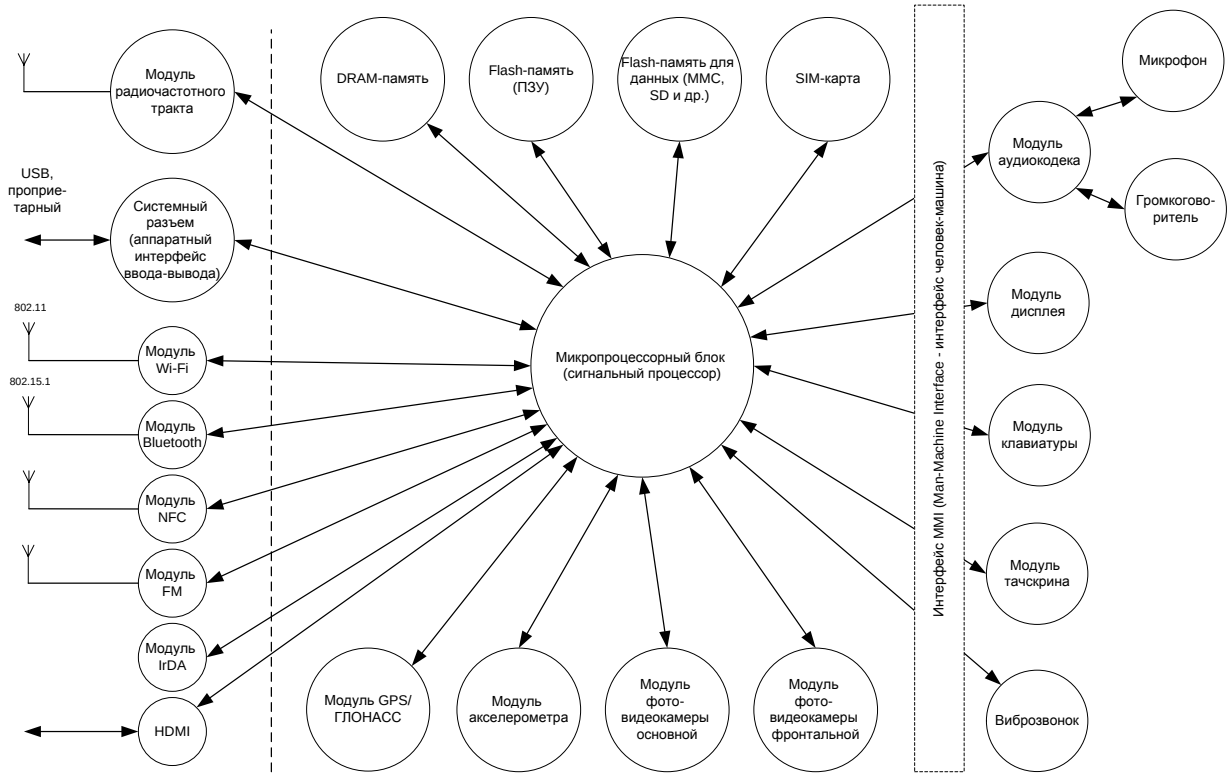
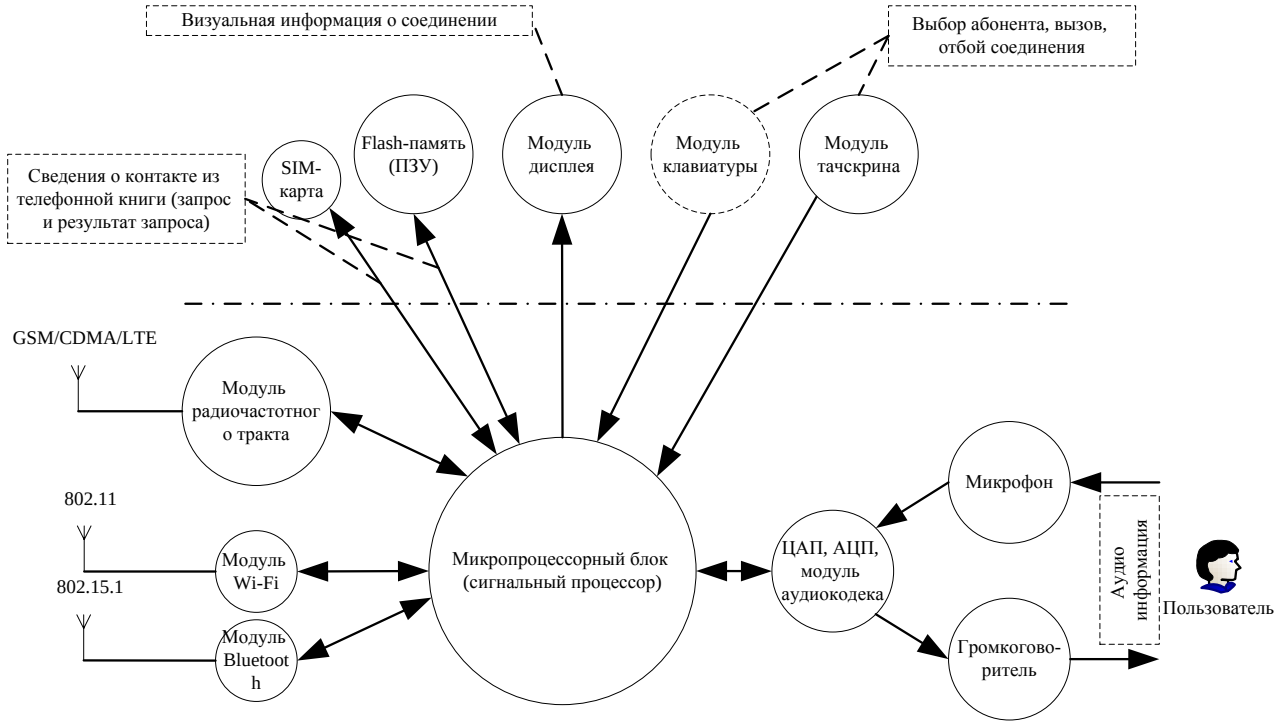


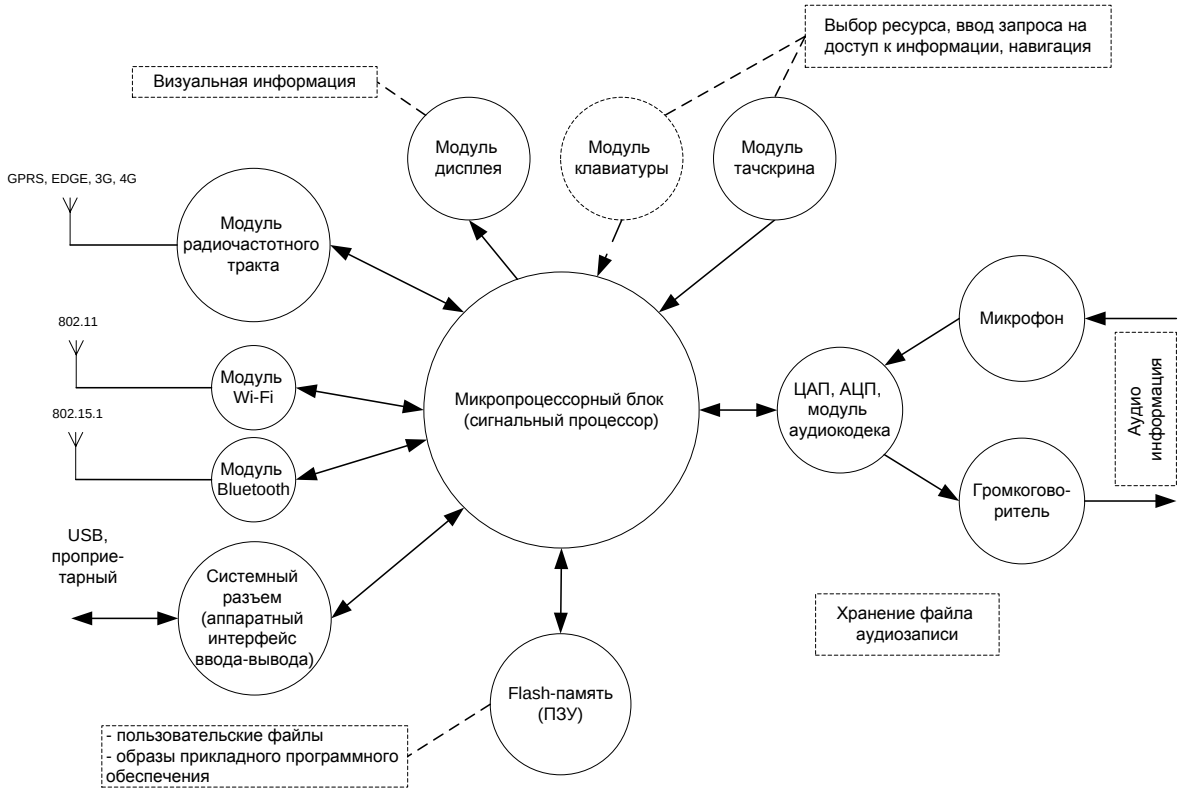
Рисунок 2.1 – Типовой состав современного МАУ

В формальной модели безопасности необходимо определить состояния КС, определяемые, в том числе, программно-аппаратной конфигурацией МАУ, обеспечивающие безопасность информации при заданных условиях доступа.

Для определения состава и структуры допустимых конфигураций МАУ целесообразно рассмотреть информационные тракты прохождения сигналов через МАУ при работе его в разных режимах [47]. На рисунке 2.2 представлен состав задействованных функциональных блоков МАУ: а) при информационном обмене голосовой информацией (без аудиозаписи разговора в локальную память), б) при информационном обмене данными.



а)



б)

Рисунок 2.2 – Состав задействованных функциональных блоков МАУ:
а) при информационном обмене голосовой информацией (без аудиозаписи разговора в локальную память); б) при обмене данных

Каждая программно-аппаратная конфигурация определяет набор тех или иных функциональных блоков МАУ, которые задействованы при предоставлении заданных услуг, а также набор прав доступа к этим функциональным блокам.

Для определения условий, в которых должны блокироваться запрещенные режимы работы МАУ, необходимо учитывать **атрибуты доступа**, связанные с пользователем МАУ, состоянием программно-аппаратной среды МАУ, адресной информацией и другими параметрами. К ним могут относиться:

– идентификационные данные о пользователе, МАУ, операционной системе (ОС) и приложениях МАУ;

– сетевая адресная информация;

– уровень конфиденциальности и идентификатор запрашиваемой услуги;

– время запроса на доступ.

Принципиально важным атрибутом доступа является местоположение. Требования безопасности к техническим средствам, включая СВТ и МАУ в рамках нормативных документов определяются, как правило, помещениями, в которых данные устройства находятся, в которых может быть предусмотрена обработка информации с ограниченным доступом. Учитывая, что местоположение МАУ является случайной величиной, а также недостаточно высокую точность определения местоположения при использовании технологий стандарта 802.11, данную характеристику состояния МАУ можно представить в виде вектора:

$$\vec{P}_{L_{Room}} = \left\{ P\left(\tilde{L}_{Room} = \text{"ОИ"} \right), P\left(\tilde{L}_{Room} = \text{"КИ"} \right) \right\}, \quad (2.1)$$

где $P\left(\tilde{L}_{Room} = \text{"ОИ"} \right)$ – вероятность того, что МАУ находится в помещении с уровнем требований по защищенности для открытой информации ("ОИ"); $P\left(\tilde{L}_{Room} = \text{"КИ"} \right)$ – вероятность того, что МАУ находится в помещении с уровнем требований по защищенности для конфиденциальной информации ("КИ").

Таким образом, для управления доступом в компьютерной системе с МАУ необходимо:

– множество объектов доступа O дополнить множеством функциональных блоков МАУ: ПЗУ, ОЗУ, ЦП, АПМДЗ, модули Bluetooth, дисплея, Wi-Fi, клавиатуры, GSM, USB, тачскрина, фото- и видеокамеры и другие;

– множество субъектов доступа S дополнить множеством МАУ MD, таким, что $MD \subseteq S$;

– множество ролей R дополнить множеством возможных конфигураций МАУ, таким, что $CONF \subseteq R$, при этом каждая конфигурация (роль) определяется набор тех или иных прав и видов прав доступа на объекты доступа, включающие в себя, в том числе, функциональные блоки МАУ;

– определить порядок оценивания местоположения с учетом известных технологий определения местоположения и их точности, позволяющий обеспечить требуемую достоверность;

– определить свойства системы защиты, учитывающие уровни конфиденциальности местоположения и особенности программно-аппаратных конфигураций МАУ с учетом мандатного разграничения доступа и особенностей функционирования системы определения местоположения МАУ.

2.2.1. Дополнения к классической модели Белла-ЛаПадулы в формальной модели безопасности мобильных абонентских устройств

Согласно [106] дано определение системы защиты на базе классической модели Белла-ЛаПадулы.

Определение 1. $\sum(Q,D,W,z_0)\subseteq X\times Y\times Z$ называется системой, когда для каждого $(x,y,z)\in\sum(Q,D,W,z_0)$ выполняется условие: для $t\in\mathbb{N}_0$, $(x_t,y_t,z_{t+1},z_t)\in W$, где z_0 – начальное состояние системы. При этом каждый набор $(x,y,z)\in\sum(Q,D,W,z_0)$ называется реализацией системы, а $(x_t,y_t,z_{t+1},z_t)\in W$ – действием системы в момент времени $t\in\mathbb{N}_0$.

Для данной системы в [106] также приведены определения трех свойств, на базе которой определяется ее безопасности:

ss – свойство простой безопасности (simple security);

* – свойства "звезда";

ds – свойства дискреционной безопасности (discretionary security).

Нарушения безопасности системы определяется утечкой права доступа, которое определяется тройкой (s,o,p). Относительно данных прав даны определения доступов в системе $\sum(Q,D,W,z_0)\subseteq X\times Y\times Z$, обладающих теми или иными из перечисленных свойств. На основе данных положений определено, какое состояние системы $\sum(Q,D,W,z_0)\subseteq X\times Y\times Z$ является безопасным и приведено последовательное доказательство данного утверждения для классической модели Белла-ЛаПадула [106].

На основе указанных утверждений и на базе известных формальных моделей [100, 102, 106, 115, 118, 135, 139] определены следующие свойства безопасности системы $\sum(Q, D, W, z_0) \subseteq X \times Y \times Z$:

ss – свойство простой безопасности (simple security);

* – свойства "звезда";

ds – свойство дискреционной безопасности (discretionary security).

Дополнительно введем новое свойство системы защиты, позволяющее повысить адекватность формальной модели условиям эксплуатации КС с МАУ:

as – свойства атрибутной безопасности (attribute security).

Свойства простой безопасности, "звезда" и свойство дискреционной безопасности описаны в классической модели Белл-ЛаПадулы [106]. Для целостного описания формальной модели безопасности МАУ приведены их определения.

Определение 2. Доступ $(s, o, p) \in S \times O \times P$ обладает *ss*-свойством относительно функций $f = (f_s, f_o, f_c) \in F$, когда выполняется одно из условий:

$p \in \{execute, append\}$;

$p \in \{read, write\}$ и $f_s(s) \geq f_o(o)$.

Определение 3. Состояние системы $(b, m, f) \in V$ обладает *ss*-свойством, когда каждый элемент $(s, o, p) \in b$ обладает *ss*-свойством относительно f.

Определение 4. Доступ $(s, o, p) \in S \times O \times P$ обладает *-свойством относительно функций $f = (f_s, f_o, f_c) \in F$, когда выполняется одно из условий:

$p \in execute$;

$p \in append$ и $f_o(o) \geq f_s(s)$;

$p \in read$ и $f_c(s) \geq f_o(o)$;

$p \in write$ и $f_c(s) = f_o(o)$.

Определение 5. Состояние системы $(b, m, f) \in V$ обладает *-свойством, когда каждый элемент $(s, o, p) \in b$ обладает *-свойством относительно f.

Определение 6. Состояние системы $(b,m,f)\in V$ обладает *-свойством относительно подмножества $S'\subseteq S$, когда каждый элемент $(s,o,p)\in b$, где $s\in S'$, обладает *-свойством относительно f. При этом $S\setminus S'$ называется подмножеством доверенных субъектов, т.е. субъектов, имеющих право нарушать требования *-свойства.

Определение 7. Состояние системы $(b,m,f)\in V$ обладает *ds*-свойством, когда каждого доступа $(s,o,p)\in b$ выполняется условие $p\in m[s,o]$.

Для учета особенностей эксплуатации МАУ в корпоративных сетях с разными требованиями по защищенности определим свойство атрибутной безопасности.

Определение 8. Состояние системы $(b,m,f)\in V$ обладает *as*-свойством, когда каждого доступа $(s,o,p)\in b$ выполняются одновременно условия $f_{LOC}(loc)=f_s(confs(ss))$, $f_{LOC}(loc)=f_s(user(ss))$ и $\left(\forall a\in A\,\exists a^{\text{треб}}\in A^{\text{треб}}: a\ =a^{\text{треб}}\ и\ a^{\text{треб}}\in ma[conf,a]\right)$.

Таким образом, на основе определений данных свойств можно сформулировать определения безопасного состояния компьютерной системы с МАУ.

Определение 9. Состояние системы (b,m,f) называется безопасным, когда оно обладает *-свойством относительно S', *ss*-свойством, *ds*-свойством и *as*-свойством.

Определение 10. Реализация системы $(x,y,z)\in\sum(Q,D,W,z_0)$ обладает *ss*-свойством (*-свойством, *ds*-свойством, *as*-свойством), когда в последовательности $(z_0,z_1,...)$ каждое состояние обладает *ss*-свойством (*-свойством, *ds*-свойством, *as*-свойством).

Определение 11. Система $\sum(Q,D,W,z_0)$ обладает *ss*-свойством (*-свойством, *ds*-свойством, *as*-свойством), когда каждая ее реализация обладает *ss*-свойством (*-свойством, *ds*-свойством, *as*-свойством).

Определение 12. Система $\sum(Q,D,W,z_0)$ называется безопасной, когда она обладает *ss*-свойством, *-свойством, *ds*-свойством, *as*-свойством одновременно.

Согласно [106] из описания данных свойств следует, что:

1. Из обладания доступом *-свойства относительно f следует обладание этим доступом ss-свойством относительно f.

2. Обладание системой *ss*-свойством обеспечивает запрет на чтение вверх, а также не допускает модификацию с использованием доступа *write*, когда $f_o(o) < f_s(s)$, задавая тем самым для субъекта s верхний уровень конфиденциальности объектов, к которым он может получить доступ *read* и *write*.

3. *-свойство исключает появление в системе запрещенного информационного потока "сверху вниз", выполняя требования мандатной политики безопасности.

4. Дополнительно введенное свойство атрибутной безопасности *as* обеспечивает выполнения требований политики безопасности для функционирования МАУ в разрешенных режимах, определяемых конфигурацией МАУ, в случае соответствия текущих условий (атрибутов) доступа, включая местоположение МАУ, заданным в требованиях политики безопасности.

Проверка безопасности системы для описанных свойств построена согласно [106] для условий безопасности, заданных на множестве действий системы $\sum(Q,D,W,z_0)$. Теоремы и их доказательства известны. Покажем, что система $\sum(Q,D,W,z_0)$ будет обладать новым свойством *as* атрибутной безопасности для множества всех возможных действий.

Теорема 1. Система $\sum(Q,D,W,z_0)$ обладает *as*-свойством атрибутной безопасности для любого начального состояния z_0, обладающего *as*-свойством, тогда и только тогда, когда для каждого действия $\left(q,d,\left(b^*,m^*,f^*\right),(b,m,f)\right)\in W$ выполняются условия 1, 2.

Условие 1. Каждый доступ $(s,o,p)\in b^*\setminus b$ обладает *as*-свойством относительно f^*.

Условие 2. Если $(s,o,p)\in b$ и не обладает *as*-свойством относительно f^*, то $(s,o,r)\notin b^*$.

Доказательство. Сначала докажем достаточность условий.

Достаточность. Пусть выполнены условия 1 и 2 и пусть $(x,y,z)\in\sum(Q,D,W,z_0)$ – произвольная реализация системы. Тогда $\left(x_t,y_t,(b_{t+1},m_{t+1},f_{t+1}),(b_t,m_t,f_t)\right)\in W$, где $z_{t+1}=(b_{t+1},m_{t+1},f_{t+1})$, $z_t=(b_t,m_t,f_t)$ для $t\in\mathbb{N}_0$.

Для $(s,o,p)\in b_{t+1}$ выполняется одно из условий: или $(s,o,p)\in b_{t+1}\setminus b_t$, или $(s,o,p)\in b_t$. Из условия 1 следует, что состояние системы z_{t+1} пополнилось доступами, которые обладают *as*-свойством относительно f^*. Из условия 2 следует, что доступы из b_t, которые не обладают *as*-свойством относительно f^*, не входят в b_{t+1}. Следовательно, каждый доступ $(s,o,p)\in b_{t+1}$ обладает *as*-свойством относительно f^* и по определению состояние z_{t+1} обладает *as*-свойством для $t\in\mathbb{N}_0$. Так как по условию состояние z_0 обладает *as*-свойством, то выбранная произвольная реализация (x,y,z) также обладает *as*-свойством. Достаточность условий теоремы доказана.

Необходимость. Пусть система $\sum(Q,D,W,z_0)$ обладает *as*-свойством. Будем считать, что во множество W входят только те действия системы, которые встречаются в ее реализациях. Тогда для каждого $\left(q,d,(b^*,m^*,f^*),(b,m,f)\right)\in W$ существует реализация $(x,y,z)\in\sum(Q,D,W,z_0)$ и существует $t\in\mathbb{N}_0$: $\left(q,d,(b^*,m^*,f^*),(b,m,f)\right)=(x_t,y_t,z_{t+1},z_t)$. Так как реализация системы (x,y,z) обладает *as*-свойством, то и состояние $z_{t+1}=(b^*,m^*,f^*)$ обладает *as*-свойством по

определению. Следовательно, условия 1 и 2 выполняются. Необходимость условий теоремы доказана. ■

Также в [25, 26, 106] доказано, что для описанной модели отсутствует логическая увязка условий выполнения системой свойств безопасности, данных в их определениях, с заложенными в модель условиями их проверки. В связи с этим большое значение имеет корректное определение свойств безопасности, непротиворечащее здравому смыслу и логике обеспечения безопасности информации.

Поскольку вновь введенное *as*-свойство атрибутной безопасности определяет совокупность дополнительных ограничений на доступы в системе, то такое описание свойства безопасности, как минимум, не ухудшает уровня безопасности, установленного в классической модели Белла-ЛаПадулы, а выполнение данного условия позволяет ограничить потенциально опасные доступы в системе, тем самым обеспечив выполнение заложенных в политику безопасности требований, и повысить адекватность формальной модели безопасности МАУ условиям ее эксплуатации в КС.

2.2.2. Дополнения к мандатной ролевой модели управления доступом в формальной модели безопасности мобильных абонентских устройств

В формальной модели безопасности МАУ учтены особенности мандатно-ролевого управления доступом. Анализ безопасности ролевого и мандатно-ролевого управления доступом известен и приведен в [29, 138, 139].

В предложенной формальной модели безопасности дополнительно введены следующие условия:

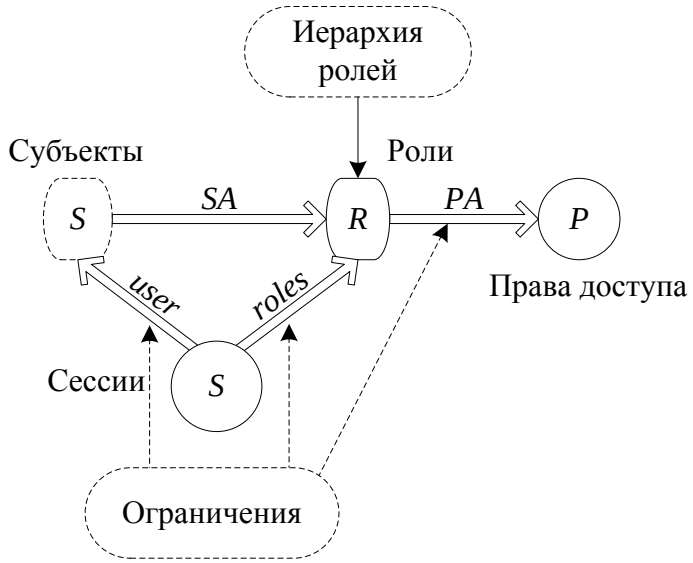
– множество МАУ *MD* представляет собой подмножество субъектов системы;

– множество функциональных блоков МАУ, таких как модуль GSM, Bluetooth, Wi-Fi, передача данных, фото- и видеокамера и другие определены как подмножество объектов системы;

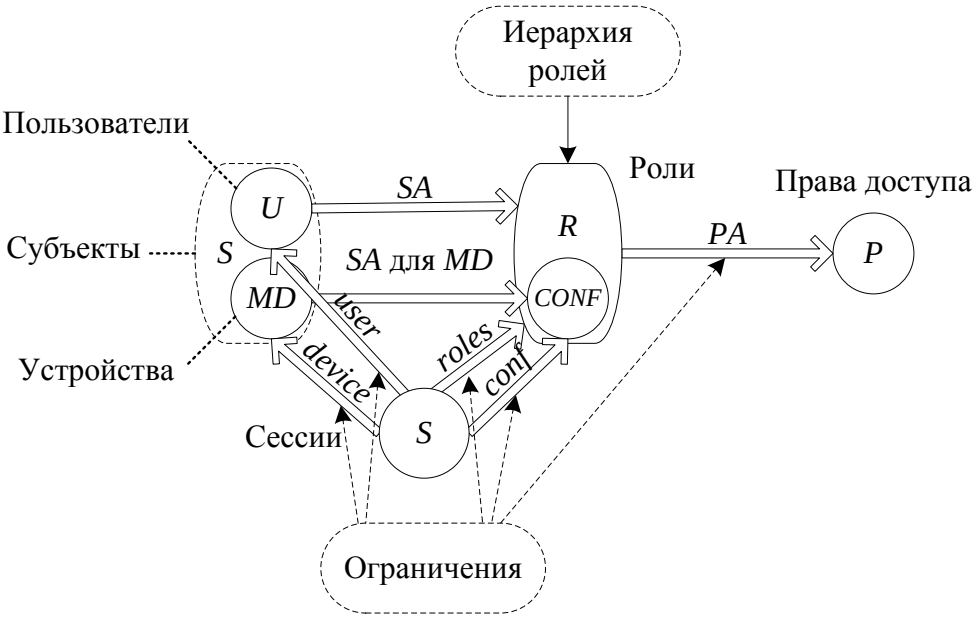
– конфигурация МАУ *conf* является аналогом роли пользователя, при этом подмножество конфигураций является элементом множества ролей;

– на множестве ролей определены соотношения $PA: R \to 2^P$ и $SA: S \to 2^R$, где каждой роли (конфигурации) задано множество прав доступа, относящихся к правам на доступ к функциональным блокам МАУ, и каждому мобильному абонентскому устройству $MD \subseteq S$ задано множество разрешенных конфигураций $SA: MD \to 2^{CONF}$.

В рамках теоретико-множественного подхода указанные условия сформулированы таким образом, что они расширяют множество субъектов, объектов и ролей, установленное в системе, не нарушая их целостности, но вводя дополнительные ограничения. В связи с этим ограничения, установленные для классических ролей, распространяются и на универсум ролей, включающих в свой состав конфигурации МАУ. Структура элементов классической ролевой модели управления доступом и ролевой модели управления доступом с конфигурациями МАУ представлены на рисунке 2.3. Из анализа рисунка 2.3б наглядно видно, что ограничения накладываются на условия определение ролей, включая конфигурации МАУ, а также права доступа.



а)



б)

Рисунок 2.3 – Структура элементов: а) классического ролевого управления доступом; б) ролевого управления доступом с МАУ и их конфигурациями

Как показано в [137] мандатное управление доступом сравнительно легко реализуется на базе ролевого управления доступом с доказательством невозможности реализации запрещенных информационных потоков от объектов с высоким уровнем конфиденциальности к объектам с низким уровнем конфиденциальности.

Покажем, что при введении понятия конфигурация МАУ, множество которых представляют собой аналог роли пользователя $CONF \subseteq R$, невозможна реализация запрещенных информационных потоков от объектов с высоким уровнем конфиденциальности к объектам с низким уровнем конфиденциальности.

Определение 13. Доступ$\left(s,\left(o,p\right)\right)\in S\times P$ является безопасным для либерального мандатного управления доступом, когда выполняется одно из условий:

$p=read$ и $f_s\left(user\left(ss\right)\right)\geq f_o\left(o\right)$ и $f_s\left(device\left(ss\right)\right)\geq f_o\left(o\right)$ (*ss*-свойство);

$p=write$ и, если существует доступ $\left(s,\left(o',read\right)\right)\in S\times P$, то $f_o\left(o\right)\geq f_o\left(o'\right)$ (либеральное *-свойство).

Определение 14. Доступ $\left(s,o,p\right)\in S\times P$ является безопасным для строгого мандатного управления доступом, когда выполняется одно из условий:

$p = read$ и $f_s(user(ss)) \geq f_o(o)$ и $f_s(device(ss)) \geq f_o(o)$ (*ss*-свойство);

$p = write$ и, если существует доступ $(s,(o',read)) \in S \times P$, то $f_o(o) = f_o(o')$ (строгое *-свойство).

Построим систему ролевого управления доступом на основе понятия конфигурация МАУ $CONF \subseteq R$. Пусть

$CONF = \{x\_read \mid x \in L\} \cup \{x\_write \mid x \in L\}$ – множество конфигураций МАУ;

$P = \{(o,read) \mid o \in O\} \cup \{(o,write) \mid o \in O\}$ – множество прав доступа, где *o* – функциональный модуль МАУ (например, модуль GSM, Wi-Fi, фото-, видео- камера и т.п.).

Зададим на множестве конфигураций МАУ $CONF$ иерархию, при этом иерархии конфигураций на множествах $\{x\_read \mid x \in L\}$ и $\{x\_write \mid x \in L\}$ будут независимы.

Определение 15. Иерархия на множестве конфигураций МАУ $CONF$ в соответствии с требованиями либерального мандатного управления доступом называется отношение частичного порядка "$\leq$", где для конфигураций МАУ $conf, conf' \in CONF$ справедливо неравенство $conf \leq conf'$, когда выполняется одно из условий:

$p = x\_read$, $p' = x'\_read$ и $x \leq x'$;

$p = x\_write$, $p' = x'\_write$ и $x' \leq x$.

Определение 16. Иерархией на множестве конфигураций МАУ $CONF$ в соответствии с требованиями строгого мандатного управления доступом называется отношение частичного порядка "$\leq$", где для конфигураций $conf, conf' \in CONF$ справедливо неравенство $conf \leq conf'$, когда выполняется одно из условий:

$p = x\_read$, $p' = x'\_read$ и $x \leq x'$;

$p = x\_write$, $p' = x'\_write$ и $x = x'$ (каждая конфигурация МАУ вида x_write сравнима только сама с собой.

Определение 17. Модель ролевого управления доступом соответствует требованиям мандатного управления доступом, когда иерархия на множестве конфигураций МАУ, являющейся подмножеством ролей, $CONF \subseteq R$ соответствует требованиям определения 15, и выполняются ограничения:

ограничение функции SA – для каждого субъекта (МАУ или пользователь) $s \in S$ конфигурация МАУ (роль) $x\_read = \oplus\left(SA(s) \cap \{y\_read \mid y \in L\}\right) \in SA(s)$ (здесь $x \in f_s(s)$ и $\{y\_write \mid y \in L\} \subset SA(s)$;

ограничение функции $conf$ – для каждой сессии $ss \in SS$ справедливо равенство $conf(ss) = \{y\_read \mid y \in L, y \le x\} \cup \{x\_write\}$;

ограничение функции PA – должно выполняться следующим образом:

для каждого $x \in L$ доступ $(o, read) \in PA(x\_read)$ тогда и только тогда, когда доступ $(o, write) \in PA(x\_write)$;

для каждого доступа $(o, read) \in P$ существует единственная конфигурация МАУ $x\_read : (o, read) \in PA(x\_read)$ (здесь $x = f_o(o)$).

Определение 18. Модель ролевого управления доступом соответствует требованиям строгого мандатного управления доступом, когда иерархия на множестве конфигураций МАУ, являющейся подмножеством ролей, $CONF \subseteq R$ соответствует требованиям определения 16, и выполняются ограничения:

ограничение функции SA – для каждого субъекта (МАУ или пользователь) $s \in S$ конфигурация МАУ (роль) $x\_read = \oplus\left(SA(s) \cap \{y\_read \mid y \in L\}\right) \in SA(s)$ (здесь $x = f_s(s)$ и $\{y\_write \mid y \in L\} \subset SA(s)$;

ограничение функции $confs$ – для каждой сессии $ss \in SS$ справедливо равенство $conf(ss) = \{x\_read \mid x\_write\}$;

ограничение функции PA – должно выполняться следующим образом:

для каждого $x \in L$ доступ $(o, read) \in PA(x\_read)$ тогда и только тогда, когда доступ $(o, write) \in PA(x\_write)$;

для каждого доступа $(o, read) \in P$ существует единственная конфигурация МАУ (роль) $x\_read : (o, read) \in PA(x\_read)$ (здесь $x = f_o(o)$).

Таким образом, требования соответствия либеральному и строгому мандатному управлению доступом для моделей ролевого управления доступом совпадают во всем, кроме требований к соответствующей иерархии ролей и ограничениям на функцию *confs*.

В рамках модели мандатного ролевого управления доступом с конфигурациями МАУ такими, что $CONF \subseteq R$, дадим определение информационного потока.

Определение 19. Будем считать, что существует информационный поток от объекта $o \in O$ к объекту $o' \in O$ (функционального модуля МАУ) тогда и только тогда, когда существуют конфигурации $conf, conf' \in CONF$, сессия $ss \in SS$ такие, что $(o, read) \in PA(conf)$, $(o', write) \in PA(r')$ и $r, r' \in confs(ss)$.

Обоснуем, что в модели ролевого управления доступом, соответствующей требованиям либерального и строгого мандатного управления доступом, невозможна реализация запрещенных информационных потоков от объектов с высоким уровнем конфиденциальности к объектам с низким уровнем конфиденциальности.

Теорема 2. Если модель ролевого управления доступом с конфигурациями МАУ соответствует требованиям либерального или строгого мандатного управления доступом, то в ней для любых объектов $o' \in O$ таких, что $f_o(o) > f_o(o')$, невозможно возникновение информационного потока от o к o'.

Доказательство. Докажем от противного. Пусть существуют объекты (функциональные модули МАУ) $o, o' \in O$ такие, что $f_o(o) > f_o(o')$, и возможно возникновение информационного потока от o к o'. По определению 19 существуют конфигурации МАУ $conf, conf' \in CONF$ и сессия $ss \in SS$ такие, что $(o, read) \in PA(conf)$, $(o', write) \in PA(conf')$ и $conf, conf' \in confs(ss)$. Следовательно, выполняется одно из условий:

выполняются требования либерального мандатного управления доступом и по определению 15 выполняются условия $conf = f_o(o)\_read$, $conf' = f_o(o')\_write$ и $f_o(o) \le f_o(o')$;

выполняются требования строгого мандатного управления доступом и по определению 16 выполняются условия $conf = f_o(o)\_read$, $conf' = f_o(o')\_write$ и $f_o(o) = f_o(o')$.

Противоречие. Теорема доказана. ■

Доказательство теорем 1 и 2, в которых учтено наличие в компьютерной системе МАУ, с помощью которых пользователи могут получать доступ к услугам корпоративных сетей с разными требованиями по защищенности, их местоположение и условия доступа, показывает, что предложенная формальная модель безопасности МАУ может быть применена в качестве основы для реализации требований политики безопасности в корпоративных сетях с разными требованиями по защищенности, эксплуатирующие МАУ.

2.3. Имитационное моделирование определения местоположения мобильного абонентского устройства, позволяющее оценить достоверность местонахождения мобильного абонентского устройства в специальном помещении

Необходимо отметить, что за рамками формальной модели безопасности МАУ и представленных доказательств осталась проблема точности определения местоположения МАУ и, в частности, точность определения местоположения МАУ в помещениях внутри здания. В отличие от определения местоположения на открытой местности внутри зданий нет возможности использовать спутниковую навигацию из-за слабого сигнала, при этом СЗИ требуют точности, соизмеримой с точностью, достигаемой в спутниковых системах навигации.

К базовым принципам [99, 120, 142], на которых основываются все способы определения местоположения, относятся:

– триангуляция и трилатерация – оценивание местоположения на основе геометрических свойств углов до объекта (триангуляция) или расстояний от трех и более объектов с известным местоположением (трилатерация) [99, 120];

– анализ карты измерений – оценка местоположения на основе карты точек измерений параметров сигнала (карты сигнального пространства) [101, 103, 104, 105, 107, 126, 130, 132 145];

– анализ близости – определение местоположения по близости к приемнику сигнала относительно других [30, 58];

– анализ динамики движения [73, 108, 142, 145].

Показатели для оценивания качества системы определения местоположения подробно представлены в [142, 143]. Сравнительная характеристика и оценка некоторых известных систем определения местоположения по представленным показателям качества представлена в таблице 2.1.

Таблица 2.1 – Сравнительная характеристика систем и технических решений определения местоположения

Система / Тех.реш.	Беспроводная технология / Алгоритм	Точн.	Погрешность	Сложность	Масшт. / Разреш.	Стоим.
Microsoft RADAR [103, 104]	Wi-Fi / метод *k*-ближайших соседей, алгоритм Витерби	3-5 м	50 % при 2,5 м, 90 % при 5,9 м	Ср	Хор / 2D, 3D	Низ
Horus [149]	Wi-Fi / вероятностный метод	2 м	90 % при 2,1 м	Ср	Хор / 2D	Низ
DIT [105, 107]	Wi-Fi / 1) нейронные сети 2) метод опорных векторов (МОВ)	3 м	1) 90 % при 5,12 м 2) 90 % при 5,4 м	Ср	Хор / 2D, 3D	Низ
Ekahau [130]	Wi-Fi / вероятностный метод (отслеживание)	1 м	50 % при 2 м	Ср	Хор / 2D	Низ
SnapTrack	GPS, TDOA	5 м – 50 м	50 % при 25 м	Выс	Хор / 2D, 3D	Ср
WhereNet	УВЧ-диапазон, TDOA / 1) метод наименьших квадратов; 2) метод минимальных остатков	2-3 м	50 % при 3 м	Ср	Оч. хор / 2D, 3D	Низ
Robot-based [126, 145]	Wi-Fi / Байесовский подход	1,5 м	Более 50 % при 1,5 м	Ср	Хор / 2D	Ср
Sappire Dart	Разнонаправленная СШП, TDOA	< 30 см	50 % при 30 см	0,1 Гц – 1 Гц	Хор / 2D, 3D	

Окончание таблицы 2.1.

Система / Тех.реш.	Беспроводная технология / Алгоритм	Точн.	Погрешность	Слож-ность	Масшт. / Разреш.	Сто-им.
MultiLoc [128]	Wi-Fi / SMP (Symmetric Multiprocessing)	2,7 м	50 % при 2,7 м.	Низ	Хор / 2D	Ср
LAND-MARC	Активный RFID, RSS / метод *k*-ближайших соседей	< 2 м	50 % при 1 м	Ср	Узлы разм. плотно	Низ
TIX [109]	Wi-Fi / TIX (Triangular Interpolation and eXtrapolation)	5,4 м	50 % при 5,4 м	Низ	Хор / 2D	Ср
PinPoint 3D-1D	УКВ (40МГц), RTOF / Байесовский подход	1 м	50 % при 1 м	5 с	Хор / 2D	Хор
GSM-"почерк"	GSM, RSS / Взвешенный метод *k* NN	5 м	80 % при 10 м	Ср	Отл / 2D, 3D	Ср
FLIPS [101]	Wi-Fi / Триангуляция и нечеткая логика	2 м	Более 50 % при 2 м	Ср	Хор / 2D	Ср

Сравнительный анализ технологий определения местоположения по точности и назначению приведен на рисунке 2.4.

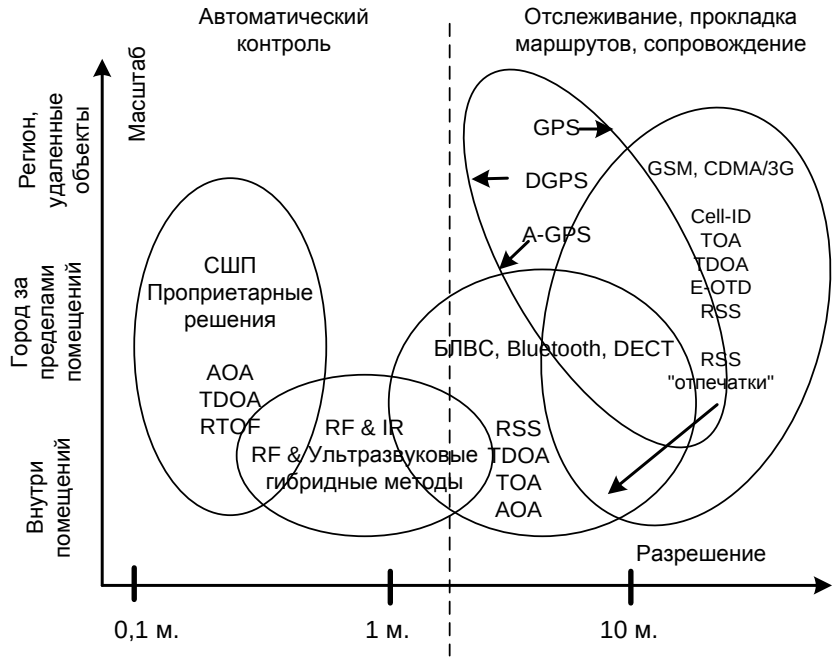


Рисунок 2.4 – Сравнительный технологий определения местоположения

Из анализа рисунка видно, что технологий, используемых для определения местоположения, относительно немного. К ним относятся GSM/CDMA/3G/LTE;

RFID/Bluetooth/Wi-Fi; УКВ/СШП, а также технологии, использующие лазерные дальномеры и датчики, измеряющие ориентацию в пространстве – альтиметры, гироскопы и 3Д-акселерометры, ВОЛС. В работе [73] показано, что современный технологический уровень не позволяет использовать инерциальные датчики в качестве основы для системы определения местоположения в помещениях вследствие эффекта накопления ошибки за краткосрочный период. Данные недостатки были частично устранены в технологии Google Tango [108], использующей в качестве дополнительной размерности, характеризующей местоположение МАУ внутри здания, графический поток, получаемый из встроенной в МАУ камеры, и соответствующую ему базу данных координат в виде 3Д-модели здания. Очевидно, что данная технология не применима в ЗКС из-за требований ИБ.

Технологии спутниковой навигации не применимы внутри помещений из-за значительного затухания сигнала от спутников [51]. Технологии на базе сигналов GSM/CDMA/3G/LTE обладают низкой точностью для решения задачи определения местоположения МАУ. Ультразвуковые методы, методы радиочастотной идентификации (RFID), технологии на базе ВОЛС не позволяют организовать защищенный канал управления МАУ, а некоторые из них не обеспечивают, в том числе, идентификацию МАУ.

К системе определения местоположения МАУ предъявляется ряд требований, выполнение которых влияет на обеспечение конфиденциальности информации:

– точность определения местоположения должна позволять идентифицировать помещение, в котором находится пользователь МАУ, с минимальной ошибкой 2-го рода;

– должна обеспечиваться идентификация пользователя МАУ в системе определения местоположения.

Исходя из анализа таблицы 2.1 и рисунка 2.4, а также известных особенностей технических реализаций указанных технологий, приемлемую точность определения местоположения внутри здания, а также идентификацию пользователя МАУ, позволяют обеспечивать методы, основанные на применения радиочастот-

ной идентификации (RFID), а также методы, основанные на применении БСПД. На основе работ [51, 99, 120, 126, 130] был проведен сравнительный анализа данных технологий. Результаты анализа представлены в таблице 2.2.

Таблица 2.2 – Сравнительный анализ эффективности датчиков радиочастотной идентификации и БСПД для решения задачи определения местоположения МАУ

Показатель	Технология	
	Радиочастотная идентификация (RFID)	Беспроводные сети передачи данных (802.11)
Средняя стоимость	Низкая/Средняя (для активных RFID)	Средняя
Точность	менее 1 м	1-7 м
Сложность реализации	Средняя	Низкая/Средняя (для систем с обучением)
Масштабируемость	Низкая	Хорошая
Пространственное покрытие	2D	3D
Устойчивость к помехам	Низкая	Хорошая
Стойкость к атакам типа "человек посередине"	Низкая	Высокая
Возможность создания канала управления МАУ	Отсутствует	Есть
Необходимость наличия считывателя/RFID-метки в МАУ	Есть (отсутствует в МАУ в настоящее время)	Есть (есть в большинстве современных МАУ)

В отличие от технологии RFID способы определения местоположения на основе БСПД лишены данных недостатков, но при этом обладают более высокой стоимостью и меньшей точностью определения местоположения МАУ. В ряде научных публикаций [51, 99, 112, 116, 120, 130, 142] предлагается использовать комбинированные технические решения, позволяющие компенсировать недостатки обеих.

Задача определения местоположения и задача защищенного информационного взаимодействия может решаться с использованием единого модуля беспроводной связи стандарта 802.11, либо может быть разделена на технологически независимые беспроводные модули. Для сигналов стандарта 802.11 решение задачи определения местоположения может быть осуществлено с использованием методов триангуляции (трилатерации) и анализа карты сигнального пространства. Следует отметить, что метод трилатерации не требует проведения предваритель-

ных измерений уровня сигналов сети в отличие от методов анализа карты измерений, что существенно упрощает ее разработку, эксплуатацию и сопровождение. Однако в то же время подсистемы определения местоположения, основанные на методе трилатерации, обладают гораздо более низкой точностью по сравнению с системами на основе анализа карты сигнального пространства.

С точки зрения решения задачи диссертационного исследования при определении местоположения существенное значение имеет не столько координаты нахождения МАУ, сколько помещение, в котором оно находится. Причина этого заключается в том, что требования безопасности определяются именно помещением, в котором находится МАУ. Очевидно, что помещение – это существенно более грубый объект для распознавания по сравнению с координатами МАУ. Каждая из рассмотренных технологий определения местоположения на базе БСПД и стандарта 802.11 предназначена именно для вычисления координат точки местоположения МАУ на карте, а уже по точке определяется помещение, к которому она относится.

Необходимо отметить, что погрешность данных технологий позволяет говорить не о координатах точки местоположения МАУ, а об окружности, в пределах которой может находиться устройство, при этом радиус данной окружности равен максимальной ошибки определения местоположения для заданной технологии. Учитывая, что в пределах данной окружности могут находиться разные помещения с разными требованиями по защищенности, была предложена следующая **гипотеза.** Для повышения достоверности определения местонахождения МАУ в специальных помещениях, к которым предъявляются повышенные требования по защищенности, необходимо вычислить площадь помещений каждого уровня защищенности, находящихся внутри окружности, определяющей вероятное местонахождение МАУ. Отношение полученной площади помещений к общей площади данной окружности позволит определить вероятность нахождения МАУ в специальном помещении.

В качестве базовых технологий, использующих БСПД для определения местоположения, а также для *обоснования алгоритмической разрешимости* предла-

гаемого подхода по вычислению вероятности нахождения МАУ в специальном помещении вне зависимости от выбранного метода, предлагается использовать технологии, основанные на применении:

– метода трилатерации (триангуляции) сигнала МАУ, принимаемого несколькими точками доступа БСПД [9, 109];

– метода k-ближайших соседей [103, 104];

– метода, основанного на использование байесовского подхода [132].

– Математический аппарат, на основе которого строятся данные технологии, и исследование их эффективности представлены в приложении А и работах [43, 50, 79]. Выбор данных методов обусловлен:

– разной вычислительной сложностью;

– разными требованиями по обслуживанию и вычислительной мощности;

– различной погрешностью определения местоположения.

Решение задачи вычисления площади помещений каждого уровня защищённости, находящихся внутри окружности и определяющей вероятное нахождения МАУ, необходимо решать, исходя из следующих условий:

– конфигурация и расположение помещений заранее известна;

– координаты точки местоположения МАУ и расположение окружности, в пределах которой может находиться МАУ, каждый раз вычисляется известными методами;

– конфигурация и расположение помещений внутри данной окружности представляют собой геометрические объекты произвольной формы;

– максимальный радиус окружности, в пределах которой может находиться МАУ, зависит от используемой технологии определения местоположения и равен максимальному значению ошибки определения местоположения для заданной технологии, получаемому эмпирическим путем.

При указанных условиях использование классического геометрического подхода для вычисления площади фигуры неприемлемо, в первую очередь, в связи с необходимостью вычисления площади фигур произвольной конфигурации в

каждый момент времени и необходимостью учета большого количество возможных вариантов. Наиболее подходящим способом определения площадей произвольных фигур является метод статистических испытаний – метод Монте-Карло [42, 51, 125]. Данный метод позволяет определить площадь произвольной фигуры внутри окружности, определяющей вероятное местонахождение МАУ, однако может потребоваться предварительное обучение.

Предварительное обучение заключается в сборе статистики ошибок определения местоположения для заданной технологии. Данная статистика (ряд распределения значений ошибки определения местоположения) является основой для проведения статистических испытаний. При этом случайной величиной является ошибка определения местоположения.

Применение метода Монте-Карло для вычисления вероятности нахождения МАУ в специальном помещении [51] при использовании совместно с технологиями определения местоположения на базе БСПД позволит снизить влияние неустойчивости радиосигналов БСПД на ошибку определения местоположения МАУ и повысить достоверность вычисления вероятности нахождения МАУ в специальном помещении ЗКС.

2.3.1. Модель системы определения местоположения мобильного абонентского устройства, позволяющая оценить вероятность его местонахождения в специальном помещении с повышенными требованиями по защищенности

Как было показано ранее, ключевое значение для определения требований безопасности, предъявляемых к МАУ, имеют не столько координаты его местонахождения, сколько информация о помещении, в котором он находится. Поэтому для решения задачи определения вероятности местонахождения МАУ в специальном помещении необходимы сведения о составе и параметрах помещений ЗКС. Данные сведения характеризуют **описательную модель здания** и могут быть представлены в виде

$$Rooms = \left\{ \left((x_{i1}, y_{i1}), ..., (x_{in}, y_{in}), L_{Room_i} \right) \right\}, i = \overline{1, N_{Room}}, \quad (2.2)$$

где $(x_{i1}, y_{i1}), ..., (x_{in}, y_{in})$ – координаты n углов i-го помещения, с уровнем требований по защищенности L_{Room_i}; N_{Room} – количество помещений.

В результате вычисления местоположения в соответствие с представленными моделями определения местоположения МАУ могут быть получены координаты МАУ – $(\tilde{x}, \tilde{y})$. Ошибка измерения местоположения в этом случае с учетом того, что реальное положение МАУ – (x, y), вычисляется с помощью выражения:

$$e_L = \sqrt{(x - \tilde{x})^2 + (y - \tilde{y})^2}. \quad (2.3)$$

В таблице 2.1 представлены статистические характеристики ошибки измерений местоположений для различных технологий определения местоположения в помещениях внутри здания. Как видно из данной таблицы, реальное местоположение пользователя МАУ находится в пределах окружности с центром с координатами $(\tilde{x}, \tilde{y})$ и радиусом, равным максимальному значению ошибки измерения местоположения: $R_e = \max[e_L]$. Учитывая, что величина R_e соизмерима с габаритами помещений, то реальное местоположение пользователя МАУ может значительно отличаться от вычисленного, поэтому решение задачи определения вероятности местонахождения МАУ в специальном помещении является нетривиальной и требует учета дополнительных факторов. Графическая иллюстрация данной задачи представлена на рисунке 2.5.

Из анализа рисунка 2.5 видно, что реальное местоположение МАУ (x, y) может находиться в помещениях любого уровня требований по защищенности, поскольку в радиусе максимальной ошибки измерения местоположения R_e от вычисленной точки $(\tilde{x}, \tilde{y})$ находятся помещения всех уровней. Очевидно, что значения координат вычисленной точки $(\tilde{x}, \tilde{y})$ зависят от ряда факторов, воздействующих случайным образом, а также выбранной технологии определения местоположения. Учитывая, что карта расположения помещений известна, а также могут быть получены эмпирическим путем (на этапе обучения системы) статистические

параметры ошибки измерения местоположения, можно оценить вероятность того, что пользователь находится в помещении с заданным уровнем требований по защищенности.

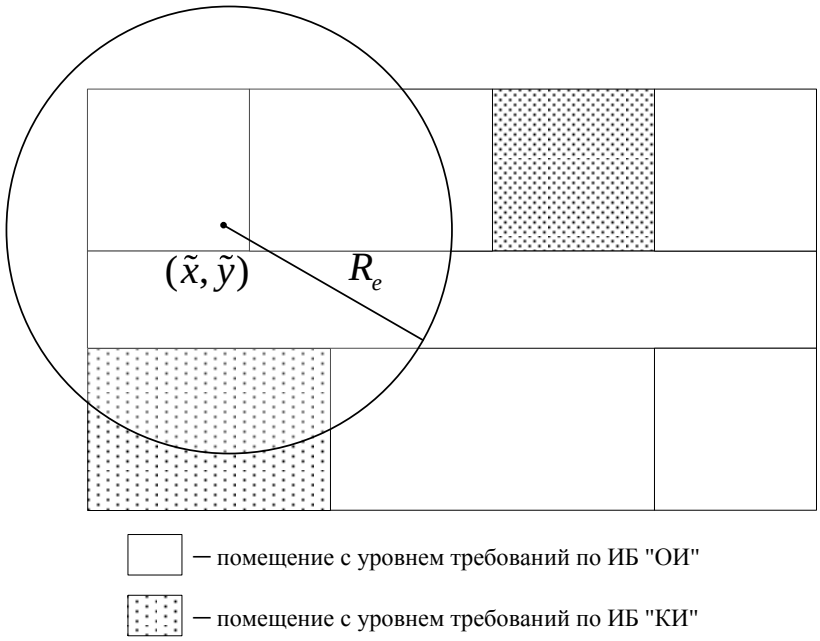


Рисунок 2.5 – Задача определения вероятности местонахождения МАУ в специальном помещении

Зная координаты центра окружности $(\tilde{x},\tilde{y})$, ее радиус R_e и карту расположения помещений, оценка вероятности того, что пользователь находится в помещении с заданным уровнем по защищенности, может быть представлена как отношение площади помещений заданного уровня к площади окружности с центром в точке $(\tilde{x},\tilde{y})$ и радиусом R_e. Таким образом, для ЗКС с уровнями требований по защищенности помещений $L_{Room}=\{\text{"ОИ","КИ"}\}$ оценка вероятности того, что пользователь находится в помещении с заданным уровнем требований по защищенности может быть представлена в виде выражения:

$$P(\tilde{L}_{Room}=L_{Room})=\frac{F_{Sq}\left(L_{Room},(\tilde{x},\tilde{y}),R_e\right)}{\pi\cdot R_e^2}, \qquad (2.4)$$

где L_{Room} – заданный уровень требований по защищенности, для которого производится оценивание; R_e – радиус окружности, характеризующей максимальную ошибку измерения местоположения; $(\tilde{x}, \tilde{y})$ – координаты вычисленного местоположения; $F_{Sq}\left(L_{Room}, (\tilde{x}, \tilde{y}), R_e\right)$ – функция, вычисляющая площадь помещений с уровнем L_{Room}, находящихся внутри окружности с центром в точке $(\tilde{x}, \tilde{y})$, радиусом R_e и площадью $\pi \cdot R_e^2$.

Тогда оценка вероятности того, что пользователь находится в помещении с тем или иным уровнем требований по защищенности может быть представлена в виде вектора:

$$P_{L_{Room}} = \left\{ P(\tilde{L}_{Room} = \text{"ОИ"}), P(\tilde{L}_{Room} = \text{"КИ"}) \right\}. \quad (2.5)$$

Вычисление функции $F_{Sq}\left(L_{Room}, (\tilde{x}, \tilde{y}), R_e\right)$ для произвольной конфигурации расположения помещений, а также произвольных значений $(\tilde{x}, \tilde{y})$ и R_e является трудноразрешимой задачей для геометрических методов, однако она легко может быть решена численным методом на основе метода статистических испытаний (метода Монте-Карло) [51, 125]. Данный метод основан на получении большого числа реализации стохастического (случайного) процесса, формируемого таким образом, чтобы его вероятностные характеристики совпадали с аналогичными величинами решаемой задачи.

Реализация метода Монте-Карло в целях решения задачи вычисления функции $F_{Sq}\left(L_{Room}, (\tilde{x}, \tilde{y}), R_e\right)$ заключается в следующем:

1) с помощью генератора случайных чисел с заданным законом распределения вероятностей формируются координаты случайной точки $(x_i', y_i'), i = \overline{1, N}_{MC}$ таким образом, чтобы они лежали внутри окружности с центром в точке $(\tilde{x}, \tilde{y})$ и радиусом R_e, где N_{MC} – количество экспериментов;

2) определяется помещение, в котором находится текущая точка (x_i', y_i'), и соответствующий ему уровень требований по ИБ – $\tilde{L}_{Room} = F_{L_{Room}}\left((x_i', y_i'), Rooms\right)$,

где $Rooms = \left\{ room_i = \left((x_{i1}, y_{i1}), (x_{i2}, y_{i2}), ..., (x_{in}, y_{in}), L_{Room_i} \right) \right\}$ – расположение и уровни требований по защищенности помещений, $i = \overline{1, N}_{Rooms}$, $(x_{i1}, y_{i1}), (x_{i2}, y_{i2}), ..., (x_{in}, y_{in})$ – координаты n углов помещений, N_{Rooms} – количество помещений;

3) счетчик попаданий в помещения с $L_{Room_i} = \tilde{L}_{Room}$ увеличивается на единицу – $N\left(L_{Room_i}\right) := N\left(L_{Room_i}\right) + 1$.

Закон распределения вероятностей для случайных величин – координат точки $\left(x_i', y_i'\right), i = \overline{1, N}_{MC}$ зависит от используемой технологии определения местоположения. Величина $\left(x_i', y_i'\right)$ характеризует вычисленное местоположение МАУ и формируется на основе статистики измерений ошибок определения местоположения. Сбор данной статистики осуществляется на этапе развертывания БСПД.

Поскольку конфигурация помещений в различных зданиях отлична друг от друга, материалы стен, межкомнатных перекрытий и дверей вносят искажения в распространение радиосигнала и сам сигнал БСПД достаточно нестабильный, то целесообразно статистику измерений ошибок определения местоположения представить в виде гистограммы частот (ряда распределения):

$$\lambda_{e_L} = \left\{ R_e, P\left\{a \le e_L < b\right\} = \sum_{a \le e_L < b} p(e_L) \middle| \sum_{0 \le e_L \le R_e} p(e_L) = 1 \right\}, \qquad (2.6)$$

где R_e – максимальное значение ошибки определения местоположения; $P\left\{a \le e_L < b\right\}$ – вероятность того, что ошибка определения местоположения лежит на отрезке (a, b), где a – нижняя граница, b – верхняя граница отрезка; $\sum_{a \le e_L < b} p(e_L)$ – сумма вероятностей возникновения ошибки определения местоположения, равной величине e_L. Графическое представление данного ряда распределения для рассматриваемых технологий изображено на рисунке А.3.

Оценка времени обучения системы определения местоположения для получения ряда распределения (2.6) зависит от количества измерений в помещениях и их плотности. Время измерения уровня принимаемого сигнала в современных

точках доступа и МАУ составляет доли секунды. Для исследуемой карты помещений, представленной на рисунке А.1, число точек измерений для методов k-ближайших соседей и байесовского подхода, с учетом того, что измерения осуществлялись через каждый метр по горизонтали и вертикали, формируя таким образом сетку измерений, составило значения порядка 400 точек. Значения получено с использованием программы для ЭВМ [79]. Таким образом, оценочное значение времени обучения системы определения местоположения для рассматриваемого примера составляет ориентировочно 7 минут без учета времени, затрачиваемого на перемещения измерителя.

Поскольку на результат измерения уровня сигнала оказывает достаточно большое количество факторов [119], включая конфигурацию помещений, размещение мебели, количество излучателей и точек приема, то периодичность переобучения системы определения местоположения необходимо устанавливать исходя из фактических изменений в данных параметрах:

– перепланировка здания;

– изменение интерьера здания;

– регистрация новых пользователей МАУ;

– изменения оборудования БСПД;

– планируемые мероприятия с привлечением новых пользователей МАУ

и другие события.

Первый этап реализации метода Монте-Карло – формирование случайной точки (x_i', y_i') по заданному закону распределения. Основой метода Монте-Карло является получение большого числа реализации стохастического (случайного) процесса, формируемого таким образом, чтобы его вероятностные характеристики совпадали с аналогичными величинами решаемой задачи. Для текущей задачи таким стохастическим процессом является процесс определения местоположения, а случайной величиной – ошибка измерения местоположения. Поэтому генератор случайных чисел, формирующий координаты случайной точки $(x_i', y_i'), i = \overline{1, N_{MC}}$ должен вырабатывать случайные числа в соответствие с законом распределения

ошибки измерения местоположения. Ряды распределения в виде гистограмм частот ошибок определения местоположения для различных технологий представлены на рисунке А.3. Если представить плотность распределения ошибки определения местоположения в виде градиента внутри окружности с диаметром R_e, то графически это будет выглядеть примерно так, как показано на рисунке 2.6. Из данного рисунка видно, что координаты случайных точек $(x_i', y_i'), i = \overline{1, N_{MC}}$ при формировании их по законам, представленным в виде рядов распределения и изображенных на рисунке А.3, чаще оказываются в районе центра окружности, чем у ее краев. Такой подход позволяет учесть особенности используемой технологии определения местоположения и повысить достоверность процесса классификации местоположения МАУ.

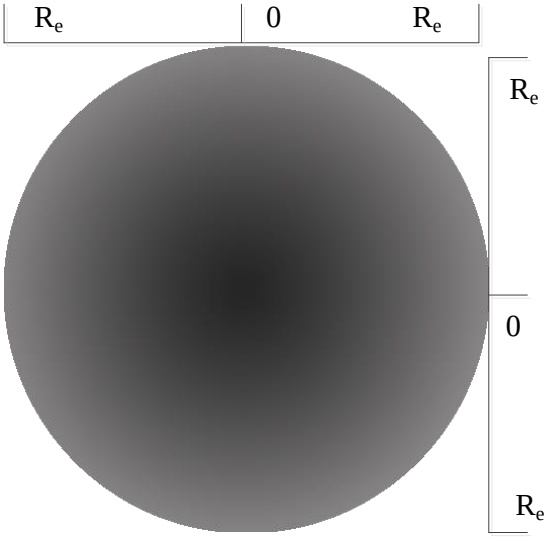


Рисунок 2.6 – Графическое представление плотности распределения ошибки определения местоположения внутри зоны погрешности с радиусом R_e

В результате применения метода Монте-Карло значение функции $F_{Sq}\left(L_{Room}, (\tilde{x}, \tilde{y}), R_e\right)$ вычисляется как

$$F_{Sq}\left(L_{Room}, (\tilde{x}, \tilde{y}), R_e\right) = \frac{N\left(L_{Room}\right)}{N_{MC}}, \qquad (2.7)$$

а оценка вероятностей того, что пользователь находится в помещении с того или иного уровня защищенности:

$$P_{L_{Room}} = \left\{ \frac{N(\tilde{L}_{Room} = \text{"ОИ"})}{N_{MC}}, \frac{N(\tilde{L}_{Room} = \text{"КИ"})}{N_{MC}} \right\}. \quad (2.8)$$

Точность данного метода существенно зависит от числа испытаний – N_{MC} и параметров генератора случайных чисел, используемого для формирования координат случайной точки $(x_i', y_i'), i = \overline{1, N}_{MC}$. В работе [4, с. 235] погрешность метода Монте-Карло оценивается как $\varepsilon \approx \frac{1}{\sqrt{N_{MC}}}$. Таким образом, при заданной точности $\varepsilon_{\text{треб}}$ необходимое количество испытаний составит $N_{MC} \approx \frac{1}{\varepsilon_{\text{треб}}^2}$. Исходя из данных выражений и заданного порога точности метода, можно выбрать требуемое количество испытаний. В таблице 2.3 представлены данные о соответствии количества испытаний заданной точности метода Монте-Карло.

Таблица 2.3 – Соответствие количества испытаний от заданной точности метода Монте-Карло

Точность, $\varepsilon_{\text{треб}}$	0,001	0,002	0,005	0,01	0,015	0,02	0,05
Количество испытаний, N_{MC}	1000000	250000	40000	10000	4444,(4)	2500	400

Поскольку предложенная оценка (2.5) является относительной частотой, то она обладает такими статистическими свойствами как несмещенность, состоятельность (на основе закона больших чисел) и эффективность [65], при этом она является асимптотически нормальной согласно теореме Муара-Лапласа.

Полученные в (2.8) оценки вероятности нахождения МАУ в помещениях того или иного уровня защищенности могут быть использованы для принятия решения системой управления безопасностью МАУ о том, в помещении какого уровня защищенности находится МАУ. Критерий принятия решения об уровне

защищенности помещения, предлагаемый в диссертационной работе представлен следующим соотношением:

$$\tilde{L}_{Room} = \begin{cases} \text{"КИ"}, \text{при } \dfrac{N(\tilde{L}_{Room} = \text{"КИ"})}{N_{MC}} \geq L_{\text{К}}^{\text{треб}} \\ \text{"ОИ"}, \text{при } \dfrac{N(\tilde{L}_{Room} = \text{"КИ"})}{N_{MC}} < L_{\text{К}}^{\text{треб}} \end{cases}, \quad (2.9)$$

где пороговое значение для критерия $L_{\text{К}}^{\text{треб}}$ определяются таким образом, чтобы выполнялось требование заказчика по количеству ошибок 2-го рода:

$$P_{\beta}\left(\tilde{L}_{Room} > L_{Room}\right) \leq P_{\beta}^{\text{доп}}. \quad (2.10)$$

Важной задачей системы управления безопасностью МАУ является обеспечение конфиденциальности информации. Основываясь на этом, пороговое значение $L_{\text{К}}^{\text{треб}}$ должно выбираться таким образом, чтобы конфиденциальность информации была обеспечена. Критичным показателем достоверности определения местонахождения МАУ в специальных помещениях ЗКС является величина ошибки 2-го рода. Ниже, в таблице 2.4 даны пояснения, характеризующие влияние ошибки классификации местоположения МАУ на обеспечение конфиденциальности информации.

Таблица 2.4 – Влияние ошибки классификации местоположения МАУ на конфиденциальность информации

Тип ошибки	Ошибка 1-го рода	Ошибка 2-го рода
Принятое решение	Конфигурация МАУ **блокирует** функциональные **возможности МАУ**, **которые** в данном местоположении МАУ **разрешены**	Конфигурация МАУ **оставляет не заблокированными** функциональные **возможности МАУ**, **которые должны быть отключены** в данном местоположении
Последствия	1. Конфиденциальность информации не нарушена 2. Нарушена доступность услуг	1. Конфиденциальность информации нарушена

Таким образом, значение критерия (2.9) и требований (2.10) позволяют регулировать уровни ошибок 1-го и 2-го рода при принятии решения о местонахождении МАУ в специальных помещениях ЗКС, при этом ошибки 2-го рода являются критическими, поскольку нарушают конфиденциальность информации, в то

время как ошибки 1-го рода приводят только к нарушению доступности некоторых услуг, предоставляемых пользователю МАУ. Графически зона ошибок 1-го, 2-го рода представлена на рисунке 2.7.

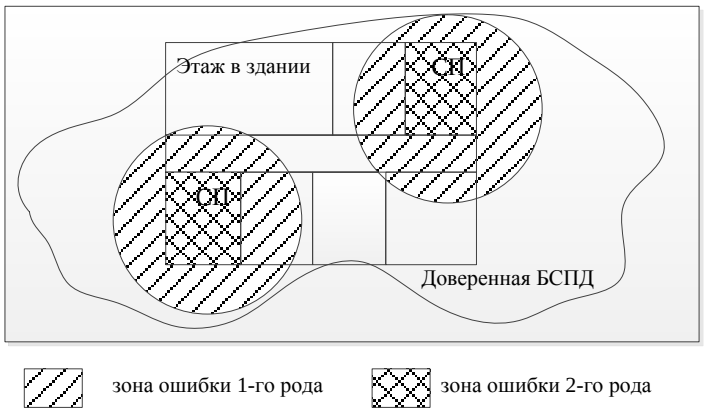


Рисунок 2.7 – Графическое представление ошибок 1-го, 2-го рода при определении местонахождения МАУ в специальных помещениях (СП)

В зависимости от выбранной технологии определения местоположения МАУ и значения порога принятия решения будут отличаться и зоны ошибок 1-го и 2-го рода.

2.3.2. Разработка имитационной модели системы определения местоположения, позволяющей оценить вероятность местонахождения мобильного абонентского устройства в специальном помещении

Результаты разработки имитационной модели изложены в работах [39, 40, 51]. В качестве *объекта моделирования* выбран процесс определения местоположения МАУ, включающий в себя:

– моделирование движения пользователей МАУ по территории здания, в котором развернуты корпоративные сети с разным уровнем защищенности;

– моделирование измерений уровней сигнала БСПД МАУ точками доступа;

– аналитическое вычисление вероятности нахождения МАУ в специальных помещениях.

Основными задачами (границами) имитационного моделирования являются:

– обоснование алгоритмической разрешимости задачи повышения достоверности определения местонахождения МАУ в специальных помещении за счет применения метода статистических испытаний (метода Монте-Карло);

– обоснование оптимальных параметров алгоритмов определения местоположения и вычисления вероятности нахождения МАУ в специальном помещении.

Имитационное моделирование осуществлялось с учетом следующих ограничений:

– БСПД, состоящая из доверенных точек доступа, охватывает все помещения, в которых необходимо предоставлять услуги мобильным пользователям;

– технические характеристики МАУ и точек доступа БСПД известны и стабильны;

– в качестве основы для технологии определения местоположения используется БСПД на базе стандарта 802.11 и один из следующих методов: метод трилатерации (триангуляции), метод k-ближайших соседей, метод, основанный на использовании байесовского подхода;

– влияние параметров, характеризующих особенности строения, в том числе, средние размеры помещений, наличие холлов и коридоров, толщина стен, этажность на распространение радиосигнала учитывается при обучении системы и формирования ряда распределения ошибок определения местоположения МАУ;

– параметры радиосигнала (вид модуляции, полоса частот, манипуляционная скорость и др.) не оказывают существенного влияния на измерение уровня сигнала МАУ, используемое в качестве исходных данных;

– влияние быстрых замираний вследствие многолучевости распространения радиоволн в помещениях в случае выбора технологии трилатерации учитывается за счет применением соответствующей модели распространения радиоволн по аналогии с условиями городской инфраструктуры для плотной застройки;

– регулировка мощности МАУ со стороны базовых станций в зоне доступа БСПД не осуществляется.

Основным критерием эффективности для сравнения технических решений по определению местоположения МАУ являются: *достоверность и своевременность определения местонахождения МАУ* в специальном помещении.

В качестве среды имитационного моделирования было использовано программное обеспечение AnyLogic [31] версии 6.4.1. Реализация предложенной модели выполнена с помощью библиотек Enterprise Library, Pedestrian Library и Rail Yard Library. Функционально разработанное приложение для имитационного моделирования в среде AnyLogic состоит из следующих компонентов:

1. Модуль формирования траектории движения пользователя МАУ.

2. Модуль формирования запросов на доступ к услугам ЗКС.

3. Модуль измерения уровня сигнала МАУ.

4. Модули определения местоположения на базе методов трилатерации, k-ближайших соседей и байесовского подхода.

5. Модуль вычисления вероятности нахождения МАУ в специальном помещении на основе метода Монте-Карло и оценивания ошибок классификации.

6. Подсистема анализа статистических характеристик исследуемых случайных процессов и случайных величин и визуализации результатов моделирования.

Таким образом, замысел имитационного моделирования заключается в моделировании движения пользователей МАУ, в процессе которого осуществляются измерения уровня сигнала МАУ точками доступа и их дальнейшая аналитическая обработка с целью вычисления вероятности нахождения МАУ в специальных помещениях и оценивания ошибок классификации.

В основе функционирования модулей формирования траектории движения пользователя МАУ и формирования запросов на доступ к услугам лежит собранная статистика использования МАУ с помощью разработанного приложения [76]. Фрагмент статистики представлен на рисунке 2.8. В ее состав входит информация об услугах, времени и месте использования услуг, идентификационные данные МАУ.

```
%%event=inc_sms:900;time=03.04.2014       18:27:17       GMT+12:00
;latitude=0.0;longitude=0.0;network_type=GSM;base_station_id=321
466;iface_name=lo,iface_mac=null,ip_addr=::1%1,ip_addr=127.0.0.1
,ip_addr=10.223.88.183,iface_name=rmnet1,iface_mac=null;
%%event=finish_call;time=04.04.2014       07:23:58       GMT+12:00
;latitude=0.0;longitude=0.0;network_type=GSM;base_station_id=321
187;iface_name=lo,iface_mac=null,ip_addr=::1%1,ip_addr=127.0.0.1
,ip_addr=10.223.106.125,iface_name=rmnet1,iface_mac=null;
```

Рисунок 2.8 – Фрагмент статистики использования мобильного устройства

Последовательность точек траектории движения, как и последовательность запросов, реализованы в виде цепи Маркова, формируемой за счет встроенного в среду AnyLogic генератора случайных чисел с равномерным законом распределения и сформированных на основе эмпирических данных матриц переходных вероятностей. Модули формирования траектории движения пользователя МАУ и формирования запросов на доступ к услугам ЗКС реализованы в приложении [77].

В качестве карты расположения помещений использовалась схема, представленная на рисунке 2.9.

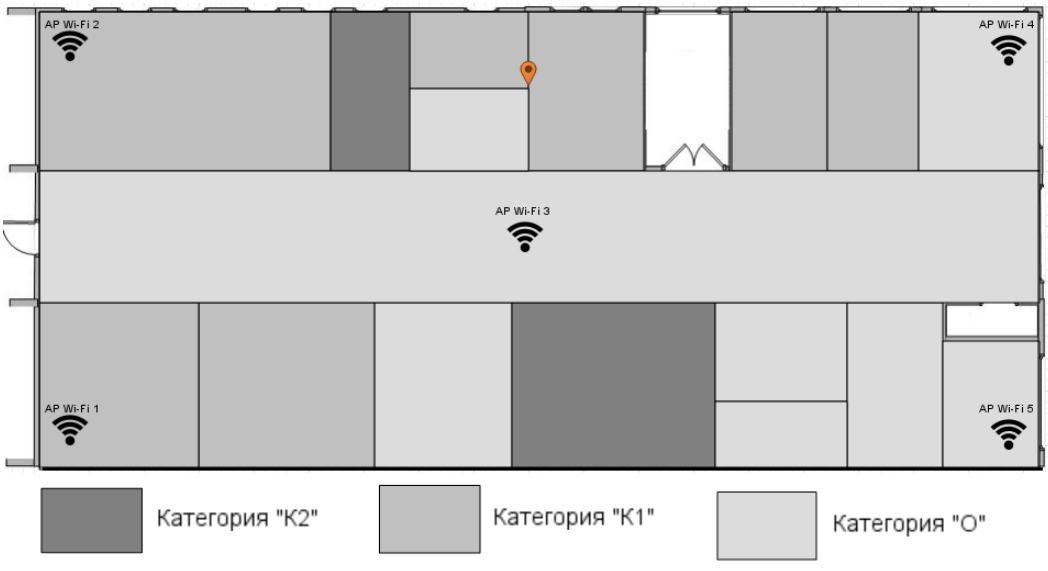


Рисунок 2.9 – Схема помещений для проведения экспериментов

Помещения разделены по уровням защищенности. Карта помещений в имитационной модели реализована в виде структуры, описываемой выражением (1.1).

Для реализации имитационного моделирования распространения радиосигнала был проведен эксперимент в целях исследования колебаний уровня сигнала в точке приема от нескольких источников. Целью данного эксперимента являлось определение наиболее оптимального закона формирования уровня сигнала в имитационной модели.

В эксперименте было использовано следующее оборудование:

1. Ноутбук с техническими характеристиками: процессор: Core i5 2300 МГц; Установленная память (ОЗУ): 4,00 ГБ; Тип системы: 64-разрядная ОС; ОС: Windows 7 Профессиональная SP 1.

2. USB-адаптеры 3Com OfficeConnect Wireless 54 Mbps 11g Compact.

3. Три точки доступа на базе трех ПЭВМ с техническими характеристиками: процессор: Dual 3.20 GHz, IntelCore i5-3470; установленная память (ОЗУ): 8,00 ГБ; тип системы: 64-разрядная ОС; ОС: Windows 7 Профессиональная SP 1.

Схема расположения помещений с точками доступа и измерителем колебаний уровня сигнала представлена на рисунке 2.10.

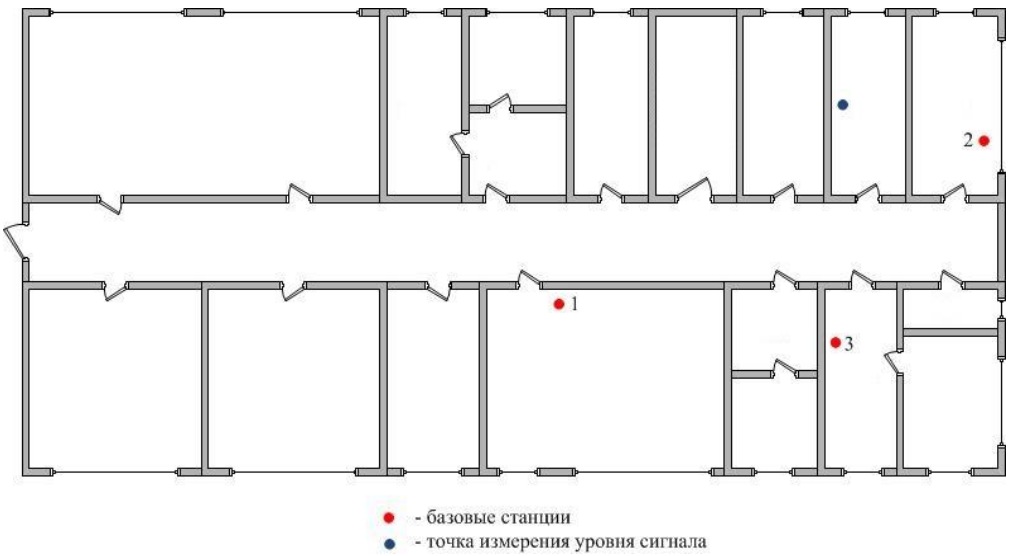
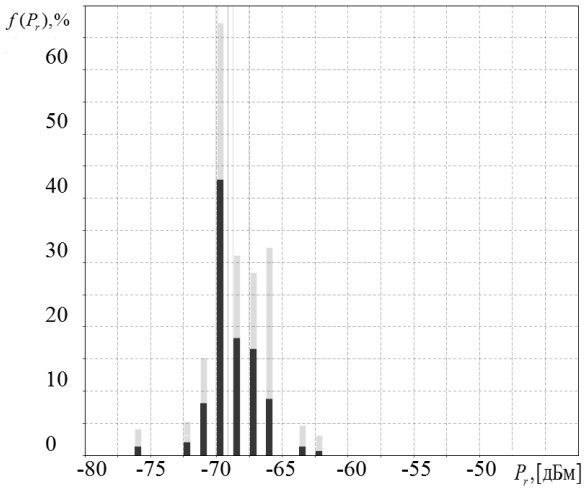


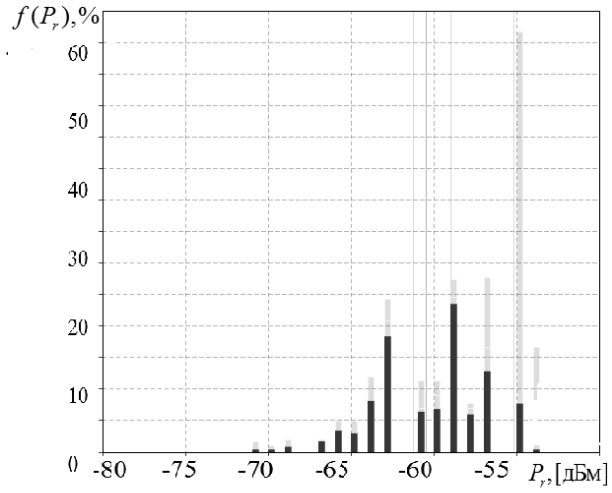
Рисунок 2.10 – Схема расположения помещений с точками доступа и измерителем колебаний уровня сигнала

В эксперименте использовались широковещательные пакеты, а также периодически производилась запись уровня сигнала базовых станций в точке приема. Измерение уровня мощность сигнала осуществлялась при четырех разных ориентациях беспроводного адаптера, выполняющего роль точки приема. Подробные численные результаты измерений представлены в таблице Б.1 приложения Б.

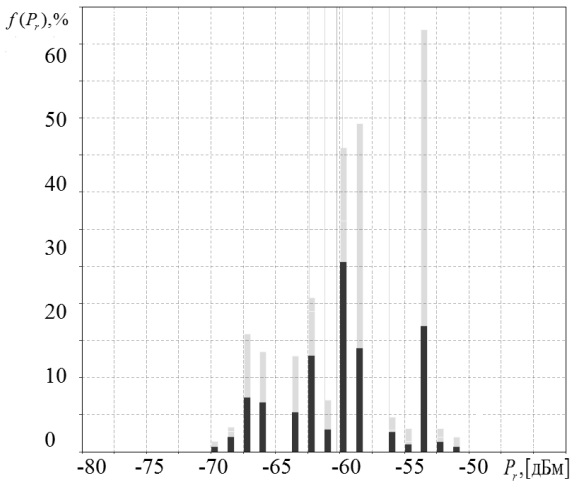
На рисунках 2.11 а-в представлены плотности распределения уровней мощности сигнала беспроводных точек доступа в точке приема.



а)



б)



в)

Рисунок 2.11 – Плотности распределения уровней мощности сигнала беспроводных точек доступа в точке приема: а) точка доступа № 1, б) точка доступа № 2, в) точка доступа № 3

Результаты измерений в виде плотности распределения уровней мощности сигнала беспроводных точек доступа для разных положений точки приема представлены на рисунке Б.1 приложения Б.

Статистические параметры функции распределения вероятностей уровней сигнала беспроводных точек доступа для разных положений точки приема, а также результаты проверки гипотезы о принадлежности выборок нормальному закону распределения в соответствии с критерием χ^2 [67] представлены в таблице 2.5.

Таблица 2.5 – Статистические параметры распределения вероятностей уровней мощности сигнала беспроводных точек доступа для разных положений точки приема

№ точки доступа	Положение	Выб. среднее	Выб. СКО	Доверит. интервал	Мин. знач.	Макс. знач	Уровень значимости α для критерия χ^2 при проверке гипотезы о принадлежности выборки к нормальному закону распределения
1	1	-71,914	0,801	0,21	-74	-70	$0,1 < \alpha < 0,2$
	2	-70,015	1,566	0,388	-73	-66	$0,0005 < \alpha < 0,001$
	3	-72,03	1,46	0,291	-77	-67	$\alpha < 0,0005$
	4	-70,986	0,972	0,225	-73	-69	$0,01 < \alpha < 0,025$
	1-4	-71,304	1,496	0,17	-77	-66	$\alpha < 0,0005$
2	1	-61,194	2,745	0,696	-71	-57	$0,01 < \alpha < 0,025$
	2	-58,969	3,216	0,796	-67	-55	$0,2 < \alpha < 0,3$
	3	-67,218	3,227	0,629	-70	-55	$\alpha > 0,5$
	4	-55,167	0,983	0,982	-57	-54	$\alpha > 0,5$
	1-4	-60,432	3,322	0,426	-71	-54	$\alpha < 0,0005$
3	1	-63,836	1,625	0,415	-71	-61	$\alpha < 0,0005$
	2	-60,923	2,938	0,727	-70	-58	$0,001 < \alpha < 0,005$
	3	-65,921	3,236	0,631	-72	-57	$0,001 < \alpha < 0,005$
	4	-64,946	3,487	0,807	-72	-59	$\alpha < 0,0005$
	1-4	-64,179	3,508	0,396	-72	-57	$0,05 < \alpha < 0,1$

Как видно из таблицы 2.5 уровень значимости α при проверке с помощью критерия типа X^2 гипотезы о принадлежности выборки нормальному закону не превышает значения 0,1.

Проведенный эксперимент также показал, что ошибка измерения уровня сигнала в среднем составляет $2{,}188$ дБм со среднеквадратическим отклонением (СКО), равным $1{,}039$ дБм при доверительном интервале для выборочного среднего – $0{,}654$ дБм. Таким образом, результаты эксперимента позволяют использовать в разработанной имитационной модели нормальный закон распределения ошибки измерения мощности принимаемого сигнала со следующими параметрами: $\mathrm{M}\,e(t) = 0$, $\sigma\, e(t) = 3$ дБм и модель измерений в виде:

$$\tilde{P}(t) = P_r(t) + e(t) = P_t \cdot \frac{\lambda^2}{\left(4\pi R^2(t)\right)} + \frac{1}{3[\text{дБм}]\sqrt{2\pi}} e^{-\frac{x^2}{18[\text{дБм}]}}, \qquad (2.11)$$

где $P_r(t)$ – уровень сигнала, вычисленный в соответствие с выражением (А.4); x – случайная величина, распределенная по равномерному закону в диапазоне $[0,1]$; $R(t)$ – известное расстояние от пользователя МАУ до точки измерения (точки доступа), определяемое траекторией движения пользователя.

Данная модель измерений уровня принимаемого точками доступа сигнала реализована в модуле измерения уровня сигнала беспроводной сети разработанной имитационной модели.

В имитационной модели изменяемыми параметрами являются:

P_t – уровень мощности передатчика [Вт];

f – частота передатчика [Гц];

Rooms – структура, содержащая сведения о координатах помещения и требованиях по уровню из защищенности;

$\mathrm{M}\,e(t)$ – математическое ожидание ошибки измерения уровня принимаемого сигнала;

$\sigma\, e(t)$ – среднеквадратическое отклонение ошибки измерения уровня принимаемого сигнала;

номера используемых для измерений точек доступа;

координаты (расположение) используемых для измерений точек доступа;

(dx_kNN, dy_kNN) – параметры сетки карты измерений сигналов для метода k-ближайших соседей, где dx_kNN – шаг сетки по горизонтали и dy_kNN – шаг сетки по вертикали;

k_kNN – число "соседей" сигнального пространства, используемое в методе k-ближайших соседей;

M – количество измерений в каждой точке сигнального пространства для метода, основанного на байесовском подходе;

(dx_HMM, dy_HMM) – параметры сетки карты измерений сигналов для метода, основанного на байесовском подходе, где dx_HMM – шаг сетки по горизонтали и dy_HMM – шаг сетки по вертикали;

k_HMM – число "соседей" сигнального пространства, используемое в методе, основанном на байесовском подходе;

N_MC – количество испытаний для метода Монте-Карло;

закон распределения случайной величины, используемый для осуществления испытаний в методе Монте-Карло (равномерные или эмпирический);

R_e – параметр, определяющий величину, задающую радиус зоны ошибки измерения местоположения с центром в точке с вычисленным местоположением пользователя МАУ.

μ – порог срабатывания для классификации местоположения МАУ.

Моделирующий алгоритм имитационной модели представлен в приложении В.

В качестве *критериев эффективности* разрабатываемой модели используются оценки ошибок классификации местоположения, выражаемые через численные значения вероятностей ошибок 1-го и 2-го рода. Принятие решения о достоверности классификации местоположения осуществляется за счет сравнения те-

кущего моделируемого местоположения и вычисленного за счет применения оцениваемой аналитической модели.

2.3.3. Оценка качества имитационной модели системы определения местоположения мобильного абонентского устройства

Оценка качества и затрат выделенных ресурсов на разработку модели проводилась на основе [86]. При имитационном моделировании на достоверность результатов влияет целый ряд дополнительных факторов, основными из которых являются:

– моделирование случайных факторов, основанное на использовании датчиков случайных чисел, которые могут вносить "искажения" в поведение модели;

– наличие нестационарного режима работы модели;

– использование нескольких разнотипных математических методов в рамках одной модели;

– зависимость результатов моделирования от плана эксперимента;

– необходимость синхронизации работы отдельных компонентов модели;

Пригодность имитационной модели для решения задач исследования характеризуется тем, в какой степени она обладает целевыми свойствами. Основными из них являются: *адекватность*, *устойчивость*, *чувствительность*.

Под *адекватностью* понимают степень соответствия модели тому реальному явлению или объекту, для описания которого она строится. Адекватность модели определяется степенью ее соответствия не столько реальному объекту, сколько целям исследования. Процедура оценки адекватности модели проводилась на основе методов математической статистики за счет сравнения измерений на реальной системе и результатов экспериментов на модели.

Устойчивость модели как способность сохранять адекватность при исследовании эффективности системы на всем возможном диапазоне рабочей нагрузки, а также при внесении изменений в конфигурацию системы. Устойчивость результатов моделирования оценена методами математической статистики.

Чувствительность модели заключается в оценивании реакции модели к изменению параметров нагрузки и внутренних параметров самой системы.

Проверка адекватности модели осуществлялась по параметру – выборочное среднее значения ошибки определения местоположения $\bar{e}_L$, а также выборочное среднеквадратичное отклонение ошибки определения местоположения $\bar{\sigma}_L$.

Проверка адекватности модели по параметру $\bar{e}_L$ (среднее значение ошибки определения местоположения) представлена в таблице 2.6, по параметру $\bar{\sigma}_L$ (также выборочное среднеквадратичное отклонение ошибки определения местоположения) – в таблице 2.7.

Таблица 2.6 – Проверка адекватности модели по параметру $\bar{e}_L$

Обозначение отклика	$\bar{e}_L$	$\bar{e}_L^*$
Количество составляющих выборок	180	177
Среднее значение, $\overline{Y}$	2,481	2,269
Оценка дисперсии отклика, D_n	2,758	2,459
Дисперсия разности, D_{pn}	2,634	
Значение *t*-статистики, t_n	0,62	
Количество степеней свободы	201	
Критическое значение *t* – статистики $t_{кр}$	1,653	

Таблица 2.7 – Проверка адекватности модели по параметру $\bar{\sigma}_L$

Обозначение отклика	$\bar{\sigma}_L$	$\bar{\sigma}_L^*$
Количество составляющих выборок	140	140
Среднее значение, $\overline{Y}$	1,661	1,763
Оценка дисперсии отклика, D_n	0,168	0,130
Дисперсия разности, D_{pn}	0,151	
Значение *t*-статистики, t_n	0,62	
Количество степеней свободы	288	
Критическое значение *t* – статистики $t_{кр}$	1,65	

Число степеней свободы (t-статистики) для выбранных параметров находиться в пределах от 200 до 300. Для уровня значимости $\alpha = 0,05$ при таком коли-

честве степеней свободы критическое значение t-статистики $t_{кр} \approx 1,653$. Сравнивая значения t-статистики в таблицах 2.6-2.7 с $t_{кр}$, видим, что можно принять гипотезу о близости среднего значения откликов модели и реальной системы ($t_{модели} \le t_{кр}$). Следовательно, **имитационная модель адекватна** исследуемой системе.

В начальный момент времени работы модели протекающие в ней процессы не будут стацинарными. Через некоторый интервал времени переходный процесс закончится, и модель перейдет в стационарный режим работы, вероятностные характеристики которого не будут зависеть от времени моделирования [6]. Так как на практике ограничиваются отсечением начального периода, равного 3-4 кратному времени прохождения модели самыми "медленными заявками", в качестве *длительности переходного периода* примем $T_0 = 2496$ модельных единиц или $N = 9$ прогонов модели.

Определение необходимого *числа реализаций* n обеспечивает заданную точность и надежность результата. Для определения числа реализаций воспользуемся формулой [6]:

$$n = \frac{t_\alpha^2 p(1-p)}{\varepsilon^2}. \qquad (2.12)$$

Для нахождения вероятности p необходима предварительная оценка на малом числе испытаний. Так как проведение предварительной оценки не предусматривается, то воспользуемся наихудшим случаем: $p = 0,5$. Для величины доверительного интервала $\varepsilon = 10^{-2}$ и априорной вероятности наступления события $\alpha = 0,99$ значение t-критерия Стъюдента равно $t_\alpha = 2,53$, а число реализаций:

$$n = \frac{2,53^2 - 0,5(1-0,5)}{10^{-4}} = 16003. \qquad (2.13)$$

Для определения наиболее влияющих входных параметров модели необходимо исследовать *чувствительность* имитационной модели. Проверку чувствительности модели к изменению исходных данных осуществим на примере. Диапазоны изменения входных параметров представлены в таблице 2.8, где k – число

наиболее вероятных состояний скрытой марковской модели, учитываемых при вычислении местоположения МАУ, а M – число измерений в точке, производимых для сбора статистики измерения уровня сигнала МАУ.

Расчет количества опытов для исследования чувствительности имитационной модели показал, что необходимо провести не менее 10 опытов. Значения входных параметров приведены в таблице 2.9.

Таблица 2.8 – Диапазоны изменения входных параметров

Входные параметры	Минимальное значение параметра	Максимальное значение параметра	Приращение параметра, %
k	1	10	100
M	10	180	100

Таблица 2.9 – Значения входных параметров для оценки чувствительности

№ эксп.	1	2	3	4	5	6	7	8	9	10
k	1	2	3	4	5	6	7	8	9	10
M	10	20	30	40	50	60	70	80	90	100

Результаты исследования чувствительности имитационной модели приведены в таблице 2.10.

Таблица 2.10 – Результаты исследования чувствительности имитационной модели

Входной параметр	Выходной параметр $\hat{e}_L$			Соотношение с приращением входного параметра
	min	*max*	$\delta\,\hat{e}_L$, %	
k	2,445	3,86	44,8	0,448
M	2,481	3,131	23,1	0,231

Приращения входных параметров и изменения выходного параметра вычисляются по формуле

$$\delta X = \frac{2 \cdot (\max X - \min X)}{\max X + \min X} \cdot 100\%. \qquad (2.14)$$

Проверка чувствительности подтвердила факт того, что "отклики" (выходные результаты) модели соответствуют критериям чувствительности модели.

В результате оценки качества модели можно сделать вывод, что **модель достаточно чувствительна** к входным результатам.

Устойчивость результатов моделирования может быть также оценена методами математической статистики. Для проверки гипотезы об устойчивости результатов может быть использован критерий Уилкоксона, который служит для проверки того, относятся ли две выборки к одной и той же генеральной совокупности (т.е. обладают ли они одним и тем же статистическим признаком). В качестве выборок для оценки устойчивости результатов взяты показатели ошибок определения местоположения МАУ, представленные в таблице 2.11.

Таблица 2.11 – Выборки результатов моделирования оценки ошибки определения местоположения МАУ

№ эксп.	1	2	3	4	5	6	7	8	9	10
Выборка № 1	1,783	4,801	3,195	1,419	1,418	0,763	2,473	2,699	0,463	1,067
Выборка № 2	1,008	0,769	0,728	0,437	1,549	1,099	1,454	2,080	3,195	5,623

Для уровня значимости $\alpha = 0{,}05$ значение статистики для принятия гипотезы об однородности выборок должна удовлетворять неравенству $|T| \le 1{,}96$. Для представленных выборок статистика по критерию Уилкоксона равна $T = 0{,}82$. Соответственно, выборки с уровнем значимости $\alpha = 0{,}05$ можно считать однородными, что свидетельствует о том, что результаты моделирования **устойчивы**.

2.3.4. Результаты моделирования определения местоположения мобильного абонентского устройства

Результаты моделирования получены для схемы помещений, представленной на рисунке 2.9. В качестве исходных данных взяты следующие:

1) Технические характеристики МАУ:

– мощность передатчика 0,07943282347242815 Вт;

– частота передатчика 2,4 ГГц;

– ошибка измерения уровня мощности МАУ моделируется нормальных законом распределения вероятностей со следующими статистическими параметрами: $M\left[P_r\right]=0$ Дбм, $\sigma\left[P_r\right]=3$ Дбм.

2) расположение, уровни защищенности и параметры помещений определяются схемой помещений, представленной на рисунке 2.9, при размерах здания $16{,}8\text{ м}\times 38{,}0\text{ м}$.

3) точки доступа беспроводной сети в системе координат исследуемого здания расположены следующим образом: $AP_1=\left(3{,}6\text{ м};19{,}2\text{ м}\right)$, $AP_2=\left(3{,}6\text{ м};5{,}2\text{ м}\right)$, $AP_3=\left(20{,}0\text{ м};12{,}0\text{ м}\right)$, $AP_4=\left(37{,}6\text{ м};5{,}2\text{ м}\right)$, $AP_5=\left(37{,}6\text{ м};19{,}2\text{ м}\right)$.

Расчет местоположения МАУ осуществлялся в соответствие с выражениями для метода трилатерации – (А.3)-(А.19), для метода k-ближайших соседей – (А.20)-(А.25), для метода на основе байесовского подхода – (А.26)-(А.31).

Расчет вероятности местонахождения МАУ в специальном помещении осуществлялся в соответствие с выражениями (2.3)-(2.9).

Ограничения и допущения, в рамках которых осуществлялось имитационное моделирование, представлены на странице 57.

Результаты моделирования получены с помощью разработанных программ для ЭВМ [76, 79].

На рисунке 2.12 представлена зависимость ошибок 1-го и 2-го рода при вычислении вероятности местонахождения МАУ в специальном помещении по полученному местоположению пользователя МАУ, рассчитанному на основе байесовского подхода, в процессе имитационного моделирования в зависимости от времени.

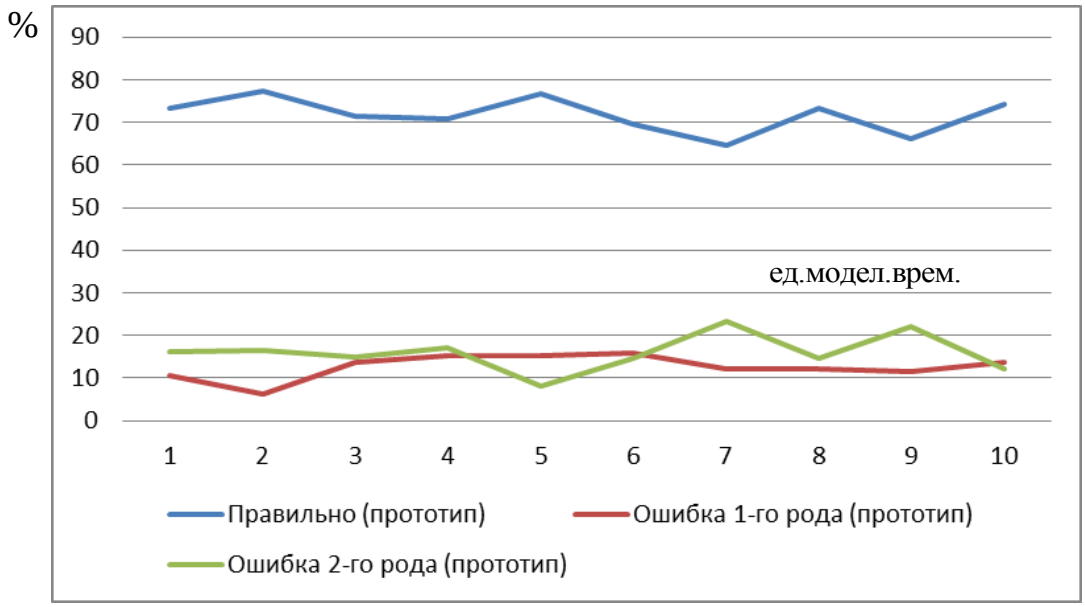


Рисунок 2.12 – График зависимости ошибок 1-го и 2-го рода при вычислении вероятности местонахождения МАУ в специальном помещении

В таблице 2.12 представлены численные результаты эксперимента.

Таблица 2.12 – Зависимость ошибок 1-го и 2-го рода при вычислении вероятности местонахождения МАУ в специальном помещении по полученному местоположению пользователя МАУ

Ед. модел. врем.	1	2	3	4	5	6	7	8	9	10
Правильно	73,25	77,277	71,335	70,922	76,661	69,572	64,644	73,209	66,29	74,209
Ошибка 1-го рода	10,664	6,24	13,657	15,09	15,107	15,849	12,006	12,225	11,599	13,579
Ошибка 2-го рода	16,085	16,481	15,006	16,987	8,23	14,577	23,348	14,565	22,11	12,21

Из результатов экспериментов видно, что в исследуемом прототипе без использования метода Монте-Карло ошибки 1-го и 2-го рода являются случайными величинами – реализациями одного и того же стационарного случайного процесса со средними значениями: $\alpha = 12,6016$ и $\beta = 15,9599$ с числом правильных принятий решений в среднем в $71,7369$ процентах случаев.

На рисунке 2.13 представлена зависимость ошибок 1-го и 2-го рода при вычислении вероятности местонахождения МАУ в специальном помещении по полученному местоположению МАУ от числа испытаний M в методе Монте-Карло.

При этом порог принятия решения об уровне защищенности помещения в соответствие с выражениями (2.7), (2.8) и (2.9) был задан на уровне $L_{К1}^{треб} = 0,05; L_{К2}^{треб} = 0,05$.

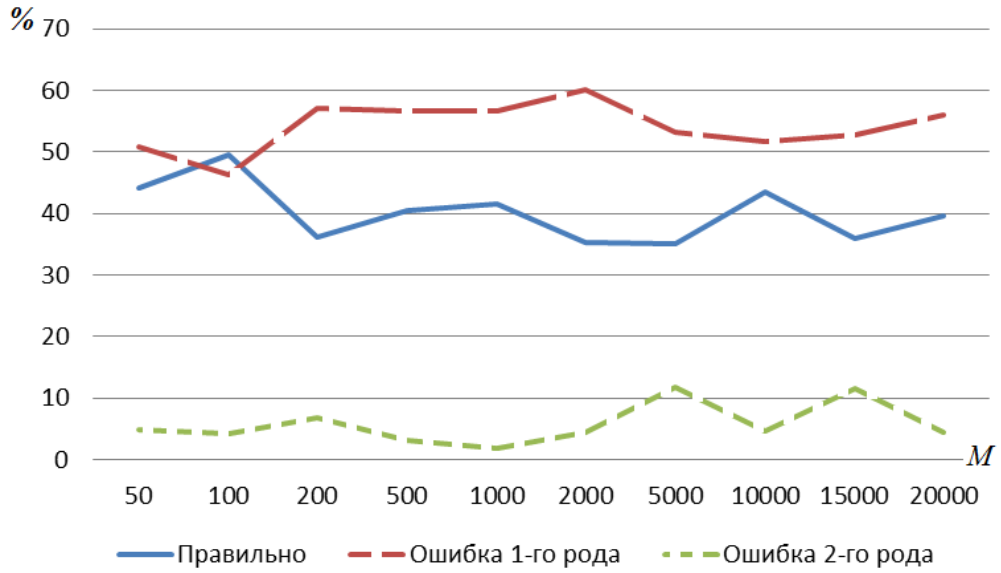


Рисунок 2.13 – График зависимости ошибок 1-го и 2-го рода при вычислении вероятности местонахождения МАУ в специальном помещении от числа испытаний M в методе Монте-Карло

В таблице 2.13 представлены численные результаты данных эксперимента.

Таблица 2.13 – Зависимость ошибок 1-го и 2-го рода при вычислении вероятности местонахождения МАУ в специальном помещении от числа испытаний M в методе Монте-Карло

M	50	100	200	500	1000	2000	5000	10000	15000	20000
Правильно	44,226	49,482	36,115	40,38	41,461	35,402	35,15	43,586	35,861	39,631
Ошибка 1-го рода	50,891	46,263	57,045	56,554	56,598	60,188	53,126	51,652	52,861	55,999
Ошибка 2-го рода	4,882	4,254	6,838	3,064	1,94	4,409	11,723	4,761	11,599	4,368

Из результатов эксперимента с использованием метода Монте-Карло можно сделать несколько выводов:

1) величина ошибки 2-го рода по сравнению прототипом ниже в среднем в 5 раз;

2) оптимальное количество испытаний для метода Монте-Карло составляет $M = 1000$.

При использовании метода Монте-Карло для вычисления вероятности местонахождения МАУ в специальном помещении в качестве закона распределения случайной величины, характеризующей ошибку определения местоположения, использовался равномерный закон распределения и эмпирический. Эмпирический закон распределения определялся гистограммой частот плотности распределения вероятностей ошибки определения местоположения для выбранного метода.

В таблице 2.14 представлены результаты исследования эффективности метода Монте-Карло при классификации местоположения МАУ методом трилатерации для разных законов распределения вероятностей случайной величины.

Таблица 2.14 – Исследование эффективности метода Монте-Карло при вычислении вероятности местонахождения МАУ в специальном помещении на основе метода трилатерации в зависимости от порога принятия решения $L^{\text{треб}}$.

$L^{\text{треб}}$	Равномерный закон			Эмпирический закон		
	Правильно	α	β	Правильно	α	β
0,0000001	36,152	60,525	3,321	14,314	85,044	0,64
0,000001	39,858	48,425	11,715	14,162	85,264	0,573
0,00001	36,208	57,335	6,456	23,178	76,821	0
0,0001	38,209	56,253	5,537	14,025	85,252	0,722
0,001	38,295	50,727	10,976	17,204	80,943	1,852
0,01	34,635	61,407	3,956	17,403	80,753	1,842
0,02	33,385	64,57	2,044	19,336	78,24	2,422
0,03	39,484	48,107	12,408	20,525	74,756	4,717
0,04	35,593	60,27	4,136	23,053	71,198	5,747
0,05	37,561	56,926	5,512	25,601	71,033	3,365
0,06	36,934	60,137	2,928	26,151	72,217	1,631
0,07	40,6	50,437	8,962	30,201	66,243	3,555
0,08	39,269	51,39	9,339	34,922	62,859	2,217

Окончание таблицы 2.14.

$L^{треб}$	Равномерный закон			Эмпирический закон		
	Правильно	α	β	Правильно	α	β
0,09	37,956	53,359	8,683	36,006	60,802	3,19
0,1	38,117	57,303	4,579	35,296	55,821	8,882
0,11	36,995	53,951	9,052	37,685	52,331	9,983
0,12	40,798	55,212	3,989	40,904	53,515	5,579
0,13	42,216	49,092	8,691	42,503	52,234	5,261
0,14	43,923	49,74	6,336	44,955	48,282	6,761
0,15	45,545	49,141	5,312	47,443	44,008	8,547
0,16	41,708	45,768	12,523	48,852	43,381	7,766
0,17	46,805	41,002	12,192	51,563	41,204	7,232
0,18	47,332	42,312	10,354	47,325	36,603	16,07
0,19	49,665	43,323	7,01	53,104	36,891	10,003
0,2	57,913	35,743	6,343	53,06	32,945	13,994

На рисунке 2.14 представлен график зависимости ошибок 1-го и 2-го рода от порога принятия решения при использовании метода Монте-Карло для определения вероятности местонахождения МАУ в специальном помещении на основе метода трилатерации.

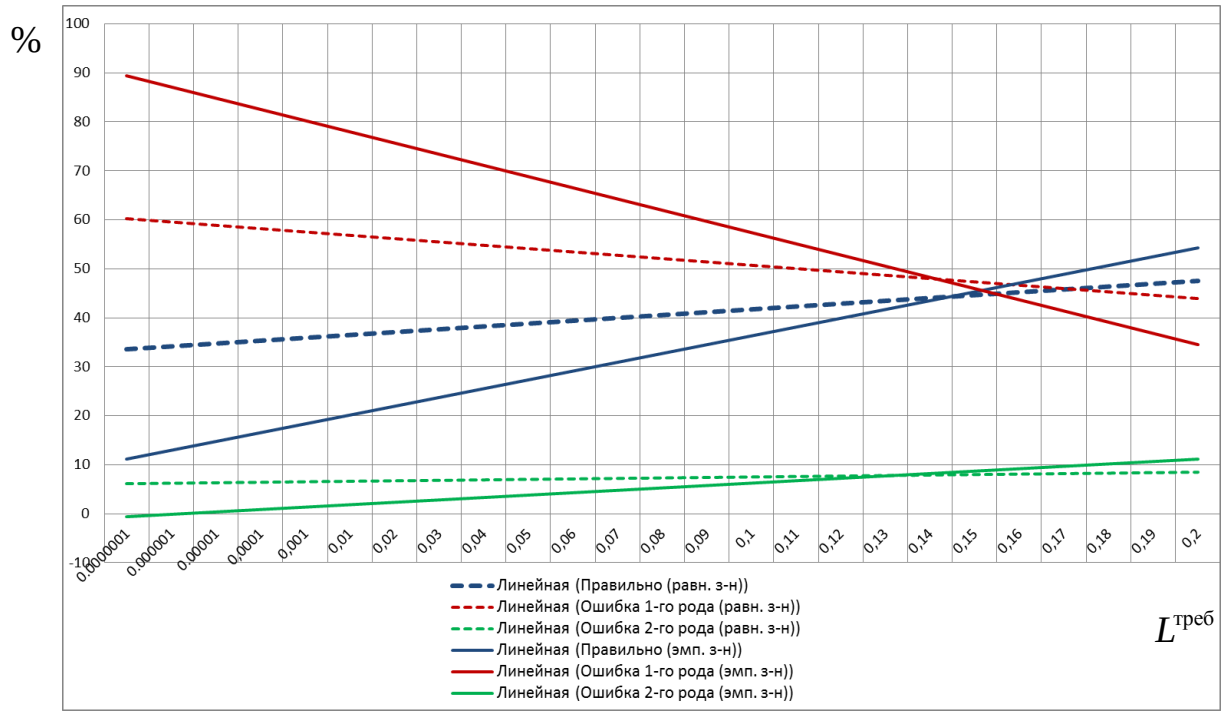


Рисунок 2.14 – График зависимости ошибок 1-го и 2-го рода от порога принятия решения при использовании метода Монте-Карло

Из результатов эксперимента видно, что при использовании эмпирического закона распределения ошибка 2-го рода меньше для $L^{\text{треб}} < 0{,}13$ по сравнению с равномерным. Однако при этом количество правильных решений для равномерного закона выше, чем для эмпирического при условии $L^{\text{треб}} < 0{,}15$.

Результаты аналогичного эксперимента для метода k-ближайших соседей представлены в таблице 2.15 и на рисунке 2.15.

Таблица 2.15 – Исследование эффективности метода Монте-Карло при классификации местоположения МАУ методом k-ближайших соседей в зависимости от порога принятия решения $L^{\text{треб}}$.

$L^{\text{треб}}$	Равномерный закон			Эмпирический закон		
	Правильно	α	β	Правильно	α	β
0,0000001	19,339	79,506	1,153	13,667	85,836	0,496
0,000001	21,859	74,041	4,099	13,232	86,308	0,458
0,00001	20,074	77,563	2,362	0,93	99,069	0
0,0001	19,838	78,456	1,704	13,831	85,653	0,514
0,001	20,165	75,584	4,249	16,559	82,143	1,296
0,01	19,596	78,927	1,476	19,92	77,403	2,675
0,02	17,953	81,382	0,664	22,036	74,949	3,013
0,03	21,364	73,834	4,801	23,955	70,673	5,371
0,04	21,904	76,248	1,846	27,355	65,943	6,701
0,05	22,26	75,302	2,437	32,786	63,153	4,06
0,06	27,321	71,127	1,55	36,279	61,576	2,144
0,07	26,244	69,09	4,664	39,179	56,364	4,455
0,08	30,389	64,118	5,492	46,022	51,044	2,932
0,09	30,994	62,866	6,139	45,492	50,627	3,88
0,1	34,375	62,692	2,931	43,006	47,872	9,12
0,11	31,251	61,987	6,761	44,941	44,004	11,054
0,12	39,263	57,877	2,859	48,101	45,353	6,544
0,13	39,288	55,053	5,658	51,535	41,857	6,607
0,14	45,067	49,818	5,114	51,313	39,92	8,765
0,15	45,459	51,236	3,304	54,031	35,921	10,047
0,16	42,064	46,685	11,25	56,583	34,664	8,751
0,17	46,281	43,852	9,866	56,987	34,252	8,759
0,18	48,712	42,436	8,85	51,965	31,159	16,874
0,19	53,653	40,579	5,766	57,816	31,137	11,045
0,2	59,867	34,924	5,208	57,108	28,341	14,55

Из результатов эксперимента видно, что при использовании эмпирического закона распределения ошибка 2-го рода меньше для $L^{\text{треб}} < 0,03$ по сравнению с равномерным, а количество правильных решений выше при условии $L^{\text{треб}} > 0,03$.

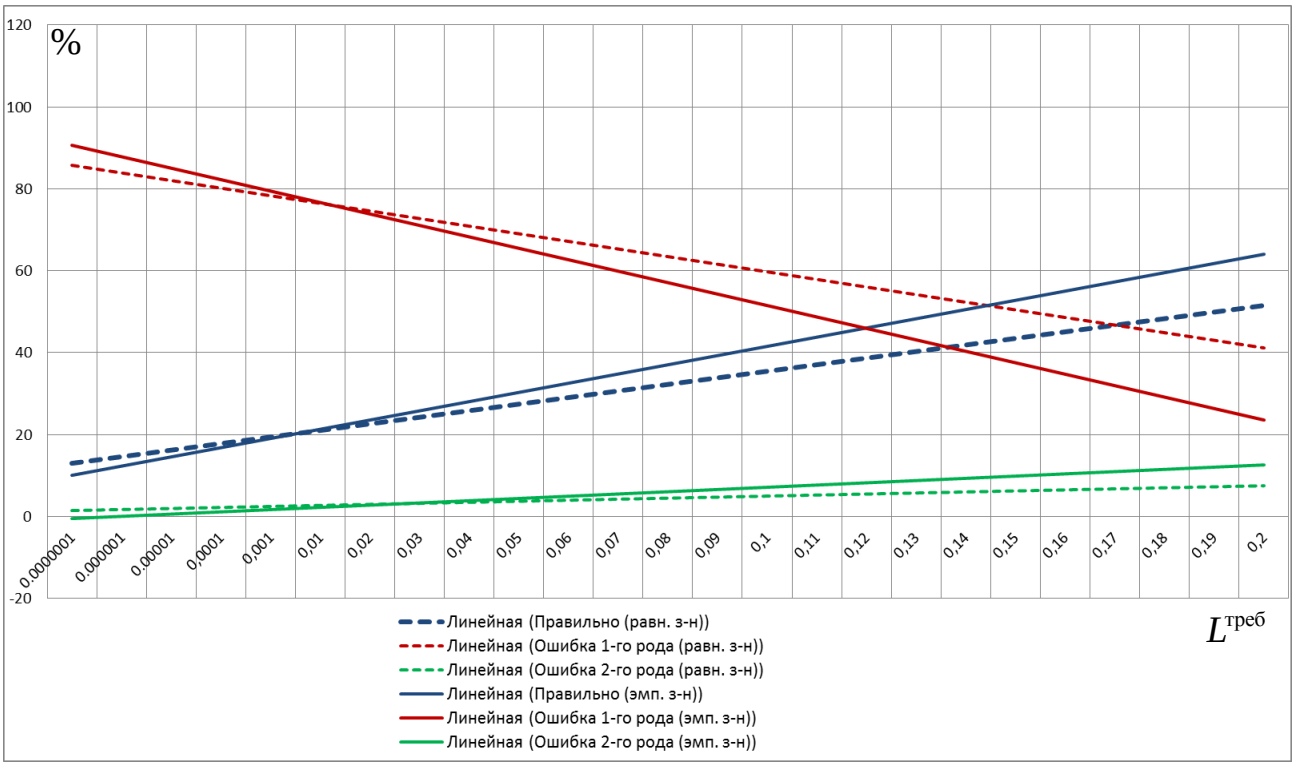


Рисунок 2.15 – График зависимости ошибок 1-го и 2-го рода от порога принятия решения при использовании метода Монте-Карло для принятия решения об уровне защищенности помещения на основе вычисленного методом k-ближайших соседей местоположения МАУ

Результаты аналогичного эксперимента для метода на основе байесовского подхода представлены в таблице 2.16 и рисунке 2.16. Параметры ошибок 1-го и 2-го рода, а также число правильных решений для байесовского подхода выше в случае применения эмпирического закона распределения по сравнению с равномерным для любых значений порога $L^{\text{треб}}$.

Таблица 2.16 – Исследование эффективности метода Монте-Карло при классификации местоположения МАУ на основе байесовского подхода в зависимости от порога принятия решения.

$L^{\text{треб}}$	Равномерный закон			Эмпирический закон		
	Правильно	α	β	Правильно	α	β
0,0000001	16,48	82,816	0,702	18,176	80,204	1,619
0,000001	20,651	77,191	2,157	15,986	82,816	1,193
0,00001	18,417	80,175	1,406	22,115	75,658	2,226
0,0001	17,734	81,273	0,991	2,114	97,84	0,044
0,001	18,977	78,69	2,331	14,096	85,185	0,717
0,01	18,442	80,502	1,055	22,554	75,625	1,82
0,02	17,287	82,143	0,568	26,496	70,312	3,191
0,03	21,488	74,751	3,76	31,977	66,301	1,72
0,04	19,575	78,751	1,672	37,745	58,432	3,822
0,05	20,456	77,467	2,076	42,744	55,38	1,875
0,06	25,507	73,186	1,306	39,596	49,931	10,471
0,07	24,708	71,321	3,97	43,642	51,51	4,847
0,08	29,497	65,462	5,04	45,64	46,598	7,761
0,09	30,932	63,643	5,424	30,277	69,7	0,021
0,1	33,246	64,057	2,695	50,416	39,296	10,287
0,11	30,969	62,654	6,675	57,181	37,895	4,922
0,12	38,832	58,575	2,592	60,205	34,882	4,912
0,13	39,443	55,39	5,166	58,332	36,459	5,207
0,14	45,148	49,996	4,854	58,406	32,301	9,292
0,15	45,97	50,963	3,065	61,099	32,334	6,565
0,16	42,331	46,754	10,913	64,88	27,814	7,304
0,17	47,385	43,209	9,404	62,225	28,026	9,748
0,18	49,548	42,119	8,331	61,861	26,107	12,031
0,19	54,951	39,32	5,728	68,815	25,945	5,238
0,2	60,579	34,567	4,852	67,104	25,201	7,693

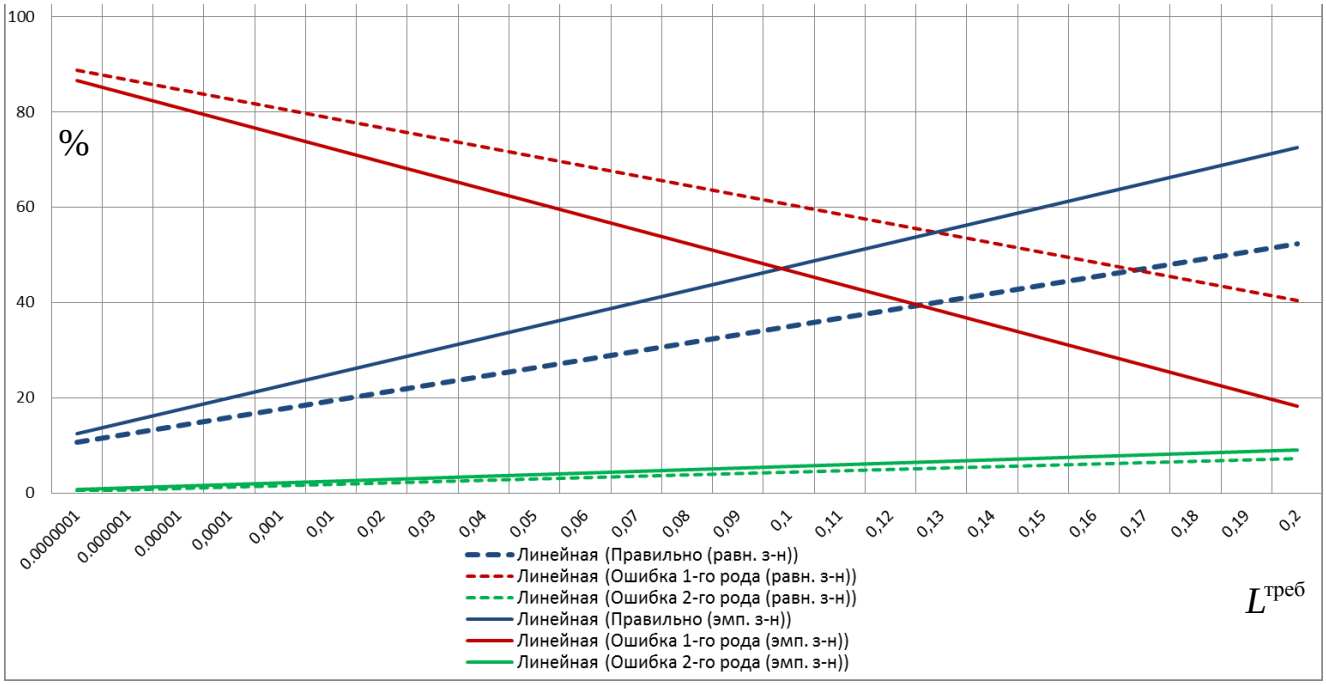
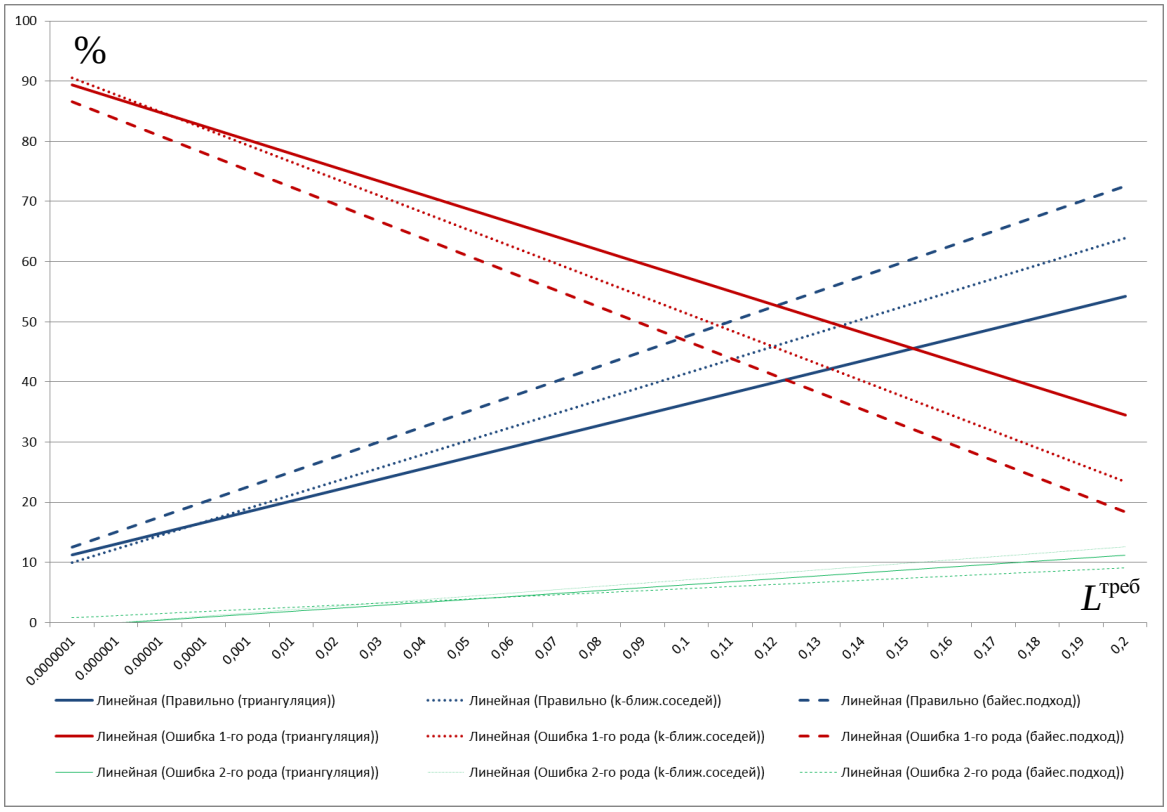


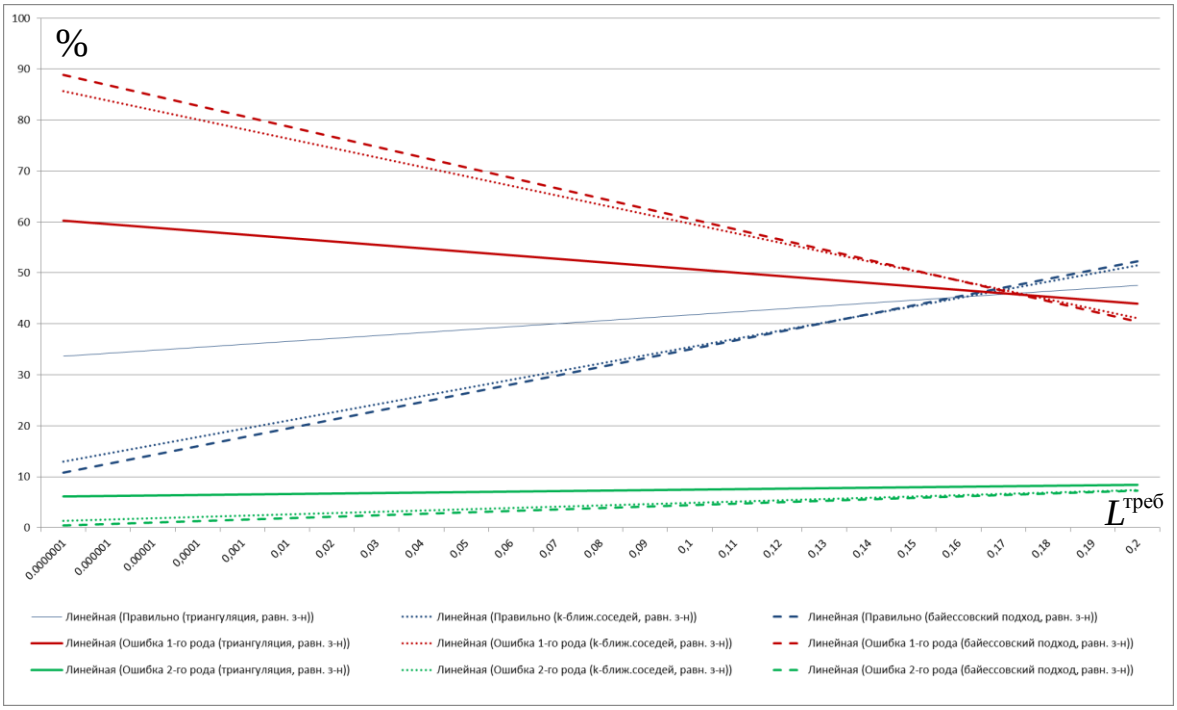
Рисунок 2.16 – График зависимости ошибок 1-го и 2-го рода от порога принятия решения при использовании метода Монте-Карло для определения уровня защищенности помещения на основе байесовского подхода

Сравнительный анализ разных технологий определения местоположения в сочетании с применением метода Монте-Карло для определения вероятности нахождения МАУ в специальном помещении приведен на рисунке 2.17.

На рисунках отчетливо видно, что количество правильных решений об уровне защищенности помещения в случае применения эмпирического закона выше, чем для равномерного, независимо от используемой технологии определения местоположения. То же самое касается и ошибок 2-го рода, показатели по которым ниже для эмпирического закона.



а)



б)

Рисунок 2.17 – Сравнительный анализ использования разных технологий определения местоположения в сочетании с применением метода Монте-Карло:

а) для закона эмпирического распределения;

б) для равномерного закона распределения

Выводы по второму разделу

1. Разработанная формальная модель безопасности МАУ позволяет учесть ряд атрибутов доступа, включая местоположение МАУ, для формирования управляющей команды на смену конфигурации МАУ с целью перевода его в защищенное состояние, удовлетворяющее требованиями безопасности информации и качества предоставляемых услуг.

2. Обоснована корректность данной модели на основе доказательств отсутствия запрещенных информационных потоков от объектов с высоким уровнем конфиденциальности к объектам с низким уровнем конфиденциальности.

3. Показано, что применение разработанной формальной модели безопасности МАУ позволяет ограничить потенциально опасные доступы в системе, тем самым обеспечив выполнение заложенных в политику безопасности требований, и повысить адекватность СЗИ, построенной на основе данной формальной модели безопасности МАУ, условиям ее эксплуатации в КС.

4. Разработана модель системы определения местоположения МАУ, позволяющая оценить вероятность его местонахождения в специальном помещении с повышенными требованиями по защищенности.

5. Обосновано использование БСПД, позволяющей одновременно осуществлять как измерение уровня сигнала МАУ точками доступа, так и защищенное информационное взаимодействие между МАУ и ЗКС, снижая тем самым издержки при проектировании и сопровождении по сравнению с системами определения местоположения на основе датчиков и других технологий.

6. Обоснована алгоритмическая разрешимости предлагаемого подхода по вычислению вероятности нахождения МАУ в специальном помещении. Показано, что для повышения достоверности определения местоположения МАУ целесообразно использовать эмпирические данные о статистике ошибки измерения местоположения, а пороговое значение критерия принятия решения об уровне защищенности помещения, в котором находится МАУ, необходимо выбирать исходя из требований заказчика и допустимых значений ошибки 2-го рода.

7. Апробация модели системы определения местоположения осуществлена с помощью имитационного моделирования. Проведена всесторонняя оценка ее качества, включающая в себя проверку адекватности, чувствительности и устойчивости, получены оценки параметров частных моделей, влияющих на достоверность определения местоположения МАУ.

3. АЛГОРИТМ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ МОБИЛЬНОГО АБОНЕНТСКОГО УСТРОЙСТВА, ПОЗВОЛЯЮЩИЙ ОПРЕДЕЛИТЬ ОПТИМАЛЬНУЮ ПРОГРАММНО-АППАРАТНУЮ КОНФИГУРАЦИЮ УСТРОЙСТВА С УЧЕТОМ АТРИБУТОВ ДОСТУПА И ТРЕБОВАНИЙ ПО БЕЗОПАСНОСТИ И КАЧЕСТВУ УСЛУГ

Данный раздел посвящен разработке алгоритма управления безопасностью МАУ в корпоративных сетях с разными требованиями по защищенности [41]. Алгоритм построен на основе разработанной формальной модели безопасности МАУ и входящей в ее состав модели системы определения местоположения, позволяющей оценить вероятность местонахождения МАУ в специальном помещении с повышенными требованиями по защищенности. Кроме того, в алгоритме реализованы процедуры, позволяющие учитывать особенности сигнально-помеховой обстановки в беспроводных сетях передачи данных и требования по качеству предоставления услуг.

В состав данного алгоритма входят:

1) комплекс алгоритмов определения местоположения МАУ, а также алгоритмы обучения подсистем определения местоположения на базе методов трилатерации, *k*-ближайших соседей и байесовского подхода;

2) алгоритм определения вероятности местонахождения МАУ в специальном помещении ЗКС;

3) алгоритм расчета оценки информационной скорости в канале БСПД;

4) алгоритм управления программно-аппаратной конфигурацией МАУ.

В разделе представлено описание цикла управления состоянием МАУ, определены уравнения состояния и наблюдения, цель управления, представлены основные критерии, на основании которых осуществляется выбор оптимальной конфигурации МАУ. Представлено доказательство основных свойств алгоритма.

3.1. Постановка задачи на разработку алгоритма управления безопасность мобильного абонентского устройства

Основная задача алгоритма управления безопасностью МАУ – управление программно-аппаратной конфигурацией МАУ, позволяющей согласовать состояние МАУ с требованиями политики безопасности ЗКС, определяемыми, в том числе, условиями, в которых находится МАУ, а также нормативными требованиями по качеству предоставляемых услуг. Для изменения состояния МАУ из управляющей подсистемы в МАУ передается управляющая команда, позволяющая применить сформированную конфигурацию.

Схема цикла управления безопасностью (программно-аппаратной конфигурацией) МАУ [41] представлена на рисунке 3.1.

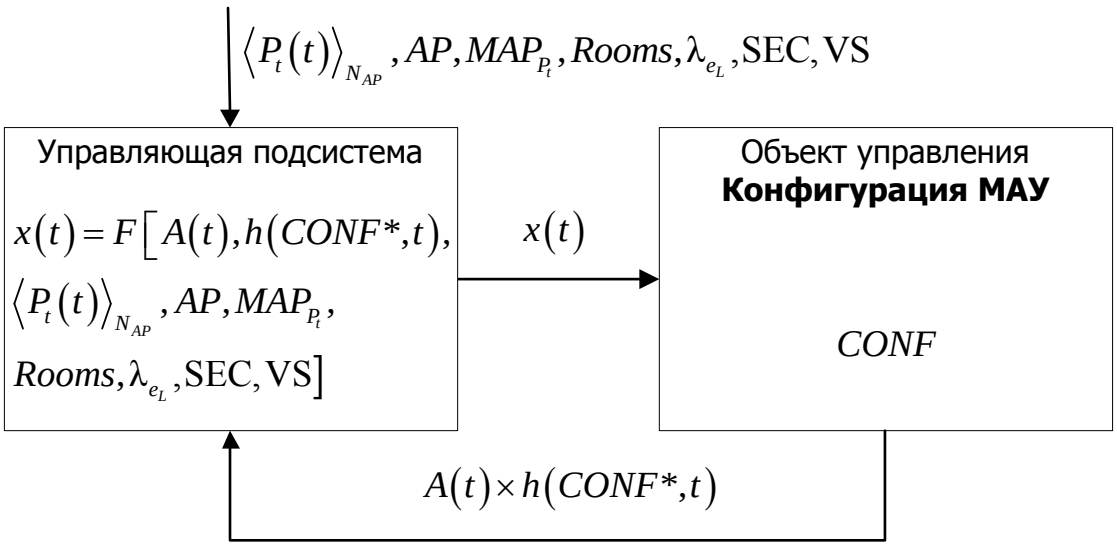


Рисунок 3.1 – Схема управления конфигурацией МАУ

Состояние объекта управления – программно-аппаратная конфигурация МАУ характеризуется совокупностью прав доступа к функциональным блокам (объектам доступа) $CONF$. Данные права реализует входящий в состав МАУ аппаратно-программный модуль доверенной загрузки.

В управляющую подсистему – центр управления информационной безопасности ЗКС, а именно, в контроллер доступа МАУ поступают данные о текущих атрибутах доступа $A(t)$ и текущей конфигурации МАУ $h(CONF^*,t)$. Доверенная БСПД передает в управляющую систему информацию об уровне сигнала МАУ в виде множества $\langle P_t(t)\rangle_{N_{AP}}$, где N_{AP} – количество точек доступа БСПД, в зоне действия которых находится МАУ. Формирование управляющей команды $x(t)$ на смену конфигурации МАУ управляющая система осуществляет также за счет учета данных о расположении точек доступа БСПД AP, карты сигнального пространства MAP_{P_t} (при необходимости), карты помещений $Rooms$, статистики ошибок определения местоположения МАУ для используемой технологии λ_{e_L}, матрицы правил политики безопасности ЗКС SEC и матрицы нормативов информационных скоростей для услуг МАУ VS.

На основе изложенного сформировано уравнение наблюдения:

$$CONF(t) = g\left[t, x(t), A(t) \times \vec{P}_{L_{Room}}(t) \times h(CONF^*,t)\right], \tag{3.1}$$

где $\vec{P}_{L_{Room}}(t)$ – вероятность нахождения МАУ в специальном помещении ЗКС.

Уравнение состояния для процесса управления конфигурацией МАУ при этом может быть представлено в виде

$$CONF(t) = f\left[CONF(t_0), x(\tau)\right], \tau \in [t_0, t], \tag{3.2}$$

где $CONF(t_0)$ – начальное (базовое) состояние МАУ при его включении; $x(\tau)$ – управляющая команда в момент времени τ для перевода МАУ в очередное состояние.

Целью управления конфигурацией МАУ является достижение максимальной результативности защиты информации при его эксплуатации в корпоративных сетях с разными требованиями по защищенности, при этом результативность может быть оценена вероятностью обеспечения безопасности информации. Тогда цель управления формально может быть определена как

$$\max\left[P_{\text{БИ}}(T)\right] = P_{\text{КИ}}(T) \cdot P_{\text{ДИ}}(T) \cdot P_{\text{ЦИ}} \,\middle|\, P_{\text{ЦИ}} = 1. \tag{3.3}$$

Задача на разработку алгоритма относится к классу оптимизационных и формально может быть представлена в виде:

$$\begin{cases} f\left(S^*\right) \longrightarrow \max, \\ \sum\limits_{i=1}^{f\left(S^*\right)} V_{lm}^{i} \le \hat{V}_{lm}, \\ S^* = F_S\left(CONF^*\right) \middle| CONF^* \in CONF^{\text{доп}}, S^* \subseteq S, \end{cases} \tag{3.4}$$

где S – множество, представляемых с помощью МАУ услуг; $f\left(S^*\right)$ – целевая функция, максимизирующая количество предоставляемых пользователю МАУ услуг при заданных условиях; $V_{lm}^{S_i^*}$ – норматив информационной скорости для i-й услуги S_i^* в беспроводном радиоканале между l-м МАУ и m-й точной доступа; $\hat{V}_{lm}$ – оценочная максимально возможная информационная скорость в беспроводном радиоканале между l-м МАУ и m-й точной доступа; $CONF^*$ – новая конфигурация МАУ; $CONF^{\text{доп}}$ – множество допустимых конфигураций МАУ при текущих атрибутах доступа и местоположении МАУ; F_S – функция отображения конфигурации МАУ на множество услуг, которые могут быть предоставлены пользователю МАУ при данной конфигурации.

Анализ формальной постановки задачи (3.4) согласно [38] позволяет классифицировать оптимизационную задачу как *многокритериальную оптимизацию целочисленного динамического программирования*.

Для выбора оптимальной конфигурации МАУ в качестве критериев оценивания оптимальности используются: матрица правил политики безопасности и нормативы информационной скорости для предоставляемых пользователю МАУ услуг.

Матрица правил политики безопасности может быть представлена как

$$\text{SEC}=\begin{vmatrix} CONF_0 & a_{00} & \ldots & a_{0N_A} & L_0 \\ CONF_1 & a_{10} & \ldots & a_{1N_A} & L_1 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ CONF_{N_{CONF}} & a_{N_{CONF}0} & \ldots & a_{N_{CONF}N_A} & L_{N_{CONF}} \end{vmatrix}, \tag{3.5}$$

где $CONF_i, i=\overline{1,N_{CONF}}$ – конфигурации МАУ; $a_{i0},..,a_{ij},..,a_{iN_A}$ – значения N_A атрибутов доступа для i-й конфигурации МАУ; L_i – местоположение МАУ для которых допустимо назначение i-й конфигурации МАУ.

Матрица нормативов информационной скорости для предоставляемых пользователю МАУ услуг может быть представлена как VS=$\left|vs_i\right|, i=\overline{1,\left|S\right|}$, где S – множество услуг; vs_i – норма информационной скорости для i-й услуги.

Решающее правило F_{RECONF} для выбора множества допустимых конфигураций МАУ на основе матрицы правил политики безопасности, множества значений текущих атрибутов доступа A_i и полученной оценки местоположения МАУ $\tilde{L}_{Room}$ может быть представлено в виде:

$$\begin{aligned} &CONF^{\text{доп}} = F_{RECONF}\left(\tilde{L}_{Room}, A_i\right)\middle|\tilde{L}_{Room} = L_{Room}^{\text{треб}}: \\ &:\left(\forall CONF_i \in CONF^{\text{доп}}\ \exists L_{Room}^{\text{треб}} = F_{L_{Room}}\left(CONF_i\right)\right)\wedge \\ &\wedge\left(\forall a_i \in A_i\ \exists a_i^{\text{треб}} \in A_i^{\text{треб}} = F_A\left(CONF_i\right): a_i = a_i^{\text{треб}}\right). \end{aligned} \tag{3.6}$$

Результатом работы системы управления МАУ является совокупность $CONF(t)=\{M, f_t, P_t\}$, представляющая собой назначаемую МАУ конфигурацию, информация о которой передается в управляющей команде. Пример разрешенных конфигураций представлен в таблице 3.1.

Таблица 3.1 – Пример таблицы правил политики безопасности, определяющей конфигурации МАУ и требования к ним

Конфигурация МАУ	Уровень защищенности помещения, $L_{Room}^{\text{треб}}$	Атрибуты доступа ($a_i^{\text{треб}}$)			
		Время	ID МАУ	User ID	…
$CONF_0$	$\overline{L_{\text{О}} \cup L_{\text{К1}} \cup L_{\text{К2}}}$	∞	∞	∞	…
$CONF_1$	$L_{\text{О}}$	∞	5, 29, 53, …	3, 7, 12,…	…
$CONF_2$	$L_{\text{О}}$	8:00-17:30	7, 11, 52, …	3, 17, 23,…	…
$CONF_3$	$L_{\text{К1}}$	∞	13, 17, …	5, 11, …	…
$CONF_4$	$L_{\text{К1}}$	16:00-17:00	17	5	…
$CONF_5$	$L_{\text{К2}}$	∞	13	1	…
$CONF_6$	$L_{\text{К2}}$	11:00-13:00	17, 21	1, 27	…

Состав данной таблицы разрабатывается на этапе проектирования системы управления доступом, а содержание определяется политикой безопасности ЗКС и задается администратором безопасности.

Обобщенная блок-схема разработанного алгоритма управления безопасностью [41] представлена на рисунке 4.4.

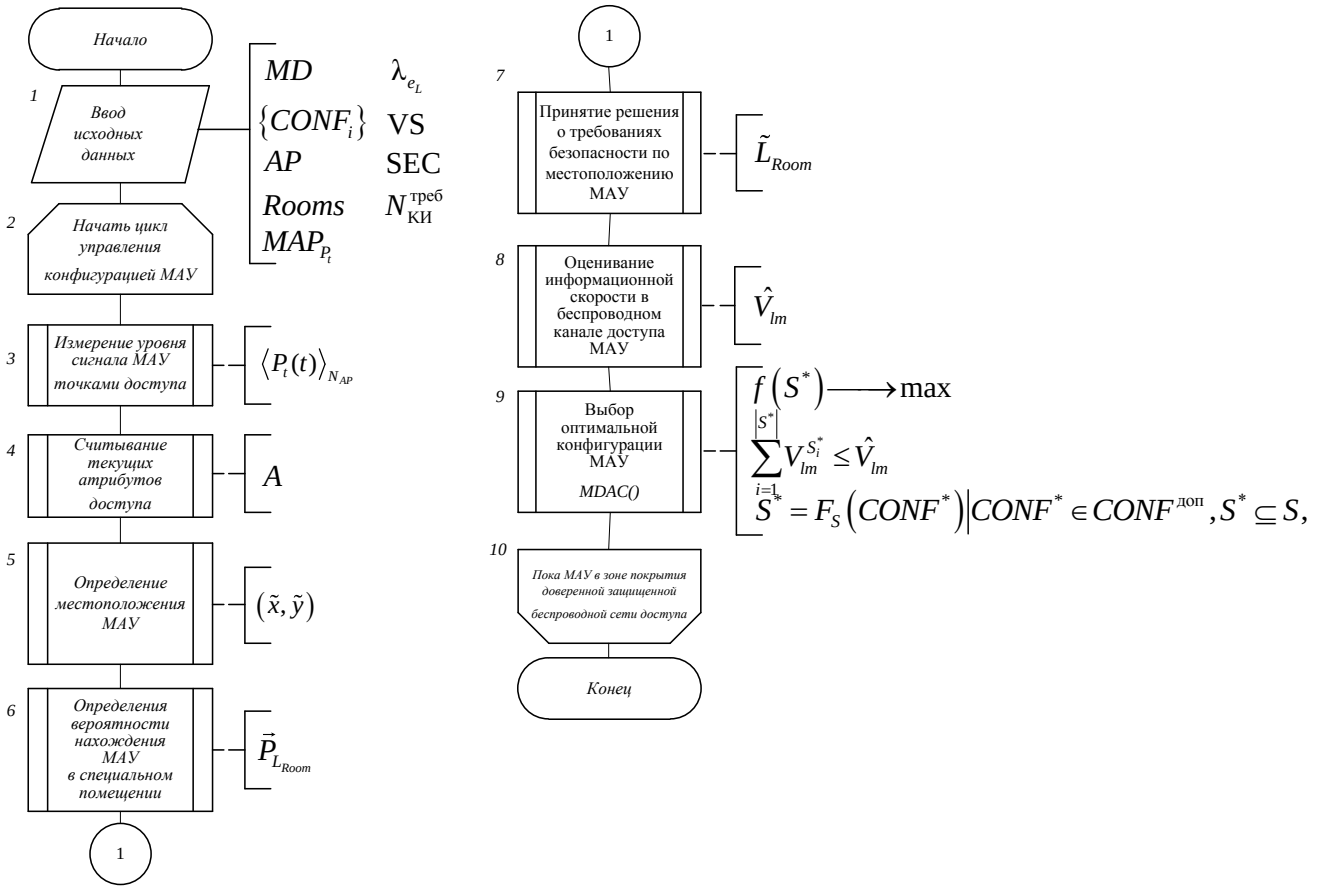


Рисунок 3.2 – Обобщенная блок-схема алгоритма управления безопасностью МАУ

На первом шаге алгоритма в блоке 1 осуществляется инициализация исходных данных:

– ввод технических характеристик приемопередающих устройств;

– ввод параметров помещений;

– ввод координат точек доступа беспроводной сети и карты сигнального пространства;

– ввод параметров алгоритмов определения местоположения МАУ;

– ввод параметров политики безопасности МАУ в ЗКС, нормативов информационной скорости.

В блоке 1 осуществляется инициализация исходных данных.

Блоки 2-10 реализуют цикл управления МАУ.

В блоке 3 реализуется измерения уровня сигнала МАУ точками доступа БСПД и передача значений в управляющую подсистему.

В блоке 4 осуществляется считывание текущих атрибутов доступа.

В блоке 5 осуществляется расчет местоположения МАУ.

В блоке 6 вычисляется вероятность нахождения МАУ в специальном помещении с помощью численного метода вычисления площади на основе метода Монте-Карло.

В блоке 7 осуществляется принятие решения о требованиях безопасности по местоположению МАУ.

В блоке 8 производится оценивание информационной скорости в беспроводном канале доступа МАУ на основе текущей сигнально-помеховой обстановки.

В блоке 9 осуществляется выбор оптимальной конфигурации МАУ на основе заданных в ЗКС правил политики безопасности МАУ и с учетом текущих атрибутов доступа.

Блок № 5 реализует алгоритм определения местоположения МАУ на территории здания, в котором предусмотрена эксплуатация корпоративных сетей с разными требованиями по защищенности. В данной работе использованы известные алгоритмы [43, 51]. На их программную реализацию получено свидетельство [79].

В работе исследовалась эффективность управления безопасностью МАУ применительно к трем известным алгоритмам определения местоположения, в состав которых входят:

1. Алгоритм определения местоположения на основе метода трилатерации, представленный на рисунке В.4. Математические выражения для расчета координат местоположения МАУ данным методом представлены выражениями (А.3)-(А.18). Отличительной особенностью данного алгоритма является отсутствие необходимости предварительных измерений уровней мощности сигнала и составлении карты сигнального пространства. Однако алгоритм на основе метода трилатерации менее точный по сравнению с алгоритмами на основе метода *k*-ближайших соседей и байесовского подхода, требующих обучения и составления карты сигнального пространства.

2. Алгоритм определения местоположения на основе метода *k*-ближайших соседей, представленный на рисунке В.5. Алгоритм обучения классификатора на основе метода k-ближайших соседей изображен на рисунке В.11. Математические выражения для расчета координат местоположения МАУ методом k-ближайших соседей представлены выражениями (А.20)-(А.25).

3. Алгоритм определения местоположения на основе байесовского классификатора (скрытых марковских моделей), представленный на рисунках В.6, В.7. Алгоритм обучения байесовского классификатора изображен на рисунке В.10. Математические выражения для расчета координат местоположения МАУ на основе байесовского подхода представлены выражениями (А.26)-(А.31).

Методы k-ближайших соседей и байесовский подход для определения местоположения МАУ в помещениях являются более точными по сравнению с методом трилатерации однако для их реализации необходимо обучение подсистемы определения местоположения – составление карты измерений. В ряде случаев такое обучение невозможно, поэтому в качестве альтернативы данным методам может использовать менее точный метод трилатерации.

3.1. Алгоритм определения вероятности местонахождения мобильного абонентского устройства в специальном помещении

На основе вычисленного местоположения МАУ можно определить помещение, в котором предположительно находится данное устройство. Уровень защищенности помещения, атрибуты доступа и установленная в ЗКС политика безопасности в совокупности определяют требования безопасности к МАУ, которые могут быть представлены в виде пакета, профиля защиты или задания по безопасности [20]. Пример варианта формализованных требований безопасности к МАУ в ЗКС представлен в таблице 3.1.

На рисунках В.8, В.9 представлен алгоритм определения вероятности местонахождения МАУ в специальном помещении на основе метода Монте-Карло.

В блоке 1 алгоритма осуществляется ввод исходных данных:

– полученные эмпирическим путем данные о выборочном среднем ошибки измерения местоположения для используемого алгоритма определения местоположения и выборочно среднеквадратическое отклонение ошибки определения местоположения;

– параметр, определяющий число "сигма", учитываемое при вычислении радиуса зоны ошибки определения местоположения;

– количество испытаний для реализации метода Монте-Карло;

– вычисленное местоположение пользователя МАУ;

– гистограмма частот плотности вероятности распределения ошибки определения местоположения;

– параметры помещений, включающие в себя их координаты и уровни защищенности.

В блоке 2 осуществляется инициализация начальных значений для:

– радиуса зоны, определяющей вероятное местоположение пользователя МАУ;

– начальные значения вектора вероятностей, определяющего вероятности отнесения к тому или иному уровню защищенности вычисленное местоположение МАУ.

В блоке 3 реализован итератор цикла вычислений испытаний в соответствие с методом Монте-Карло.

В блоке 4 осуществляется выбор закона распределения вероятностей случайной величины процесса, используемого в методе Монте-Карло.

В блоке 5 задается значение радиуса зоны, определяющей вероятное местоположение МАУ, для равномерного закона распределения вероятностей случайной величины процесса, используемого в методе Монте-Карло.

В блоках 6-10 реализовано моделирование случайного процесса в соответствие с законом распределения вероятностей ошибки вычисления местоположения, определяемым гистограммой частот и эмпирическими данными. В процессе моделирования вычисляется значение радиуса зоны, определяющей вероятное местоположение МАУ, для эмпирического закона распределения вероятностей случайной величины процесса, используемого в методе Монте-Карло.

В блоке 11 за счет использования генератора случайных чисел с равномерным распределением вероятностей генерируется точка с координатами внутри окружности с вычисленным в блоках 4-10 радиусом.

В блоках 12-14 осуществляется поиск помещения, в котором находится сгенерированная точка со случайными координатами, а также подсчет количества точек попавших в помещения различных уровней защищенности. Попадание точки в помещение с уровнем "ОИ" увеличивает счетчика уровня "ОИ" на единицу. Аналогично происходит и для других уровней защищенности.

В блоках 15-19 осуществляется расчет вероятности нахождения МАУ в помещениях с различными уровнями защищенности, выполняемого на основе метода Монте-Карло и заданного порога принятия решения.

В блоке 20 на основе вычисленной оценки местоположения МАУ и текущих атрибутов доступа осуществляется выборка из базы данных совокупности требований безопасности, предъявляемых к МАУ.

Математические выражения для расчета вероятности нахождения МАУ в специальном помещении и принятия решения об уровне защищенности помещения, в котором предположительно находится МАУ представлены выражениями (2.2)-(2.9).

3.2. Алгоритм оценивания информационной скорости в беспроводном канале доступа с OFDM модуляцией, учитывающий сигнально-помеховую обстановку

Использование беспроводного канала доступа для МАУ характеризуется достаточно сложной сигнально-помеховой обстановкой. В первую очередь из-за того, что устройства используются в помещениях внутри здания, вследствие чего серьезное влияние оказывает многолучевость распространения сигнала и появление быстрых замираний, а также значительное количество переотражений, поглощение сигнала, проходящего через конструкции здания.

Исходя из этого, для формирования оптимальной конфигурации МАУ, позволяющей предоставить пользователю услуги необходимого качества, возникает потребность учитывать реальную информационную скорость в беспроводном канале доступа с учетом сигнально-помеховой обстановки.

Классический метод оценки информационной скорости предполагает, что прием сигнала осуществляется на фоне белого гауссова шума. В реальности же, как показано в [13], в условиях помещений, а также других МАУ и базовых станций в сети возникают дополнительные внутрисистемные помехи, которые необходимо учитывать. Существуют подходы, позволяющие получить оценку информационной скорости с использованием индекса модуляции и схемы кодирования [12], а также на основе формулы Шеннона для канала с аддитивным белым гауссовским шумом [89]. В работе [63] проведен анализ данных и сделан вывод, что они дают достаточно завышенные значения. В [63] предложена методика, основанная на формуле Шеннона, но позволяющая учитывать сигнально-помеховую

обстановку в канале с OFDM модуляцией с многолучевым распространением и межсимвольной интерференцией.

В основе методики, предложенной в работе [63], лежит оценка информационной скорости V_{lm} от l-го МАУ до m-й базовой станции на основе формулы Шеннона:

$$V_{lm} \approx k_{\lambda} \cdot \frac{\nu_c}{2} \cdot \sum_{r=1}^{I^u} \log_2\left(\gamma_{lm}^{sr} + 1\right), \tag{3.7}$$

где k_{λ} – коэффициент, учитывающий долю информационной составляющей скорости передачи в пропускной способности канала связи; ν_c – количество OFDM символов в секунду; I^u – количество поднесущих в радиоканале; γ_{lm}^{sr} – отношение сигнал/помеха для r-й поднесущей.

Факторами, влияющими на ошибки при приеме отдельного OFDM символа, кроме шума измерения, являются многолучевое распространение сигнала, а также присутствие сигналов соседних кодовых символов, связанное с асинхронностью работы различных передающих устройств при демодуляции. Исходя из этого, сигнал на входе демодулятора может быть представлен в виде:

$$\begin{aligned} Z_{lm}^{k}(t) = \sum_{i=1}^{I^u} \sum_{m'=1}^{M} \sum_{q=1}^{Q} \mathrm{Re}\Big\{ A_{qlm'} \cdot \Big[\dot{x}_{ik}^{m'} \cdot \exp\Big(j\omega_{im'} \Big(t - t_{qk}^{lm'}\Big)\Big) \cdot \upsilon\Big(t - t_{qk}^{lm'}, -T_p, T_D\Big) + \\ + \dot{x}_{i(k+1)}^{m'} \cdot \exp\Big(j\omega_{im'} \Big(t - t_{q(k+1)}^{lm'}\Big)\Big) \cdot \upsilon\Big(t - t_{q(k+1)}^{lm'}, -T_p, T_D\Big) \Big] \Big\} \cdot \upsilon\Big(t - \hat{t}_k^{lm}, 0, T_D\Big) + n(t), \end{aligned} \tag{3.8}$$

где M – количество передающих устройств; Q – количество учитываемых лучей; $A_{qlm'}$ – амплитуда q-го луча от m'-го передающего устройства к l-му принимающему; $\dot{x}_{ik}^{m'}$ – модулированый k-й OFDM символ на i-й поднесущей от m'-го передатчика; $\hat{t}_{qk}^{lm'}$ – время прихода q-го луча, k-го кодового символа m'-го передатчика к l-му приемнику; T_p – длительность циклического префикса; T_D – длительность OFDM символа; $\hat{t}_k^{lm}$ – выбранное время приема k-го кодового символа m-

го передатчика; $\upsilon(t,T_-,T_+)=\begin{cases}1,-T_-\le t\le T_+\\0,(t<-T_-)\cup(t>-T_+)\end{cases}$ – прямоугольный импульс; $n(t)$ – помеха.

В работе [63] сделано допущение, что для оценивания статистических параметров помех, входящих в выражение (3.8), достаточно определить математическое ожидание и дисперсию, поскольку стандартные алгоритмы приема рассчитаны на гауссовское распределение помех. При этом показано, что, приняв распределение символов $\dot{x}_{ik}^{m'}$ равномерным, математическое ожидание помехи будет равно нулю. Дисперсия помехи, с учетом того, что распределение вероятностей момента поступления сигнала $P\left(\Delta t_k^l\right)$ принято равномерным, всеми передатчиками используются одинаковые поднесущие, их количество одинаково, вид модуляции и средняя передаваемая мощность постоянна, может быть определена как

$$\sigma^2_{\dot{y}_{rl}^{kE}}=\frac{1}{\pi^2\cdot(I-1)}\cdot\sum_{\substack{m'=1\\m'\neq m}}^{M}\bar{A}_{lm'}{}^2\cdot\sum_{i=N_{m'rm}+1}^{I^u+N_{m'rm}}\frac{1}{i^2}\cdot\sum_{\Delta t_k^l=1}^{I-1}\left\{\sin^2\left(\frac{\pi\cdot i\cdot\left(I-\Delta t_k^l\right)}{I}\right)+\sin^2\left(\frac{\pi\cdot i\cdot\Delta t_k^l}{I}\right)\right\},\quad(3.9)$$

где $\bar{A}^2_{lm'}$ – средняя мощность, поступающая от передатчика с номером m' на вход приемника l по всем лучам.

Анализ данного выражения показывает, что дисперсия помех определяется мощностями сигналов помех $\bar{A}^2_{lm'}$ и некоторым коэффициентом, учитывающим степень влияния помехи, зависящей от частотного разноса поднесущей, на которой идет передача и каналов помех. Обозначив данный коэффициент через $K(f)$, дисперсия помех может быть представлена как:

$$\sigma^2_{\dot{y}_{rl}^{kE}}=\sum_{\substack{m'=1\\m'\neq m}}^{M}\bar{A}^2_{lm'}\cdot K(f_{m'}-f_{rm}),\qquad(3.10)$$

где $\bar{A}^2_{lm'}$ – средняя мощность сигнала от m'-го передающего устройства к l-му принимающему; $f_{m'}$ – частота передатчика помехи; f_{rm} – частота поднесущей, на которой осуществляется передача; $K(f)$ – функция, учитывающая влияние помехи и рассчитываемая по формуле:

$$K(f)=\sum_{i=f\cdot T_D+1}^{f\cdot T_D+I^u}\begin{cases}\dfrac{(2\cdot I-1)}{3\cdot I}, \text{ при } i=0,\\ \dfrac{1}{\pi^2\cdot(I-1)\cdot i^2}\cdot\sum\limits_{\Delta t_k^l=1}^{I-1}\left(1-\cos\left(\dfrac{2\cdot\pi\cdot i\cdot\Delta t_k^l}{I}\right)\right), \text{ при } i\neq 0,\end{cases} \tag{3.11}$$

где I – общее количество поднесущих, используемых в OFDM сигнале; Δt_k^l – возможная задержка передачи OFDM символа от момента его приема.

На основе представленных выражений отношение сигнал/помеха на входе канального демодулятора будет выглядеть как

$$\gamma_{lm}^{sr}=\frac{\overline{A}_{lm}^{r\ 2}}{\sum\limits_{\substack{m'=1\\ m'\neq m}}^{M}\overline{A}_{lm'}{}^2\cdot K(f_{m'}-f_{rm})+\sigma_n^2}. \tag{3.12}$$

Дополнительно необходимо учесть отличие мощности полезного сигнала от средней мощности, вызванное многолучевостью распространения. Для этого вводится некоторый коэффициент запаса Γ по отношению к уровню сигнал/помеха [11]:

$$\gamma_{lm}^{sr}\approx\frac{\gamma_{lm}^{r}}{\Gamma}. \tag{3.13}$$

Учитывая, что, как правило, $\gamma_{lm}^{sr}\gg 1$, искомую оценку информационной скорости можно записать в виде:

$$\hat{V}_{lm}\approx k_\lambda\cdot\frac{v_c}{2}\cdot\sum_{r=1}^{I^u}\log_2\left(\gamma_{lm}^{sr}+1\right)-k_\lambda\cdot\frac{v_c}{2}\cdot I^u\cdot\log_2(\Gamma). \tag{3.14}$$

Значения k_λ и Γ для сети с известными параметрами и развернутыми в конкретных условиях можно считать постоянными и оценить их при помощи критерия минимума СКО на основе результатов проведенных эмпирических тестов:

$$k_\lambda=\frac{L\cdot\sum\limits_{l=1}^{L}V_{lm}\cdot V_{lm_{real}}-\sum\limits_{l=1}^{L}V_{lm}\cdot\sum\limits_{l=1}^{L}V_{lm_{real}}}{L\cdot\sum\limits_{l=1}^{L}V_{lm}^2-\left(\sum\limits_{l=1}^{L}V_{lm}\right)^2}, \tag{3.15}$$

$$\Gamma = 2^{-2\cdot\frac{\sum_{l=1}^{L} V_{lm_{real}} - k_\lambda \cdot \sum_{l=1}^{L} V_{lm}}{k_\lambda \cdot \upsilon_c}}. \qquad (3.16)$$

Таким образом, итоговая, рассчитываемая в алгоритме оценка информационной скорости передачи, может быть получена на основе известных технических характеристик БСПД, результатов проведенных эмпирических тестов и измерения параметров k_λ и Γ в беспроводном радиоканале, рассчитываемых с помощью выражений (3.15) и (3.16), и аналитических выражений (3.11)-(3.14).

3.3. Алгоритм управления программно-аппаратной конфигурацией МАУ

Реализация алгоритма управления программно-аппаратной конфигурацией МАУ основывается на применении правил политики безопасности, определяемых местоположением устройства и атрибутами доступа, и критериями качества предоставляемых пользователю МАУ в ЗКС услуг. Вариант реализации данного алгоритма описан в работах [47, 80]. Для формирования конфигурации МАУ необходимо решить многокритериальную оптимизационную задачу.

Требования безопасности определяют функциональные требования к МАУ и его пользователю, а также гарантии, которые технически реализуются в виде совокупности прав доступа пользователя, определяющей разрешенные пользователю доступы (операции) и конфигурацию МАУ, определяющую разрешенные функциональные возможности МАУ при текущих условиях доступа. Помимо требований безопасности еще одним критерием выбора конфигурации МАУ являются нормативы информационной скорости в радиоканале, позволяющие обеспечить мобильному пользователю требуемый уровень качества услуг связи на основе полученной оценки информационной скорости, учитывающей сигнально-помеховую обстановку.

Реализация алгоритма управления программно-аппаратной оптимальной конфигурацией МАУ представлена на рисунке 3.3.

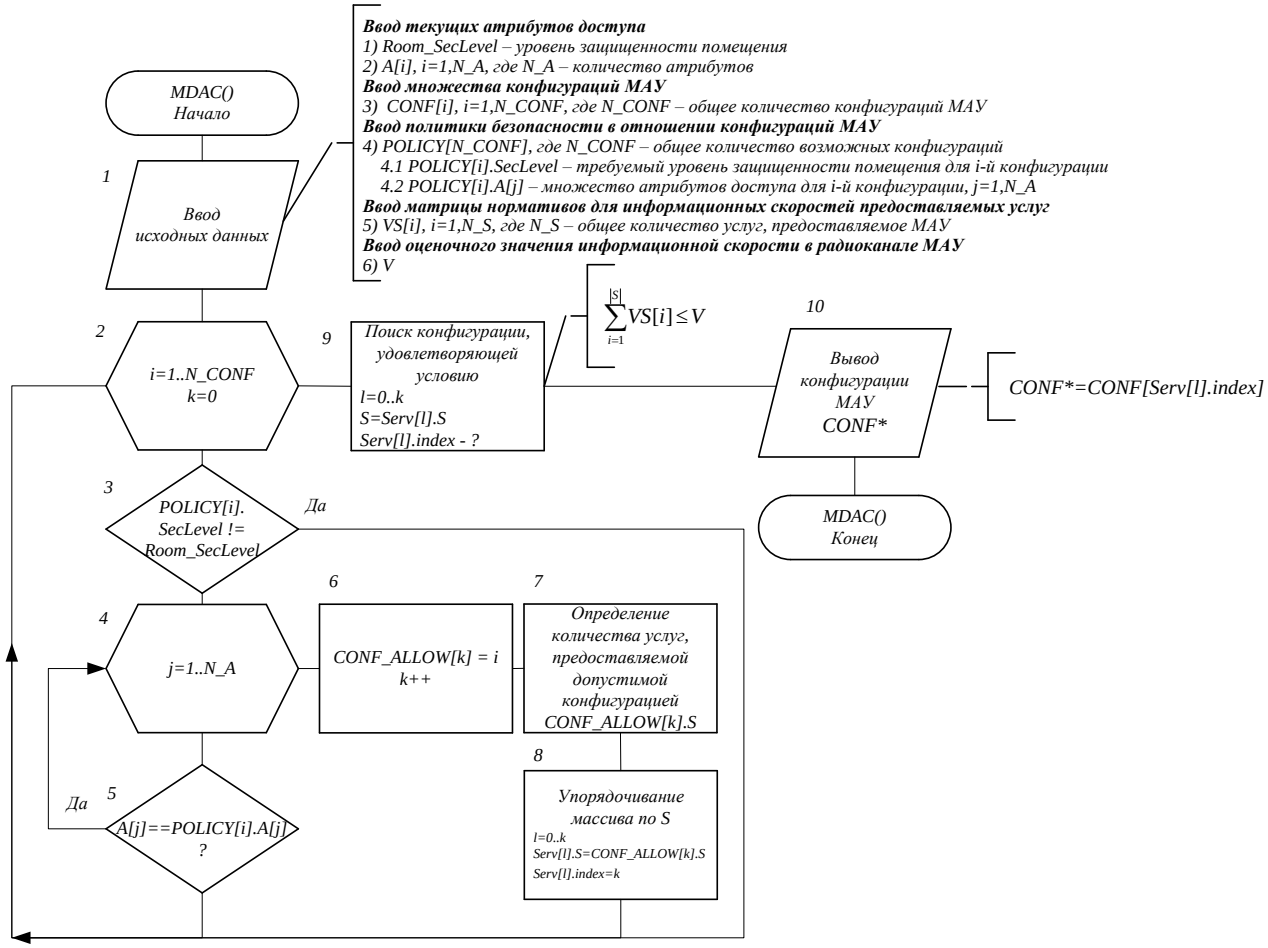


Рисунок 3.3 – Блок-схема алгоритма управления программно-аппаратной конфигурацией мобильного абонентского устройства

В блоке 1 данного алгоритма осуществляется ввод исходных данных:

– уровень защищенности помещения, в котором находится пользователь МАУ;

– вектор атрибутов доступа пользователя МАУ;

– множество возможных конфигураций МАУ и политика безопасности в отношении конфигураций МАУ;

– множество возможных прав доступа пользователя МАУ;

– матрица нормативов информационных скоростей представляемых МАУ услуг;

– оценка информационной скорости в радиоканале МАУ.

В блоках 2-6 осуществляется выборка допустимых конфигураций МАУ, соответствующих текущим условиям доступа.

В блоке 7 осуществляется определение количества услуг, которое будет предоставлять МАУ при заданной допустимой конфигурации.

В блоке 8 происходит упорядочивание массива допустимых конфигураций по количеству предоставляемых услуг.

В блоке 9 осуществляется поиск конфигурации из массива допустимых, удовлетворяющий критерию соответствия суммы требуемой информационной скорости для предоставляемых услуг значению оценки информационной скорости в радиоканале МАУ.

В блоке 10 осуществляется вывод оптимальной конфигурации МАУ.

Решение оптимизационной задачи методом целочисленного динамического программирования данным алгоритмом осуществляется следующим образом:

1. Задается область значений в виде множества возможных конфигураций МАУ $CONF$ и исходные данные в виде множества атрибутов доступа A и уровня защищенности помещения $L_{\text{МАУ}}$, в котором находится в данный момент МАУ.

2. Задаются множества критериев в виде:

– политики безопасности МАУ, определяющей значения атрибутов доступа для выбора допустимых конфигураций МАУ в виде матрицы SEC выражения (3.5);

– множества VS нормативов информационных скоростей для услуг, предоставляемых МАУ.

3. Определяется множество допустимых конфигураций $CONF^{\text{доп}} \subset CONF$ в соответствие с решающим правилом, представленным выражением (3.6).

4. Множество $CONF^{\text{доп}}$ упорядочивается в соответствие с критерием $\left|S^*\right| \to \max$, где $S^* = F_S\left(CONF^*\right)\left|CONF^* \in CONF^{\text{доп}}, S^* \subseteq S\right.$, S – множество, представляемых с помощью МАУ услуг; $\left|S^*\right|$ – мощность множества S^*; F_S – функция отображения конфигурации МАУ на множество услуг, которые могут быть предоставлены пользователю МАУ при данной конфигурации. На данном этапе

осуществляется поиск допустимой конфигурации МАУ, позволяющей предоставлять мобильному пользователю максимальное количество услуг. Данный поиск осуществляется циклически для упорядочивания массива $CONF^{\text{доп}}$ по убыванию, в соответствие с критерием $\left|S^*\right| \to \max$. Таким образом, что $\left|S_1^*\right| \le \left|S_2^*\right| \le ... \le \left|S_n^*\right|$, где $S_i^* = F_S\left(CONF_i\right),\ CONF_i \in CONF^{\text{доп}} = \left\{CONF_1, CONF_2, ..., CONF_n\right\}$.

5. Осуществляется пошаговый анализ множества $CONF^{\text{доп}}$ на предмет удовлетворения его элементов критериям $\left(\sum_{i=1}^{|S^*|} V_{lm}^{S_i^*}\right)_{\langle CONF_j \rangle} \le \hat{V}_{lm} \mid CONF_j \in CONF^{\text{доп}}$ и $\left|S^*\right| \to \max$, где в левой части неравенства расположена сумма информационных скоростей для услуг, предоставляемых j-й конфигурацией $CONF_j$.

Таким образом, на 5-м шаге определяется оптимальная конфигурация МАУ, удовлетворяющая требованиям безопасности в соответствие с политикой безопасности МАУ, определяемой матрицей SEC, и требованиям качества предоставляемых МАУ услуг, определяемых множеством VS.

В качестве численного примера рассмотрим ЗКС с политикой безопасности МАУ, заданной матрицей:

$$\text{SEC}=\begin{vmatrix} CONF_0 & U & U & U & \overline{L_0 \cup L_1 \cup L_2} \\ CONF_1 & 2 & 101 & 15 & L_2 \\ CONF_2 & 3 & 102 & 18 & L_0 \\ CONF_3 & 2 & 102 & 17 & L_1 \\ CONF_2 & 2 & 102 & 17 & L_1 \\ CONF_4 & 3 & 103 & 18 & L_2 \\ CONF_2 & 3 & 101 & 16 & L_1 \\ CONF_1 & 4 & 101 & 17 & L_1 \\ CONF_3 & 3 & 103 & 16 & L_1 \\ CONF_4 & 2 & 102 & 17 & L_1 \end{vmatrix},$$

а множество нормативов информационных скоростей согласно [70] задано как $\mathrm{VS}=\{vs_i\}=\{384,64,128,128,64,512,256,64,1024\}$ для $|S|=9$, где vs_i – норматив информационной скорости для i-й услуги s_i.

Пусть необходимо определить оптимальную конфигурацию для МАУ со следующими атрибутами доступа: $A=\{2,102,17\}$, $L_{\text{МАУ}}=L_1$ при рассчитанной оценке информационной скорости в радиоканале $V=1024$.

Правило F_S для рассматриваемых конфигураций задано следующими отношениями

$$CONF_0 \xrightarrow{F_S} \{s_1,s_2,s_3,s_4,s_5\},$$

$$CONF_1 \xrightarrow{F_S} \{s_2,s_4,s_5,s_6,s_7\},$$

$$CONF_2 \xrightarrow{F_S} \{s_6,s_7,s_8\},$$

$$CONF_3 \xrightarrow{F_S} \{s_2,s_6,s_7,s_8\},$$

$$CONF_4 \xrightarrow{F_S} \{s_4,s_5,s_6,s_7,s_9\}.$$

Найдем оптимальную конфигурацию МАУ для заданных условий и критериев поиска.

Шаг 1. Область значений задана множеством $CONF=\{CONF_0,CONF_1,CONF_2,CONF_3,CONF_4\}$, $A=\{2,102,17\}$, $L_{\text{МАУ}}=L_1$.

Шаг 2. Критерии заданы матрицей SEC и множеством VS.

Шаг 3. В соответствие с решающим правилом, представленным выражением (3.6), заданными атрибутами доступа $A=\{2,102,17\}$ и $L_{\text{МАУ}}=L_1$ множество допустимых критериев определено как $CONF^{\text{доп}}=\{CONF_2,CONF_3,CONF_4\}$.

Шаг 4. Упорядочиваем множество $CONF^{\text{доп}}$ в соответствие с критерием $|S^*|\to\max$, где $S^*=F_S\left(CONF^*\right)\left|CONF^*\in CONF^{\text{доп}},S^*\subseteq S\right.$. В результате получаем $CONF^{\text{доп}}=\{CONF_4,CONF_3,CONF_2\}$.

Шаг 5. Осуществляется пошаговый анализ полученного упорядоченного множества $CONF^{\text{доп}}$ на предмет удовлетворения его элементов критериям $\left(\sum_{i=1}^{|S^*|} V_{lm}^{S_i^*}\right)_{\langle CONF_j\rangle} \le \hat{V}_{lm} \mid CONF_j \in CONF^{\text{доп}}$ и $|S^*| \to \max$. В результате получаем:

– для $CONF_4$ $|S^*| = 5$, $\left(\sum_{i=1}^{|S^*|} V_{lm}^{S_i^*}\right)_{\langle CONF_4\rangle} = 1984$, $\left(\sum_{i=1}^{|S^*|} V_{lm}^{S_i^*}\right)_{\langle CONF_j\rangle} > \hat{V}_{lm}$

– для $CONF_3$ $|S^*| = 4$, $\left(\sum_{i=1}^{|S^*|} V_{lm}^{S_i^*}\right)_{\langle CONF_3\rangle} = 896$, $\left(\sum_{i=1}^{|S^*|} V_{lm}^{S_i^*}\right)_{\langle CONF_j\rangle} \le \hat{V}_{lm}$

– для $CONF_4$ $|S^*| = 2$, $\left(\sum_{i=1}^{|S^*|} V_{lm}^{S_i^*}\right)_{\langle CONF_2\rangle} = 832$, $\left(\sum_{i=1}^{|S^*|} V_{lm}^{S_i^*}\right)_{\langle CONF_j\rangle} \le \hat{V}_{lm}$.

Таким образом, из допустимых конфигураций МАУ заданным критериям удовлетворяет конфигурация $CONF_3$.

3.2. Оценка свойств разработанного алгоритма управления безопасностью мобильного абонентского устройства

Для разработанного алгоритма управления безопасностью МАУ была произведена оценка следующих основных свойств [1, 8, 41]:

– результативность;

– элементарность;

– корректность;

– вычислительная сложность;

– сложность алгоритма по памяти;

– точность;

– сходимость.

Результативность (отсутствие аварийного останова) алгоритма достигается проверкой корректности входных данных. Все данные вводятся в алгоритм на этапе пуско-наладочных работ, поэтому при условии, что они введены корректно, *алгоритм результативен*.

Данный алгоритм является **элементарным**, так как содержит блоки, выполняющие простые операции: присвоение, вычисление математических выражений и сравнение. Для блоков, не являющихся элементарными, предназначенных для преобразования исходных данных, элементарность достигается подробным описанием операций, совершаемых над данными в этих блоках. Не элементарными блоками в разработанном алгоритме являются только блоки измерения уровня сигнала, принимаемого точками доступа. В данном блоке реализуется операция вывод данных из драйвера модуля беспроводной связи, содержащих информацию об уровне мощности принимаемого от МАУ сигнала.

Доказательство **корректности** алгоритма сводится к указанию блоков, являющихся выходами из всех возможных циклов. Общий алгоритм циклов не имеет. Частные подпрограммы имею циклы, построенные по принципу цикла "for" без операций дополнительной модификации итератора внутри тела цикла, что дает основание говорить о том, что все циклы конечны. Таким образом, *алгоритм является корректным*.

Общая **временная сложность алгоритма** определяется временем инициализации ($T_{\text{иниц}}$) и временем, затрачиваем на процедуры определения местоположения (T_{LOC}), формирование требований безопасности (T_{POLICY}) и формирования конфигурации МАУ (T_{CONF}). Таким образом, сложность алгоритма составит

$$S_t = T_{\text{иниц}} + T_{LOC} + T_{POLICY} + T_{CONF}, \qquad (3.17)$$

где $T_{LOC} = \left\{ t_{\text{трилат}}, t_{kNN}, t_{\text{НММ}} \right\}$, $t_{\text{трилат}}$ – сложность алгоритма трилатерации, t_{kNN} – сложность алгоритма определения местоположения на основе метода k-ближайших соседей, $t_{\text{НММ}}$ – сложность алгоритма определения местоположения на основе байесовского подхода.

Наиболее трудоемкими процедурами являются процедуры определения местоположения методами k-ближайших соседей, методом на основе байесовского подхода и процедура формирования требований безопасности (T_{POLICY}).

Сложность алгоритма определения местоположения методом k-ближайших соседей составляет:

$$t_{kNN} \sim k \cdot N_{kNN}, \tag{3.18}$$

где k – число "соседей", N_{kNN} – число точек сигнального пространства.

Сложность алгоритма определения местоположения методом на основе байесовского подхода составляет:

$$t_{HMM} \sim N_{AP} \cdot N_{Int} + k \cdot N_{HMM}, \tag{3.19}$$

где N_{AP} – число точек доступа беспроводной сети; k – число наиболее вероятных состояний; N_{Int} – число интервалов гистограммы частот для функции плотности распределения вероятностей ошибки измерений местоположения; N_{HMM} – число точек сигнального пространства.

Сложность алгоритма формирования требований безопасности зависит от количества помещений и заданного числа испытаний метода Монте-Карло. Таким образом,

$$T_{POLICY} \sim N_{MC} \cdot N_{Int} \cdot N_{Rooms}, \tag{3.20}$$

где N_{MC} – заданное число испытаний для метода Монте-Карло; N_{Int} – число интервалов гистограммы частот для плотности распределения вероятностей ошибки измерений местоположения; N_{Rooms} – количество помещений. Таким образом, сложность алгоритма по времени будет составлять:

$$S_t = C_1\left(N_{AP} \cdot N_{Int} + k \cdot N_{HMM}\right) + C_2 \cdot N_{MC} \cdot N_{Int} \cdot N_{Rooms}, \tag{3.21}$$

где C_1, C_2, – константы.

Оценивание временной сложности алгоритма проводилось на ПЭВМ со следующими техническими характеристиками: процессор: Intel® Core™2 Duo CPU E4600 @ 2,40 ГГц; Установленная память (ОЗУ): 2,00 ГБ; Тип системы: 32-разрядная ОС; ОС: Windows 7 Профессиональная SP 1.

В качестве исходных данных использовались:

1) технические характеристики МАУ:

– мощность передатчика 0,07943282347242815 Вт;

– частота передатчика 2,4 ГГц с поднесущими, определяемыми стандартом 802.11n;

– параметры k_λ и Γ, характеризующие сигнально-помеховую обстановку, определены равные 0,53 и 12,77 соответственно;

2) расположение, уровни защищенности и другие параметры помещений определяются схемой помещений, представленной на рисунке 2.9, при размерах здания $16{,}8\,\text{м} \times 38{,}0\,\text{м}$;

3) точки доступа беспроводной сети в системе координат исследуемого здания расположены следующим образом: $AP_1 = (3{,}6\,\text{м}; 19{,}2\,\text{м})$, $AP_2 = (3{,}6\,\text{м}; 5{,}2\,\text{м})$, $AP_3 = (20{,}0\,\text{м}; 12{,}0\,\text{м})$, $AP_4 = (37{,}6\,\text{м}; 5{,}2\,\text{м})$, $AP_5 = (37{,}6\,\text{м}; 19{,}2\,\text{м})$;

4) политика безопасности МАУ в ЗКС определена таблицей 3.1;

5) матрица нормативов информационной скорости для предоставляемых пользователю МАУ услуг в соответствие с [70] определена таблицей 3.2.

Таблица 3.2 – Нормативы информационной скорости для предоставляемых пользователю МАУ услуг

Услуга	Норматив, КБ/с
Работа в режиме видеоконференцсвязи (два абонента)	384
Электронный почтовый обмен	64
Работа в режиме VoIP-клиента	128
Передача мультимедийных сообщений через сеть сотовой связи	128
Прием и передача защищенных SMS сообщений	64
Защищенная видеоконференцсвязь	512
Защищенная IP-телефония	256
Защищенный электронный почтовый обмен	64
Защищенный доступ к передаче данных по беспроводным каналам связи Wi-Fi (802.11n)	10000

Расчет местоположения МАУ осуществлялся в соответствие с выражениями для метода трилатерации – (А.3)-(А.19), для метода k-ближайших соседей – (А.20)-(А.25), для метода на основе байесовского подхода – (А.26)-(А.31).

Расчет вероятности местонахождения МАУ в специальном помещении осуществлялся в соответствие с выражениями (2.3)-(2.9).

Оценивание информационной скорости в радиоканале МАУ с учетом сигнально-помеховой обстановки осуществляется в соответствие с выражением (3.14).

Разработанные алгоритмы реализованы в программном комплексе, состоящем из рядом программ для ЭВМ [76, 77, 79]. Оценки временной сложности указанных алгоритмов, полученные с помощью данных программ, представлены в таблице 3.3.

Таблица 3.3 – Оценки временной сложности процедур алгоритма управления конфигурацией МАУ

Алгоритм (процедура)	Параметр	Временная сложность, мс
Инициализация исходных данных	$T_{\text{иниц}}$	0,01
Алгоритм определения местоположения – на основе метода трилатерации – на основе метода *k*-ближайших соседей – на основе байесовского подхода	T_{LOC}	 0,98 1,01 2,92
Алгоритм определения вероятности местонахождения МАУ в специальном помещении	T_{POLICY}	710
Алгоритм оценивания информационной скорости в беспроводном канале доступа	T_V	0,3
Алгоритм формирования оптимальной конфигурации МАУ	T_{CONF}	1,12
Итого:	S_t	714,35

Анализ таблицы показывает, что наиболее вычислительно емкой является процедура определения вероятности МАУ в специальном помещении, при этом суммарная временная сложность алгоритма управления конфигурацией МАУ не превышает 714,35 мс.

Сложность алгоритма по памяти равна $S_v = N_{AP} \cdot N_{Int} \cdot N_{HMM} + N_{Rooms}$. Такая оценка сложности является полиномиальной. В процессе определения местоположения методом на основе байесовского подхода необходимо хранить данные обо всех помещениях, а также статистику условных вероятностей наблюдения уровней мощности сигнала МАУ в N_{HMM} точках сигнального пространства.

Сходимость. Критическими операциями в алгоритме являются:

– цикл с условием, реализуемый блоками 3-8, рисунок 3.2; блоками 2, 3, рисунок В.4; блоками 2, 4, 5; блоками 3, 4, 6, 7, рисунок В.5; блоками 2, 4, 5, 13, 15, 17, 18, рисунки В.6, В.7; блоками 3, 7, 12, 15, рисунки В.8, В.9; блоками 2, 4, рисунок 3.3;

– функция деления на переменную в блоках 4, 6, 8, 10, 13, рисунок В.4; блоке 10, рисунок В.5 блоках 2, 3, рисунок В.3; блоках 9, 16, рисунки В.8, В.9;

– вычисление квадратного корня в блоках 4, 6, 8, 10, 17, 13, рисунок В.4.

На основе анализа набора предусловий и постусловий для каждого шага алгоритм можно считать сходимым при условии корректности и непротиворечивости исходных данных.

Точность. Точность разработанного алгоритма определяется погрешностью вычислений, которая в общем случае состоит из $\delta_н$ – неустранимой погрешности исходных данных, $\delta_м$ – погрешности метода и $\delta_в$ – погрешности вычислительной платформы, т.е.

$$\delta = \delta_н + \delta_м + \delta_в . \qquad (3.22)$$

Погрешность исходных данных зависит от числа значащих цифр значений параметров и определяется по формуле:

$$\delta_н = 10^{-N+1}, \qquad (3.23)$$

где N – длина мантиссы.

В рассматриваемом алгоритме минимальная длина мантиссы исходных данных $N = 10$. Таким образом, $\delta_н \approx 10^{-10+1} = 10^{-9}$.

Для оценки погрешности метода будем руководствоваться следующими правилами:

1. При суммировании чисел одного знака точность суммы равна наименьшей точности любого слагаемого:

$$\delta_{\text{м}}^{+} = \sup(\delta_1, \delta_2, ..., \delta_{\text{n}}). \tag{3.24}$$

2. При вычитании чисел происходит увеличение наибольшей относительной погрешности одного из компонентов выражения в ν раз, где

$$\nu = \frac{|a+b|}{|a-b|}, \tag{3.25}$$

тогда

$$\delta_{\text{м}}^{-} = \sup(\delta_1, \delta_2, ..., \delta_{\text{n}}) \cdot \nu, \tag{3.26}$$

где a и b – величины, входящие в операцию вычитания.

3. Произведение и частное двух величин обладают погрешностью, приблизительно равной сумме относительных погрешностей компонентов выражений:

$$\delta_{\text{м}}^{\times} \approx \sum_{i=1}^{n} \delta_i, \tag{3.27}$$

$$\delta_{\text{м}}^{\div} \approx \sum_{i=1}^{n} \delta_i. \tag{3.28}$$

4. Для оценки погрешности функций используются следующие соотношения:

$$\delta_{\text{м}}^{y} \approx \nu \cdot \delta_{\text{н}}(x), \tag{3.29}$$

где

$$\nu = \frac{|x| \cdot |f'(x)|}{|f(x)|}, \tag{3.30}$$

где $y = f(x)$ – исследуемая функция; x – аргумент исследуемой функции; y – рассчитанное значение функции.

Таким образом, расчетная точность алгоритма составляет 10^{-4}.

Выводы по третьему разделу

1. Разработан алгоритм управления безопасностью МАУ, позволяющий обеспечить изменение программно-аппаратной конфигурации МАУ в зависимости от условий (атрибутов) доступа, включающих в себя, в том числе, местоположение МАУ, и критериев качества предоставляемых услуг. Отличительными особенностями данного алгоритма являются:

– реализация формальной модели безопасности МАУ, предусматривающей учет условий (атрибутов) доступа, включая местоположение МАУ, требования мандатной ролевой политик управления доступом;

– применение метода Монте-Карло для повышения достоверности определения местоположения МАУ в специальном помещении на основании вычисленного местоположения методами трилатерации, k-ближайших соседей и метода, основанного на байесовском подходе;

– использование алгоритма оценки информационной скорости в канале БСПД, учитывающем сигнально-помеховую обстановку, для выбора оптимальной, с точки зрения требований по качеству предоставляемых услуг, программно-аппаратной конфигурации МАУ;

– формирование оптимальной программно-аппаратной конфигурации МАУ с точки зрения выполнения требований политики безопасности в ЗКС и качества предоставляемых услуг, реализованное в форме многокритериальной оптимизации целочисленного динамического программирования.

2. Представлено описание цикла управления конфигурацией МАУ с уравнениями состояния и наблюдения, обоснованием цели управления.

3. Описаны основные процедуры, входящие в состав разработанного алгоритма. Исследованы основные свойства алгоритма и его процедур, включая временную сложность, сложность по памяти и точность. Получены их численные оценки, а также представлен численный пример работы алгоритма.

4. СИСТЕМА УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ МОБИЛЬНЫХ АБОНЕНТСКИХ УСТРОЙСТВ, ОБЕСПЕЧИВАЮЩАЯ ПОВЫШЕНИЕ ВЕРОЯТНОСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПРИ ДОСТУПЕ К ИНФОКОММУНИКАЦИОННЫМ УСЛУГАМ И ИНФОРМАЦИИ КОРПОРАТИВНЫХ СЕТЕЙ С РАЗНЫМИ ТРЕБОВАНИЯМИ ПО ЗАЩИЩЕННОСТИ ПРИ ИСПОЛЬЗОВАНИИ ЕДИНОГО МАУ

4.1. Научно-технические предложения по составу, структуре и месту системы управления безопасностью мобильными абонентскими устройствами в составе корпоративных сетей с разными уровнями защищенности

Разработанная система управления безопасностью МАУ в корпоративных сетях с разными требованиями по защищенности предполагает наличие следующих компонентов:

– центр управления информационной безопасностью (ЦУИБ);

– контроллер доступа мобильных устройств [76, 77];

– доверенная беспроводная сеть передачи данных;

– подсистема определения местоположения [79];

– доверенные многофункциональные мобильные устройства, в состав которых входит агентный модуль, способный принимать сигналы управления и управлять программно-аппаратной конфигурацией устройства [80].

В рамках управления информационной безопасностью могут быть также реализованы механизмы удаленного мониторинга, основанные на использование особенностей реализации сетевых протоколов. В работах [60, 74, 78] описаны способ удаленного мониторинга и управления информационной безопасностью сетевого взаимодействия на основе использования системы доменных имен и программное обеспечение, позволяющее реализовать данный способ. Для защиты ЗКС от компьютерных атак, а также предотвращения перегрузок в сети и ошибок функционирования необходимо использовать механизмы межсетевого экраниро-

вания. Реализация таких механизмов защиты рассмотрена в работе [62], описывающих способ анализа информационного потока и определения состояния защищенности сети на основе адаптивного прогнозирования и устройство для его осуществления, а также варианты построение систем дистанционного управления и мониторинга перспективных межсетевых экранов.

Для решения задачи безопасного доступа мобильного пользователя к услугам сетей с разными требованиями по защищенности должно обеспечиваться выполнение следующих условий:

1. Существует беспроводная сеть доверенных точек доступа с известным местоположением точек доступа.

1. Канал управления между доверенными точками доступа и МАУ защищен криптографическими средствами защиты информации.

2. МАУ имеет возможность функционировать в различных программно-аппаратных конфигурациях.

3. На МАУ функционирует аппаратно-программный модуль доверенной загрузки (АПМДЗ).

4. На мобильном устройстве функционирует доверенная операционная система (ДОС).

5. В ДОС МАУ функционирует изолированная программная среда.

6. Пользователь МАУ успешно аутентифицирован в системе управления доступом корпоративной сети.

В [61] предложен способ построения защищенного удаленного доступа к информационным ресурсам.

На рисунке 4.4 представлена общая структура основных компонентов ЗКС, обеспечивающих функционирование разработанной системы.

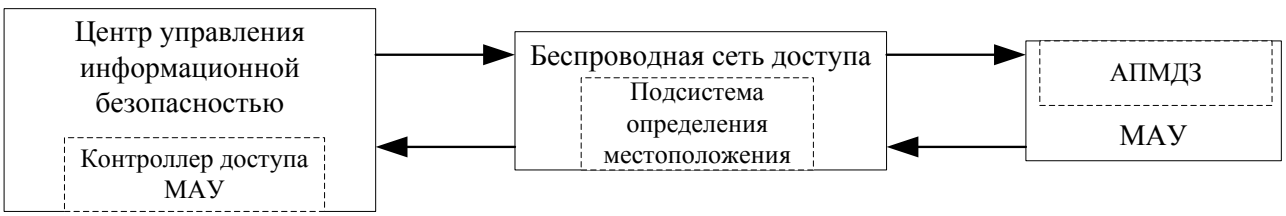


Рисунок 4.4 – Обобщенная структура основных компонентов ЗКС

Для обеспечения наличия управляемой конфигурацией, а также возможности независимой обработки информации в МАУ, данное устройство может включать в свой состав дублируемые компоненты, отвечающие за обработку данных. Дублирование компонентов должно обеспечивать оптоэлектронную или иную развязку трактов прохождения сигналов с разными требованиями по защищенности (разными уровнями конфиденциальности обрабатываемой информации). Пример такой компоновки в составе МАУ представлен на рисунке 4.5.

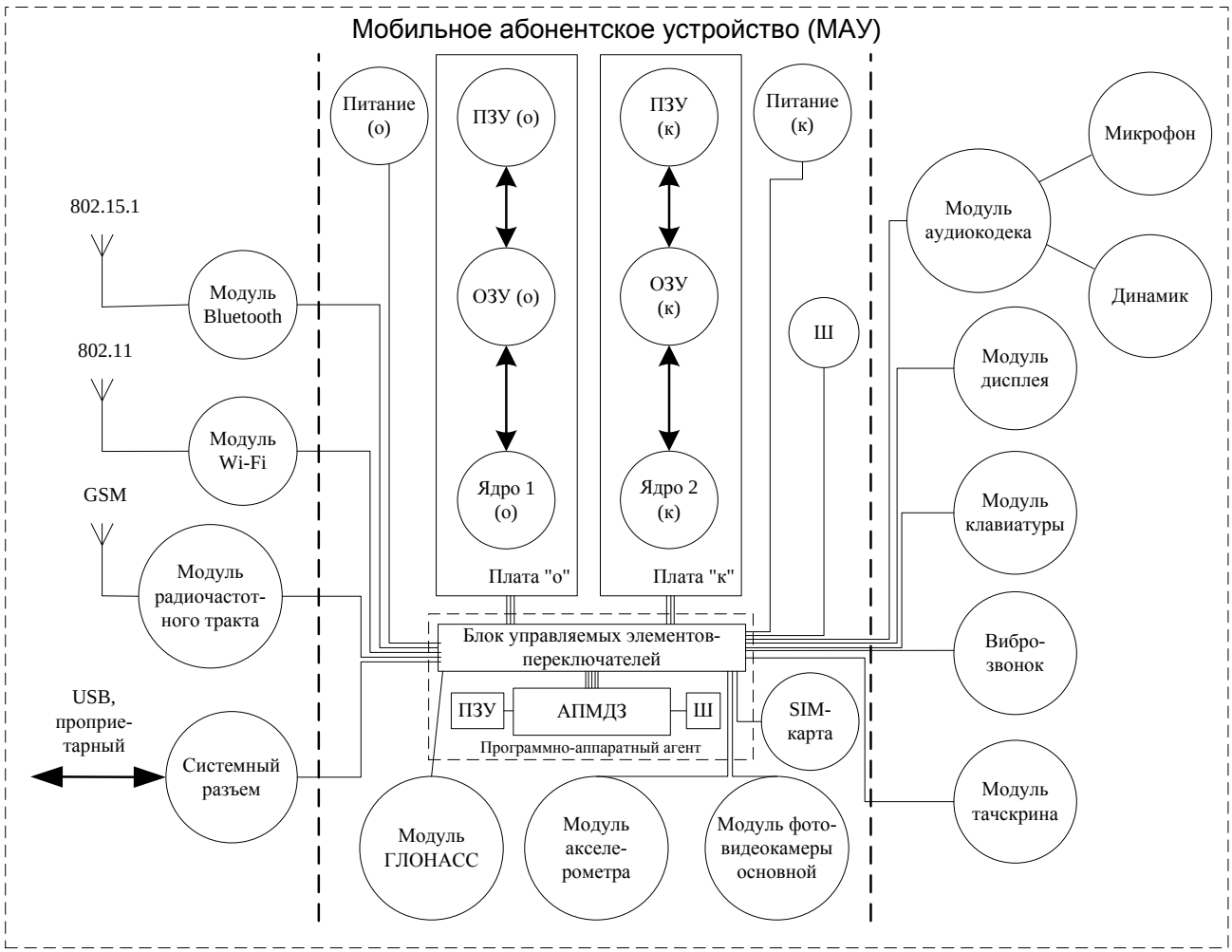


Рисунок 4.5 – Состав и структура мобильного абонентского устройства с дублированием функциональных блоков, отвечающих за обработку информации в сетях с разными требованиями по защищенности

Управляемая программно-аппаратная конфигурация МАУ определяет его состояние. Конфигурация МАУ в зависимости от его местоположения и других атрибутов доступа определяет возможности пользователя и МАУ по доступу к услугам корпоративных сетей с разными требованиями по защищенности и, соответственно, ограничения на использование тех или иных услуг и функциональных возможностей МАУ. Таким образом, система управления безопасностью МАУ позволяет согласовывать состояния МАУ с требованиями политики безопасности корпоративных сетей с разными уровнями защищенности, а также требованиями по качеству предоставляемых услуг.

4.1.1. Предложения по составу и структуре логической модели базы данных для хранения требований политики безопасности

Логическая модель отражает логические связи между элементами данных вне зависимости от их содержания и среде хранения, и строится в терминах информационных единиц, но без привязки к конкретной СУБД. Более того, логическая модель данных необязательно должна быть выражена средствами именно реляционной модели данных. Основным средством разработки логической модели данных в настоящий момент являются различные варианты ER-диаграмм. Одну и ту же ER-модель можно преобразовать как в реляционную модель данных, так и в модель данных для иерархических и сетевых СУБД, или в постреляционную модель данных.

Логическая модель базы данных, в которой возможно хранение совокупности требований политики безопасности МАУ в корпоративных сетях с разными требованиями по защищенности представлена на рисунке 4.6.

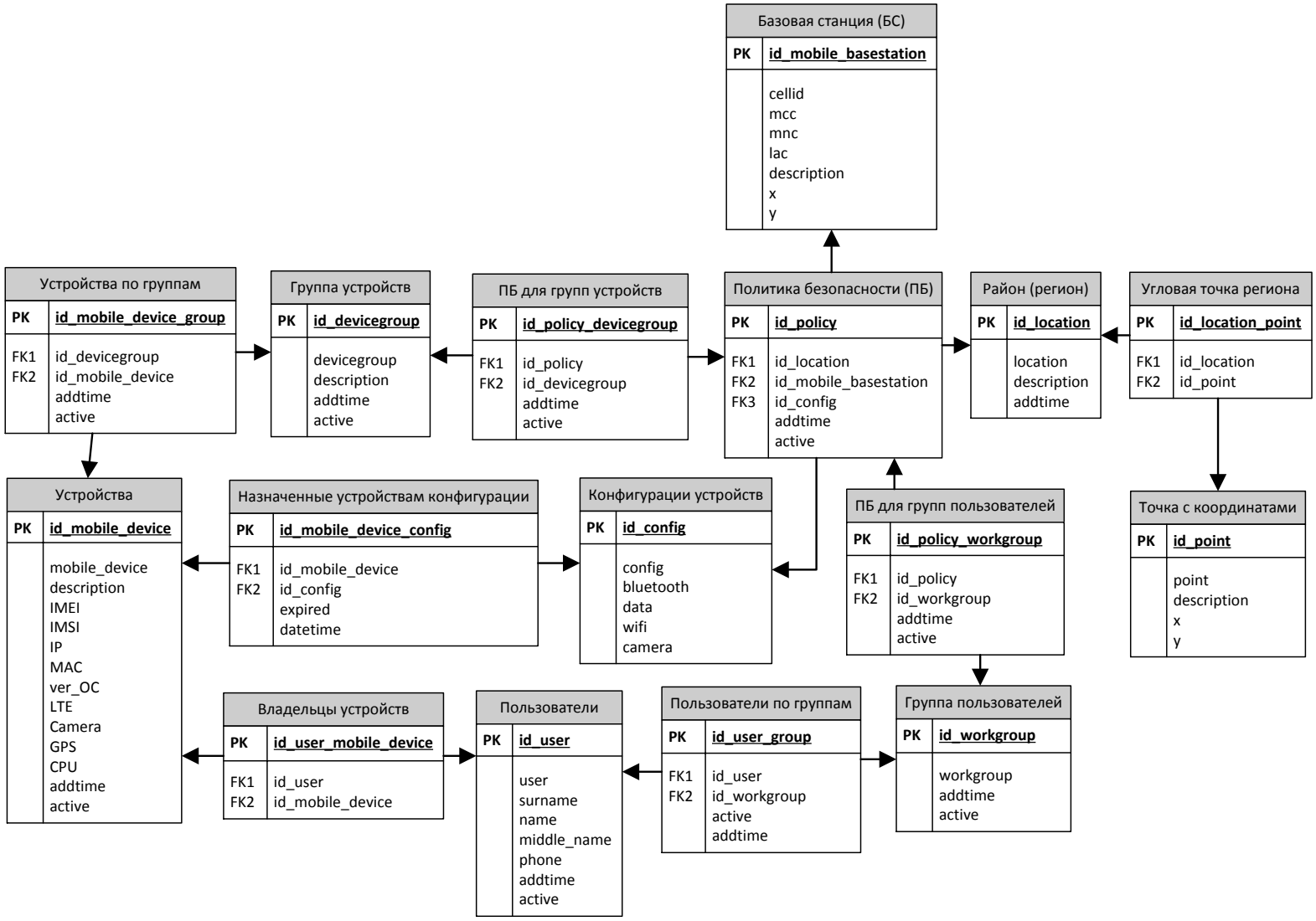


Рисунок 4.6 – Логическая схема структуры базы данных, хранящей требования политики безопасности мобильных абонентских устройств защищенной корпоративной сети

Для хранения требований политики безопасности МАУ необходимо наличие защищенной базы данных и системы управления базой данных (СУБД). Среди существующих сертифицированные систем криптографической защиты информации (СКЗИ) известны такие технические решения как "Крипто БД" компании "Алладин Р.Д." [36], представляющее собой СКЗИ для организаций, использующих СУБД Oracle, MS SQL, Tibero.

Логическая структура содержит следующие сущности: политика безопасности (ПБ); политика безопасности для группы пользователей; политика безопасности для группы устройств; устройства по группам; устройства; группа устройств; назначенные устройствам конфигурации; владельцы устройств; конфигурации устройств; пользователи; пользователи по группам; группа пользователей; базовая станция; район; угловая точка; точка с координатами.

На сервере необходимо использовать защищенную СУБД с соответствующим уровнем защищенности и сертификации, в которой имеет значение согласование и целостность данных. Согласование данных обеспечивается созданием таблиц, соответствующих сущностям логической модели базы данных.

4.1.2. Предложения по реализации защищенного канала управления между контроллером доступа и мобильным абонентским устройством

Известно, что управление должно обладать свойствами устойчивости, непрерывности, оперативности и скрытности. Для обеспечения данных свойств канал управления должен обладать дополнительными механизмами защиты. Поскольку между контроллером доступа и МАУ возможен канал управления только через БСПД, то возможны следующие варианты:

VPN-соединение в БСПД, например, на базе протокола HTTPS;

защищенные SMS-сообщения;

VPN-соединения в составе инкапсулированных данных протоколов низких уровней (канального, сетевого, транспортного).

Вариант построения защищенного канала управления между контроллером доступа МАУ на примере протокола HTTPS представлен на 4.7.

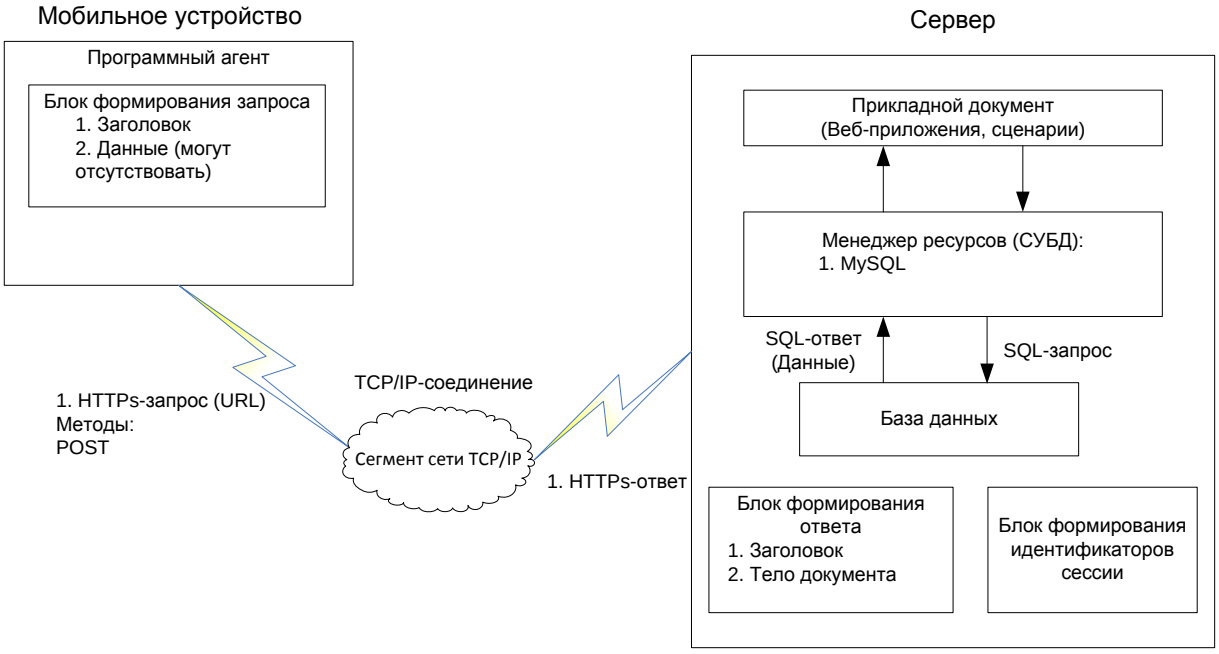
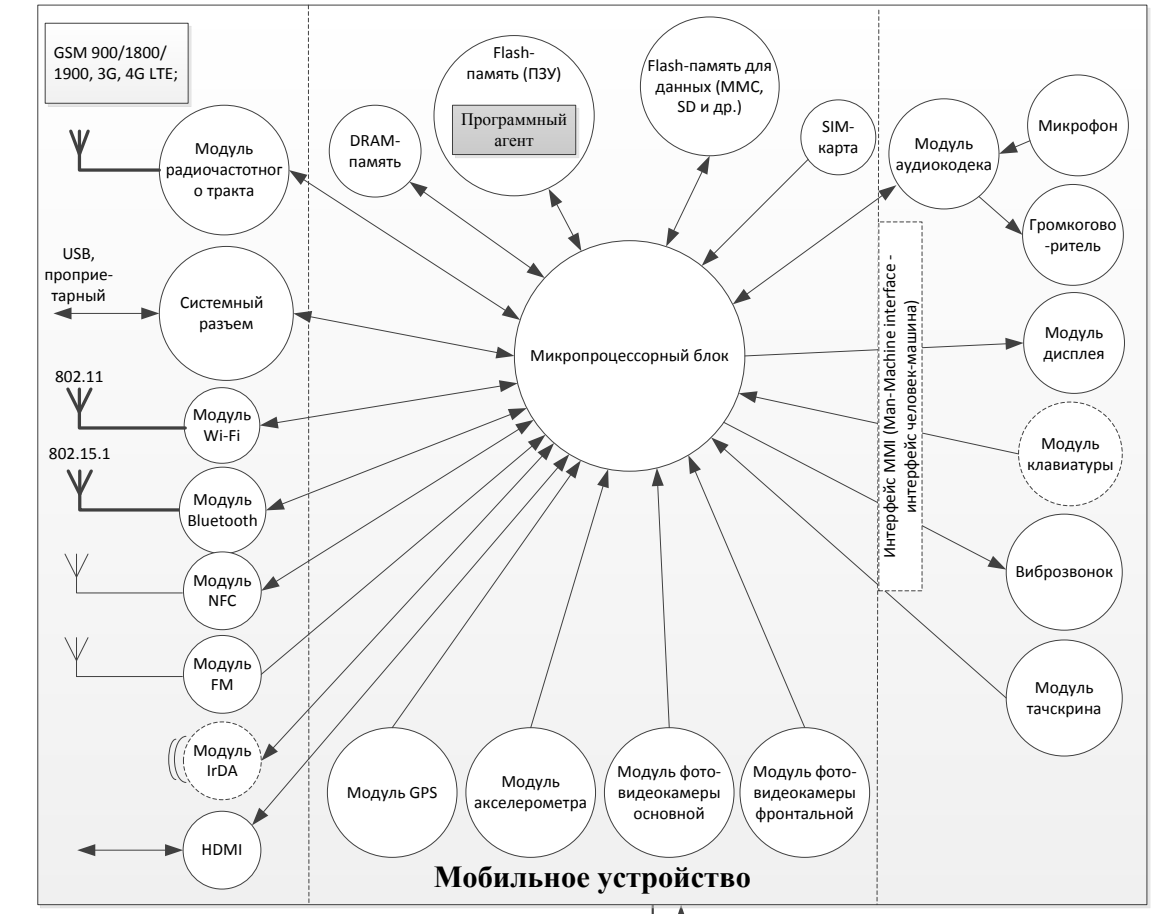


Рисунок 4.7 – Вариант построения защищенного канала управления на базе протокола HTTPS

Расширенная схема взаимодействия МАУ и контроллера доступа представлена на примере протокола HTTPS на рисунке 4.8. Целесообразно канал управления между мобильным устройством и удаленным сервером доступа реализовать защищенным с установлением VPN-канала. В случае если разглашение местоположения пользователя мобильного устройства критично, могут быть использованы протоколы, реализующие конфиденциальные распределенные вычисления, такие как "Забывчивая передача" [96] или "Передача данных на хранение" [95].

Необходимо отметить, что реализация защищенного канала управления на базе протокола прикладного уровня HTTPS имеет существенные недостатки в отношении устойчивости, оперативности, скрытности, надежности и разведзащищенности. Одним из вариантов решения данной проблемы может быть использо-

вание возможностей протоколов низкого уровня для реализации такого защищенного канала управления.



HTTP-запрос (атрибуты доступа):
1) данные о местоположении (CellID, геокоординаты);
2) ID устройства, ОС, прикладного ПО;
3) информация о процессах.
4) ...

HTTP-ответ (конфигурация МУ):
1) перечень разрешенных/запрещенных функций
2) перечень разрешенных/запрещенных приложений
3) ...

Политика безопасности

Контроллер управления мобильными устройствами

БД

Сервер удаленного доступа

Сведения о мобильных устройствах

Сведения о пользователях

Сведения о карте местности (помещениях)

Конфигурация	Местоположение	Атрибуты доступа			
		Время	ID УМУ	User	...
$CONF_0$	$\Gamma(L_O \vee L_{K1} \vee L_{K2})$	∞	∞	∞	...
$CONF_1$	L_O	∞	5,29,53,...	3,7,12,...	...
$CONF_2$	L_O	8^{00}-17^{30}	7,11,52,...	9,17,23,..	...
$CONF_3$	L_{K1}	∞	13,17,...	5,11,...	...
$CONF_4$	L_{K1}	16^{00}-17^{00}	17	5	...
$CONF_5$	L_{K2}	∞	13	1	...
$CONF_6$	L_{K2}	11^{00}-13^{00}	17,21	11,27	...

Рисунок 4.8 – Структурная схема, реализующая взаимосвязь мобильного устройства и удаленного сервера доступа мобильных устройств

На рисунках 4.8 представлен вариант реализации защищенного канала управления в составе MAC-подуровня канального уровня стека протоколов.

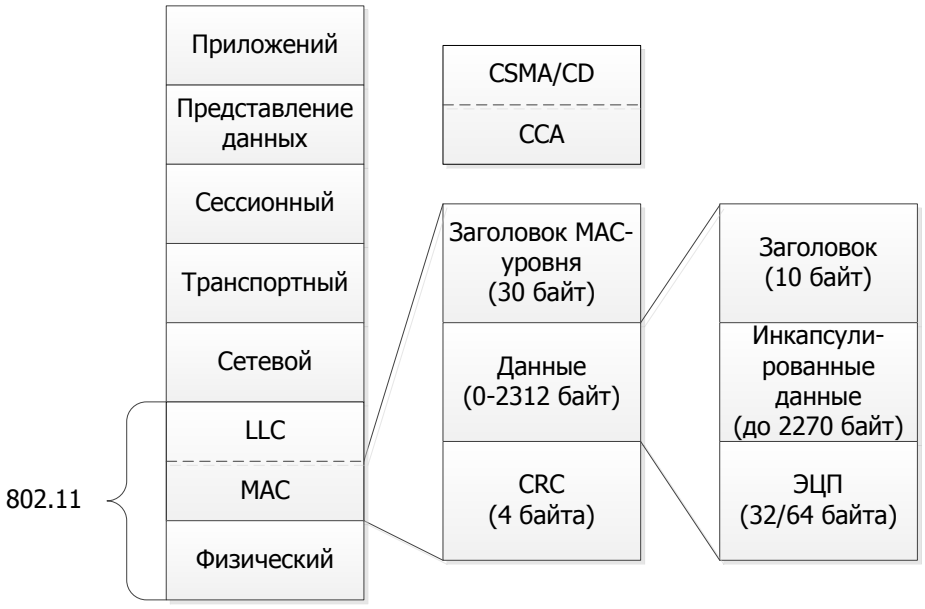


Рисунок 4.9 – Защищенный канал управления МАУ в составе инкапсулированных данных MAC-подуровня канального уровня 802.11

За счет использования инкапсулированных данных в составе пакета может передаваться зашифрованные сигналы управления. Вариант построения структуры данных в составе пакета инкапсулированных данных представлен на рисунке 4.10.

Обработка сигналов управления должна быть возложена на программно-аппаратный модуль в составе АПМДЗ МАУ либо на элементы программного кода драйверов интерфейсов беспроводной передачи данных.

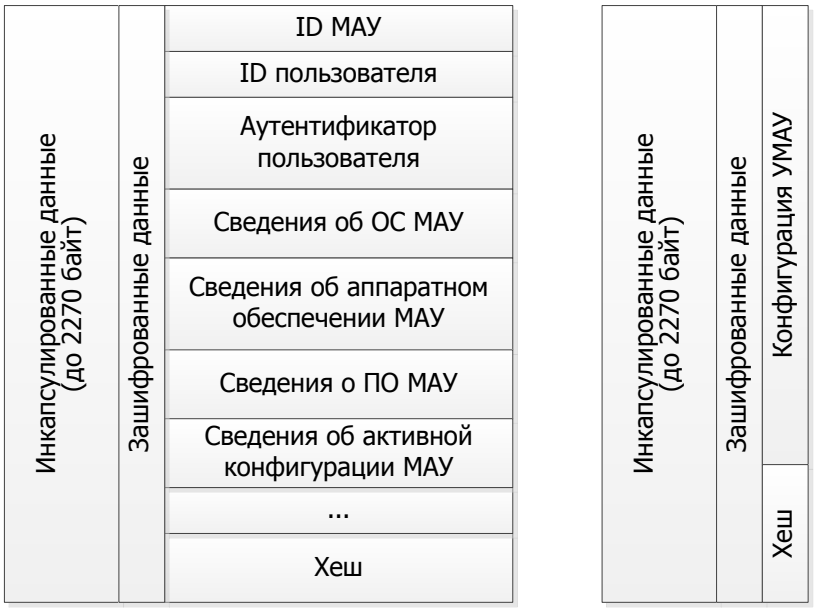


Рисунок 4.10 – Варианты реализации структуры данных:
а) при передаче атрибутов доступа контроллеру МАУ;
б) при передаче МАУ управляющего воздействия в виде конфигурации

4.2. Разработка рекомендаций по проектированию подсистемы определения местоположения в системе управления безопасностью мобильных абонентских устройств в корпоративных сетях с разными требованиями по защищенности

Эффективность подсистемы определения местоположения в системе управления безопасностью мобильных абонентских устройств в корпоративных сетях с разными требованиями по защищенности определяется ее параметрами, которые должны настраиваться в зависимости от условий эксплуатации. Для выбора оптимальных параметров алгоритмов определения местоположения была проведена группа экспериментов, результаты которых представлены в работе [43]. В качестве инструмента исследования в экспериментах использовалась разработанная имитационная модель [42, 43, 79]. Схема помещений, исследуемая в экспериментах, представлена на рисунке 2.9. Исходные данные, ограничения и допущения представлены на странице 57.

4.2.1. Рекомендации по оптимальному взаимному расположению точек доступа беспроводной сети в системе определения местоположения

Для метода трилатерации было исследовано влияние количества используемых точек доступа и их расположения на точность определения местоположения. Формальная постановка оптимизационной задачи имеет вид:

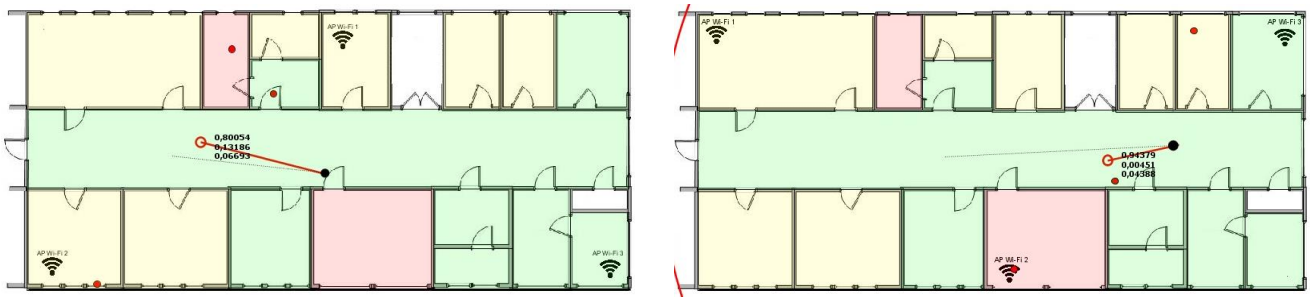
$$\begin{cases} e_L \to \min, \\ \text{var } AP_j = \left(x_j, y_j\right), j = \overline{1, N}_{AP}, \\ \text{var } N_{AP} = 3..5, \end{cases} \tag{4.1}$$

где e_L – ошибка определения местоположения, вычисляемая в соответствие с выражением (2.3), в котором $\left(\tilde{x}_{tr}, \tilde{y}_{tr}\right)$ – вычисленные методом трилатерации координаты местоположения МАУ, а $\left(\tilde{x}, \tilde{y}\right)$ – реальные координаты местоположения МАУ; N_{AP} точек доступа с заданными координатами $\left(x_j, y_j\right), j = \overline{1, N}_{AP}$.

Результаты экспериментов для трех точек доступа представлены в таблице 4.1, для четырех – в таблице 4.2 и для пяти – в таблице 4.3.

Таблица 4.1 – Статистические параметры ошибки определения местоположения для различного расположением трех точек доступа на карте помещений

№ карты расположения точек доступа	Выборочное среднее, м	Выборочное среднеквадратическое отклонение, м	Максимальное значение, м	Минимальное значение, м	Доверительный интервал для среднего
1	7,533	4,063	23,669	0,069	0,101
2	8,877	5,11	30,573	0,036	0,133
3	4,984	10,378	52,716	0,212	0,284
4	5,45	3,759	56,847	0,068	0,098
5	5,924	4,623	25,037	0,055	0,125
6	5,297	3,456	22,087	0,097	0,094
7	5,883	4,379	26,92	0,026	0,119
8	7,705	4,712	25,493	0,079	0,125
9	6,484	3,766	27,166	0,078	0,102
10	6,088	4,387	32,627	0,115	0,12
11	5,561	4,221	28,042	0,031	0,115
12	9,538	3,66	29,606	0,047	0,096
13	9,547	4,471	29,685	0,115	0,119
14	15,548	7,393	39,889	1,616	0,198



а) б)

Рисунок 4.1 – Схема оптимального расположения трех точек доступа на исследуемой схеме этажа с точки зрения минимальной ошибки определения местоположения: а) карта № 3, б) карта № 6

Таблица 4.2 – Статистические параметры ошибки определения местоположения для различного расположением четырех точек доступа на карте помещений

№ карты расположения точек доступа	Выборочное среднее, м	Выборочное среднеквадратическое отклонение, м	Максимальное значение, м	Минимальное значение, м	Доверительный интервал для среднего
1	5,592	3,43	20,495	0,023	0,078
2	5,305	3,351	26,896	0,054	0,089
3	6,499	4,167	20,79	0,024	0,112
4	5,024	2,89	21,372	0,037	0,078
5	4,904	3,213	19,442	0,05	0,087
6	5,132	3,271	22,431	0,09	0,088
7	4,967	3,341	21,898	0,121	0,089
8	5,806	3,447	23,277	0,072	0,09
9	8,505	3,057	24,891	0,096	0,078
10	15,467	7,591	38,175	1,496	0,201
11	5,742	3,484	18,007	0,041	0,091

Для четырех точек доступа наилучшая точность определения местоположения достигается при взаимном расположении точек доступа так, как показано на рисунке 4.2.

а) б)

Рисунок 4.2 – Схема оптимального расположения четырех точек доступа на исследуемой схеме этажа с точки зрения минимальной ошибки определения местоположения: а) карта № 5, б) карта № 7

Таблица 4.3 – Статистические параметры ошибки определения местоположения для различного расположением пяти точек доступа на карте помещений

№ карты расположения точек доступа	Выборочное среднее, м	Выборочное среднеквадратическое отклонение, м	Максимальное значение, м	Минимальное значение, м	Доверительный интервал для среднего
1	4,986	2,865	24,135	0,1	0,077
2	5,792	3,549	23,549	0,054	0,066
3	5,837	3,994	23,574	0,094	0,108
4	6,251	3,849	26,811	0,126	0,104
5	6,193	3,931	23,195	0,029	0,105
6	5,823	3,02	23,631	0,08	0,075
7	6,375	3,696	21,159	0,03	0,098

Для пяти точек доступа наилучшая точность определения местоположения достигается при взаимном расположении точек доступа так, как показано на рисунке 4.3.

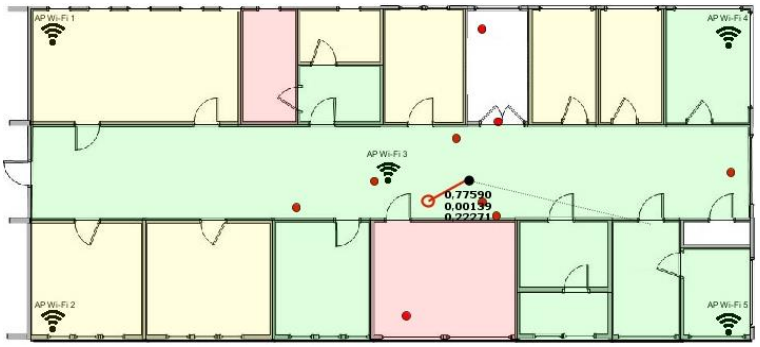


Рисунок 4.3 – Схема оптимального расположения пяти точек доступа на исследуемой схеме этажа с точки зрения минимальной ошибки определения

Эксперименты, проведенные в аналогичных условиях для методов k-ближайших соседей и байесовского подхода, показали, что наилучшая точность определения местоположения достигается при аналогичном расположении точек доступа как и для метода трилатерации.

4.2.2. Рекомендации по значениям параметров метода *k*-ближайших соседей в системе определения местоположения

В таблице 4.4 представлены результаты экспериментов, в которых исследовалась зависимость точности определения местоположения для метода k-ближайших соседей в зависимости от числа k.

Формальная постановка оптимизационной задачи имеет вид:

$$\begin{cases} e_L \to \min, \\ \operatorname{var} k = 1..10, \\ \operatorname{var}\left(x_i, y_i\right) \left| X^{N_{kNN}} = \left\langle \left\{ \left(x_i, y_i\right), \upsilon_i \right\}, P_{r_i}^{RSS} \right\rangle, i = \overline{1, N_{kNN}}, \right. \\ \operatorname{var} N_{kNN} \left| X^{N_{kNN}} = \left\langle \left\{ \left(x_i, y_i\right), \upsilon_i \right\}, P_{r_i}^{RSS} \right\rangle, i = \overline{1, N_{kNN}}, \right. \end{cases} \tag{4.2}$$

где e_L – ошибка определения местоположения, вычисляемая в соответствие с выражением (2.3), в котором $\left(\tilde{x}_{kNN}, \tilde{y}_{kNN}\right)$ – вычисленные методом k-ближайших соседей координаты местоположения МАУ, а $\left(\tilde{x}, \tilde{y}\right)$ – реальные координаты местоположения МАУ; k – число "соседей" в сигнальном пространстве; $\left(x_i, y_i\right)$ – координаты i-й точки карты сигнального пространства; υ_i – угол ориентации в пространстве МАУ; $P_{r_i}^{RSS}$ – уровень мощности принимаемого сигнала от МАУ; $i = \overline{1, N}_{kNN}$ – индекс точки измерений карты сигнального пространства, а N_{kNN} – их количество.

Эксперименты осуществлялись для пяти точек доступа и карты помещений, изображенных на рисунке 4.3.

Таблица 4.4 – Статистические параметры ошибки определения местоположения для метода k-ближайших соседей в зависимости от числа k

Значение числа k	Выборочное среднее, м	Выборочное среднеквадратическое отклонение, м	Максимальное значение, м	Минимальное значение, м	Доверительный интервал для среднего
1	4,225	2,848	30,415	0,024	0,078
2	3,529	2,387	22,187	0,04	0,065
3	3,617	2,561	30,47	0,007	0,069
4	3,254	2,128	22,169	0,079	0,057
5	3,261	2,164	19,499	0,01	0,054
6	3,185	1,994	19,923	0,098	0,055
7	3,221	2,283	21,627	0,055	0,061
8	3,289	2,284	21,931	0,011	0,062
9	3,147	2,028	19,336	0,009	0,054
10	4,477	2,565	21,428	0,034	0,067

Как видно из таблицы наилучшая точность определения местоположения достигалась при значениях $k=6$ и $k=9$.

На рисунке 4.11 представлен график зависимости выборочного среднего и среднеквадратического отклонения (СКО) для ошибки определения местоположения от числа "соседей".

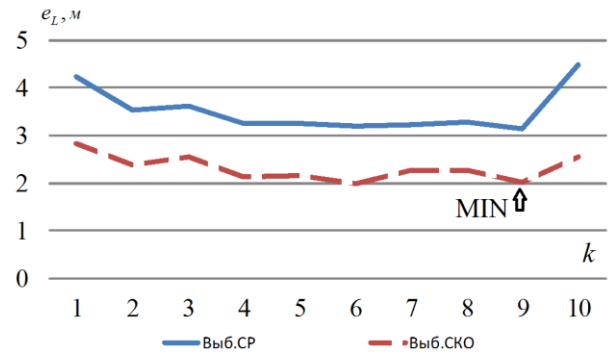


Рисунок 4.11 – График зависимости выборочного среднего и СКО для ошибки определения местоположения от числа "соседей"

Для значений числа учитываемых ближайших "соседей" $k=6$ и $k=9$ были проведены эксперименты с целью исследования влияния расположения точек измерений уровня сигнала на карте сигнального пространства. Расположение точек

измерений в имитационной модели выбиралось в виде сетки квадратов или прямоугольников, стороны которых определялись шагом сетки по горизонтали и вертикали. Например, шаг сетки карты сигнального пространства $h = 1,5x1,5$ означает ширину и длину прямоугольника сетки, равные 1,5 м. В таблице 4.5 представлены результаты данного эксперимента.

Таблица 4.5 – Статистические параметры ошибки определения местоположения для метода k-ближайших соседей в зависимости от шага сетки карты сигнального пространства

Шаг сетки карты h, м	Выборочное среднее, м	Выборочное среднеквадратическое отклонение, м	Максимальное значение, м	Минимальное значение, м	Доверительный интервал для среднего
$k = 6$					
0,5x0,5	3,27	2,33	22,995	0,073	0,064
1x1	3,185	1,994	19,923	0,098	0,055
1,5x1,5	3,162	2,072	22,075	0,003	0,056
2x2	3,067	2,058	22,306	0,007	0,051
2,5x2,5	3,36	2,079	14,773	0,043	0,053
3x3	3,484	2,205	17,341	0,023	0,06
$k = 9$					
0,5x0,5	3,18	2,021	18,224	0,035	0,037
1x1	3,147	2,028	19,336	0,009	0,054
1,5x1,5	2,603	1,702	21,212	0,023	0,046
2x2	3,104	2,181	22,769	0,034	0,06
2,5x2,5	3,291	1,894	14,394	0,072	0,049
3x3	4,472	2,393	14,033	0,067	0,065

График зависимости статистических параметров ошибки определения местоположения от шага сетки измерений карты сигнального пространства представлен на рисунке 4.12.

Из таблицы и рисунка видно, что наилучшая точность определения местоположения для метода k-ближайших соседей достигается при значениях шага сетки измерений карты сигнального пространства равного $h = 1,5x1,5$ м и $h = 2,0x2,0$ м как при $k = 6$, так и $k = 9$.

Наилучшие значения статистических параметров ошибки определения местоположения в проведенных экспериментах были достигнуты при значениях $k = 9$ и $h = 1{,}5x1{,}5$ м.

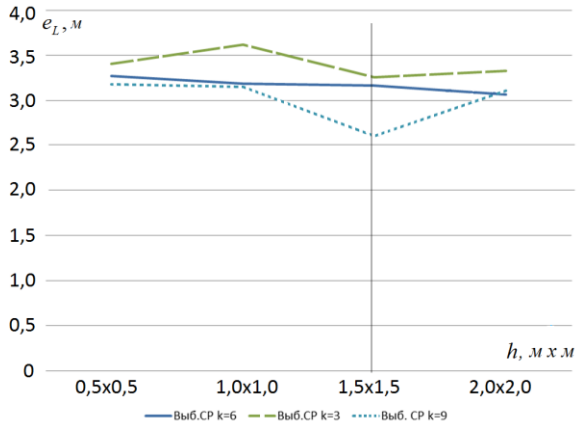


Рисунок 4.12 – График зависимости ошибки определения местоположения от шага сетки измерений карты сигнального пространства

4.2.3. Рекомендации по значениям параметров метода на основе байесовского подхода в системе определения местоположения

Для исследования эффективности подсистемы определения местоположения на основе байесовского подхода были проведены эксперименты с целью выбора оптимальных параметров для

– числа "соседей" – количества наиболее вероятных состояний, учитываемых при вычислении местоположения;

– расположения точек измерений на карте сигнального пространства;

– количество измерений в каждой точке карты измерений при формировании статистики распределения вероятностей уровней мощности сигнала МАУ.

Формальная постановка оптимизационной задачи имеет вид:

$$\begin{cases} e_L \to \min, \\ \operatorname{var} k = 1..10, \\ \operatorname{var}\left(x_i, y_i\right) \left| X^{N_{HMM}} \right. = \left\langle \left(x_i, y_i\right), P_{r_i}\left[\lambda_i / \left(x_i, y_i\right)\right] \right\rangle, i = \overline{1, N_{HMM}}, \\ \operatorname{var} N_{HMM} \left| X^{N_{HMM}} \right. = \left\langle \left(x_i, y_i\right), P_{r_i}\left[\lambda_i / \left(x_i, y_i\right)\right] \right\rangle, i = \overline{1, N_{HMM}}, \end{cases} \tag{4.3}$$

где e_L – ошибка определения местоположения, вычисляемая в соответствие с выражением (2.3), в котором $(\tilde{x}_{HMM}, \tilde{y}_{HMM})$ – вычисленные методом на основе байесовского подхода координаты местоположения МАУ, а $(\tilde{x}, \tilde{y})$ – реальные координаты местоположения МАУ; k – число учитываемых наиболее вероятных состояний; (x_i, y_i) – координаты i-й точки карты сигнального пространства; $P_{r_i}\left[\lambda_i / (x_i, y_i)\right]$ – условная вероятность получения измерений сигнала передатчика МАУ со статистическим распределением λ_i в точке с координатами (x_i, y_i); N_{HMM} – количество точек сигнального пространства обучающей выборки.

В таблице 4.6 представлены результаты эксперимента, в котором исследовалась зависимость статистических параметров ошибки определения местоположения от числа "соседей" – количества наиболее вероятных состояний, учитываемых при вычислении местоположения, на основе байесовского подхода.

Таблица 4.6 – Статистические параметры ошибки определения местоположения для метода на основе байесовского подхода в зависимости от числа k

Значение числа k	Выборочное среднее, м	Выборочное среднеквадратическое отклонение, м	Максимальное значение, м	Минимальное значение, м	Доверительный интервал для среднего
1	3,86	2,309	16,367	0,124	0,063
2	3,376	2,076	13,538	0,082	0,056
3	2,445	1,448	9,764	0,024	0,039
4	2,512	1,616	11,514	0,07	0,043
5	2,466	1,705	11,458	0,033	0,042
6	2,689	1,769	12,948	0,039	0,047
7	2,641	1,84	11,8	0,018	0,05
8	3,195	2,084	10,996	0,034	0,056
9	2,62	1,809	11,17	0,02	0,041
10	2,651	1,812	11,246	0,01	0,049

График зависимости статистических параметров ошибки определения местоположения от числа "соседей" – количества наиболее вероятных состояний, учитываемых при вычислении местоположения, представлен на рисунке 4.13.

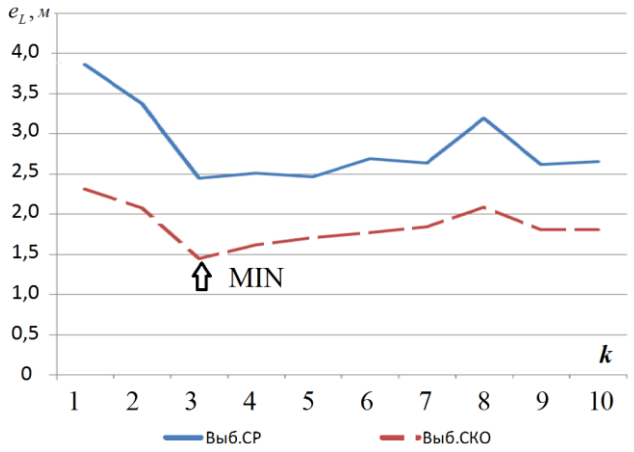


Рисунок 4.13 – График зависимости выборочного среднего и СКО для ошибки определения местоположения от количества наиболее вероятных состояний

Из таблицы и рисунка видно, что наилучшая точность определения местоположения для байесовского подхода достигается при значении $k = 3$.

В таблице 4.7 представлены результаты эксперимента, в котором исследовалась зависимость статистических параметров ошибки определения местоположения от шага сетки карты сигнального пространства для метода на основе байесовского подхода.

График зависимости статистических параметров ошибки определения местоположения от шага сетки измерений карты сигнального пространства представлен на рисунке 4.14.

Таблица 4.7 – Статистические параметры ошибки определения местоположения для метода на основе байесовского подхода в зависимости от шага сетки карты сигнального пространства

Шаг сетки карты h, м	Выборочное среднее, м	Выборочное среднеквадратическое отклонение, м	Максимальное значение, м	Минимальное значение, м	Доверительный интервал для среднего
0,5x0,5	2,669	1,662	12,333	0,025	0,044
1x1	2,828	1,747	14,438	0,041	0,044
1,5x1,5	2,728	1,788	11,915	0,054	0,047
2x2	2,662	1,657	11,419	0,03	0,045
2,5x2,5	3,304	2,149	13,44	0,05	0,058
3x3	3,703	2,394	14,505	0,076	0,064

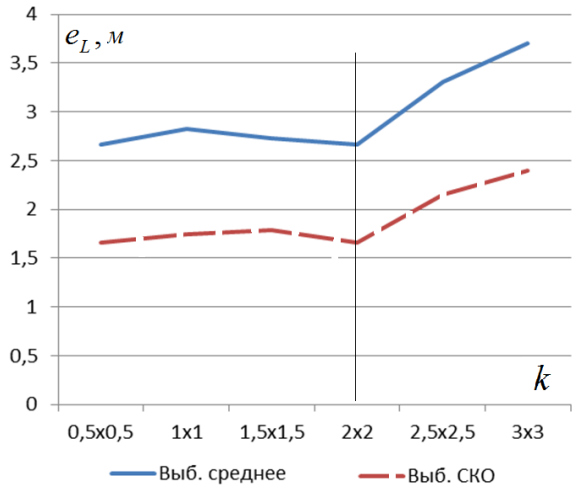


Рисунок 4.14 – График зависимости выборочного среднего и СКО для ошибки определения местоположения от шага сетки измерений карты сигнального пространства

Из таблицы и рисунка видно, что наилучшая точность определения местоположения для метода на основе байесовского подхода достигается при значениях шага сетки измерений карты сигнального пространства равного $h = 1{,}5x1{,}5$ м и $h = 2{,}0x2{,}0$ м. Таким образом, результаты для данного метода совпадают с аналогичным экспериментом для метода k-ближайших соседей.

В таблице 4.8 и на рисунке 4.15 представлены результаты эксперимента, в котором исследовалась зависимость статистических параметров ошибки определения местоположения от количества измерений M в каждой точке карты измерений при формировании статистики распределения вероятностей уровней мощности сигнала МАУ для метода на основе байесовского подхода.

Из таблицы и рисунка видно, что наилучшая точность определения местоположения для метода на основе байесовского подхода достигается при значениях количества измерений равного $M = 30$, при этом близкие значения для выборочного среднего ошибки определения местоположения получены для $M = 110$.

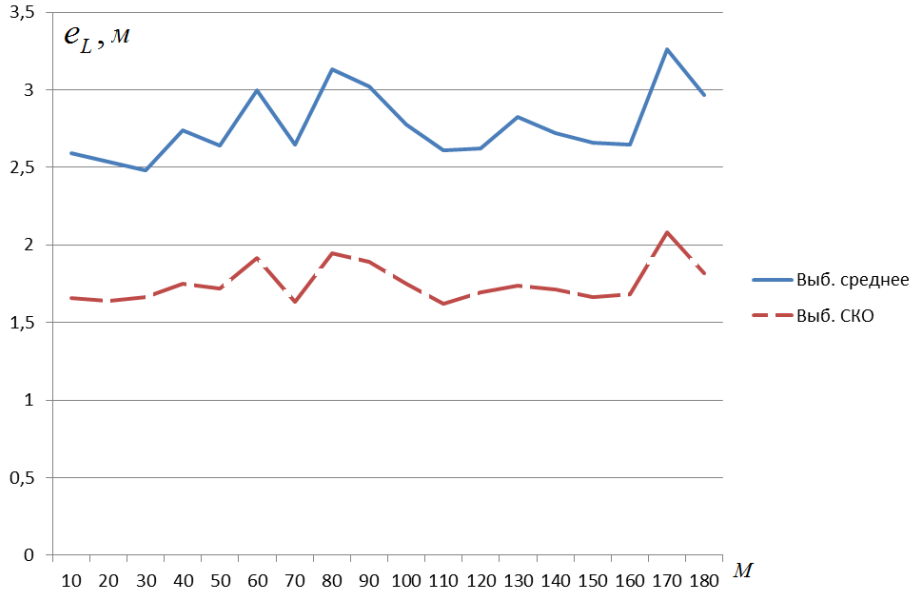


Рисунок 4.15 – График зависимости ошибки определения местоположения от количества измерений в каждой точке карты измерений при формировании статистики распределения вероятностей уровней мощности сигнала МАУ

Таблица 4.8 – Статистические параметры ошибки определения местоположения для метода на основе байесовского подхода в зависимости от количества измерений M в каждой точке карты измерений

Количество измерений M	Выборочное среднее, м.	Выборочное среднеквадратическое отклонение, м.	Максимальное значение, м.	Минимальное значение, м.	Доверительный интервал для среднего
10	2,59	1,66	10,855	0,031	0,045
20	2,537	1,638	12,393	0,012	0,044
30	2,481	1,661	12,596	0,025	0,045
40	2,739	1,751	11,709	0,019	0,047
50	2,642	1,72	11,966	0,063	0,045
60	2,997	1,913	13,744	0,053	0,052
70	2,649	1,632	11,509	0,026	0,044
80	3,131	1,949	12,307	0,048	0,052
90	3,023	1,893	12,842	0,031	0,051
100	2,778	1,75	11,938	0,051	0,048
110	2,61	1,618	12,347	0,005	0,043
120	2,623	1,695	11,726	0,022	0,046
130	2,822	1,74	12,191	0,038	0,047
140	2,722	1,712	12,316	0,055	0,046

4.3. Оценка эффективности системы управления безопасностью мобильных абонентских устройств в корпоративных сетях

Для выработки предложений по применению разработанной системы управления безопасностью МАУ необходимо произвести расчет оценок частных показателей эффективности, характеризующих процесс функционирования данной системы. Одной из ключевых подсистем в работе системы управления безопасностью МАУ является подсистема определения местоположения, реализованная с использованием технологий на базе методов трилатерации, k-ближайших соседей и байесовского подхода, а также предложенного подхода по повышению достоверности определения местоположения МАУ.

4.3.1. Расчет оценки времени, необходимого для смены конфигурации мобильного абонентского устройства

В процессе движения пользователя с МАУ неизбежно возникают ситуации, когда меняются атрибуты доступа и в том числе уровень защищенности помещений, в которых находится мобильный пользователь. Атрибуты доступа и политика безопасности определяют требования к конфигурации МАУ при текущих условиях доступа. Для мобильных пользователей время смены конфигурации МАУ в некоторых ситуациях является важным показателем качества.

Процесс смены конфигурации МАУ осуществляется в несколько этапов:

1. Измерение уровня сигнала МАУ на точках доступа беспроводной сети передачи данных (T_{RSS}).

2. Определение местоположения МАУ (T_{LOC}).

3. Отправка атрибутов доступа (запроса на доступ к услугам) с МАУ (T_{REQ}).

4. Обработка запроса с учетом параметров политики безопасности (T_{POLICY}).

5. Формирование и отправка управляющей команды на смену конфигурации МАУ (T_{RESP}).

6. Прием и обработка управляющей команды на стороне МАУ, применение новой конфигурации (T_{CONF}).

Таким образом, оценка общего времени, необходимого для смены конфигурации МАУ, может быть представлена в виде

$$T_{RECONF} = T_{RSS} + T_{LOC} + T_{REQ} + T_{POLICY} + T_{RESP} + T_{CONF}. \quad (4.4)$$

Расчет времени, необходимого на каждом этапе, осуществим для наиболее распространенного стандарта беспроводной передачи данных – IEEE 802.11 [117] при следующих ограничениях и допущениях:

– доступ к беспроводной сети передачи данных установлен, мобильное устройство прошло аутентификацию и находится в зоне действия доверенной беспроводной сети передачи данных;

– расчет временных параметров производится на наихудший случай.

В соответствие со стандартом IEEE 802.11 передача пакета данных на канальном уровне, обладающем идентификационной информацией о передатчике осуществляется в 4 этапа. Данные этапы представлены на рисунке

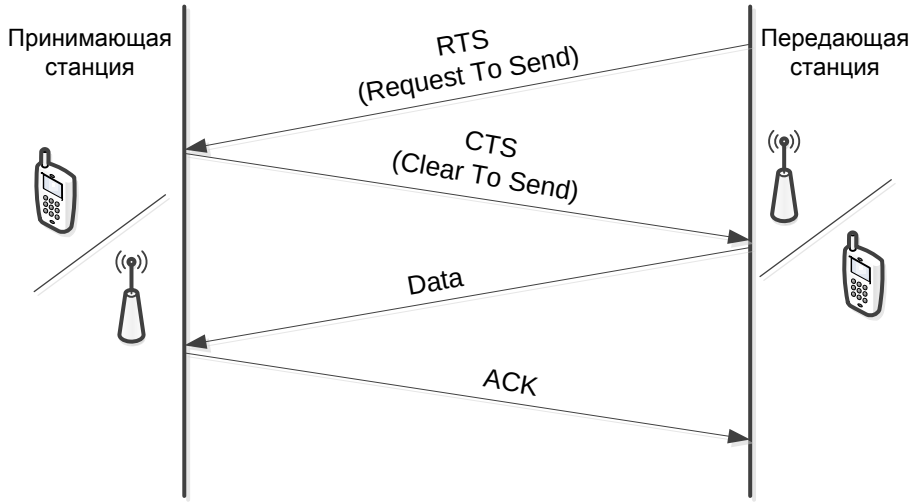


Рисунок 4.16 – Четырехэтапный протокол передачи данных, реализующий метод коллективного доступа к среде с минимизацией вероятности возникновения столкновений

В стандарте IEEE 802.11 используется метод коллективного доступа с обнаружением несущей и избеганием коллизий (Carrier Sense Multiple Access / Collision Avoidance, CSMA/CA). Перед началом передачи данных осуществляется выбор свободного канала на основе алгоритма оценки чистоты канала (Channel Clearance Algorithm, CCA). В основе данного алгоритма лежит измерение энергии сигнала на антенне и мощности принятого сигнала (Received Signal Strength Indicator, RSSI). Если мощность принятого сигнала ниже заданного порога, то канал объявляется свободным и MAC-уровень получает статус CTS (Clear To Send).

Перед началом передачи данных, МАУ отправляет сообщение RTS (Ready To Send), содержащее информацию о готовности отправки данных, адресате и продолжительности передачи. Если приемная станция (точка доступа) отвечает посылкой сигнала CTS, то МАУ начинает передачу данных. По завершении передачи данных точка доступа возвращает кадр ACK, подтверждающий безошибочный прием.

Максимальная дальность действия беспроводной сети определяется множеством параметров и в первую очередь мощностью передатчика, чувствительностью приемника и наличием препятствий. Расчет времени передачи сигнала от передатчика к источнику в условиях здания произведем для дальности в $l = 100$ м. Тогда четырехэтапная передача данных будет осуществляться за время, равное

$$t_{data} \approx \frac{4 \cdot l}{c} = \frac{4 \cdot 100}{299\,792\,458} = 1{,}334256 \cdot 10^{-6}\ \text{с}. \qquad (4.5)$$

Соответственно, передача пакета данных с идентифицирующей МАУ информацией будет осуществляться за время $T_{RSS} = t_{data}$.

Исходя из тех же соображений, осуществляется расчет значений T_{REQ} и T_{RESP}. При этом необходимо учесть, что максимальный размер блока данных, предусмотренный спецификацией пакетирования данных, предусматривает блок данных до 2048 байт, рекомендуя при этом использовать пакеты длиной 1500 и 2048 байт. Поскольку в запросе на доступ содержатся сведения об атрибутах доступа и запрашиваемой услуге, а в ответе на запрос – информация о назначаемой

конфигурации, то размер передаваемых данных может превышать максимальный размер пакета, поэтому для значений T_{REQ} и T_{RESP} предусмотрим 10-кратное превышение максимального размера пакета. Тогда с учетом (4.5) получим:

$$T_{REQ} \approx T_{RESQ} \approx 10 \cdot t_{data} = 1{,}334256 \cdot 10^{-5}\ \text{с}.$$

Значение T_{LOC} определяется временем, необходимым для получения данных об уровне сигнала МАУ точками доступа, в зоне действия которых, находится данное устройство, а также временем работы алгоритма определения местоположения МАУ и уровня защищенности помещения, в котором оно находится.

Значения T_{LOC}, T_{POLICY}, T_{CONF} определяются быстродействием программно-аппаратной составляющей системы управления МАУ.

В процессе имитационного моделирования и функционирования разработанных программ для ЭВМ [76, 77, 79] были получены следующие результаты: $T_{LOC} \approx 2{,}92 \cdot 10^{-3}$ с, $T_{POLICY} \approx 0{,}71 \cdot 10^{-3}$ с, $T_{CONF} \approx 1{,}12 \cdot 10^{-3}$ с.

Исходя из полученных оценок времени выполнения процедур и выражения (4.4) получим оценку значения времени, необходимого для смены конфигурации мобильного устройства:

$$\begin{aligned} T_{RECONF} &= T_{RSS} + T_{LOC} + T_{REQ} + T_{POLICY} + T_{RESP} + T_{CONF} \approx \\ &\approx 0{,}001334256 \cdot 10^{-3} + 2{,}92 \cdot 10^{-3} + 0{,}01334256 \cdot 10^{-3} + 0{,}71 \cdot 10^{-3} + \\ &+ 0{,}01334256 \cdot 10^{-3} + 1{,}12 \cdot 10^{-3} = 4{,}778019376 \cdot 10^{-3}\ \text{с} \approx 4{,}778\ \text{мс} \end{aligned}$$

Полученная оценка времени, необходимого для смены конфигурации МАУ в $4{,}778$ мс позволяет сделать вывод, что при данных ограничениях и допущениях время переконфигурации МАУ не превышает заданный порог и не снижает уровень защищенности при движении мобильного пользователя.

Данные расчеты не учитывают частоту опроса доверенных точек доступа, находящихся в радиусе их зоны действия МАУ, и соответственно не учитывают частоту получения оценок уровня мощности сигнала МАУ. Значения измерений уровня сигнала МАУ являются критичными, поскольку являются исходными данными для подсистемы определения местоположения МАУ. Поэтому при разработке программного обеспечения и драйверов для точек доступа и беспровод-

ного адаптера МАУ необходимо учитывать данные соображения и использовать частоту опроса доступных МАУ соизмеримую с полученной оценкой времени конфигурации.

Для оценивания зависимости времени переконфиграции МАУ от числа испытаний в методе Монте-Карло был проведен эксперимент, результаты которого представлены на рисунке 4.17. Из анализа данных эксперимента видно, что для текущих условий при числе испытаний в численном методе Монте-Карло $M < 5000$ время переконфигурации МАУ находится в пределах допустимых значений. Также из анализа графика видно, что зависимость обладает экспоненциальным ростом сложности. Данный факт предъявляет повышенные требования к производительности оборудования системы управления доступом и условию ее эксплуатирования.

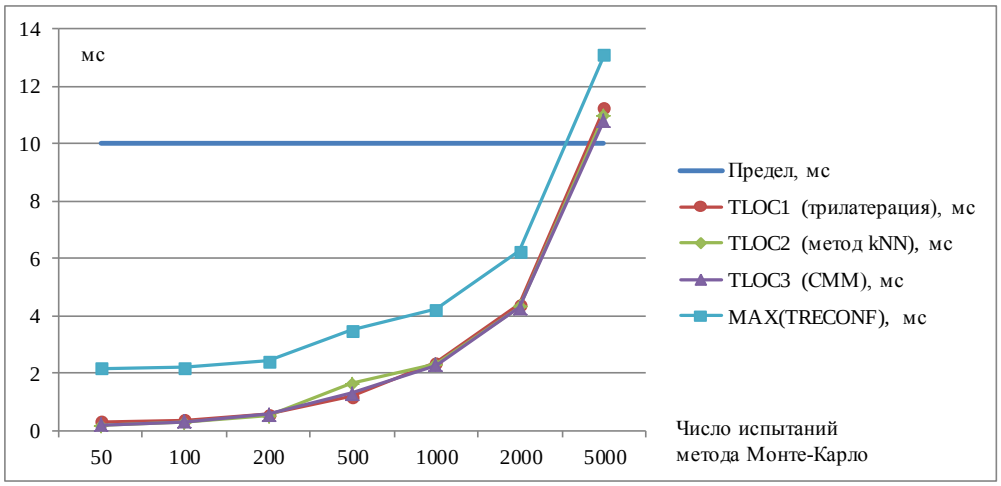


Рисунок 4.17 – График зависимости времени переконфиграции МАУ от числа испытаний в методе Монте-Карло

На основании полученных значений может быть получена оценка вероятности сохранения конфиденциальности информации при доступе к услугам сетей с разными требованиями по защищенности согласно принятой системе показателей эффективности. Вероятность сохранения конфиденциальности информации предложено оценивать с помощью выражения (1.10), при этом принято, что вероятность преодоления системы защиты $P_{\text{Пр3}} \to 0$. Таким образом, при условии

$CONF \subset CONF^{доп}$, принятых ограничениях и допущениях ($P_{Прз} \to 0$), а также полученной оценки времени переконфигурации $T_{RECONF} = 4{,}778 \cdot 10^{-3}$ с, находящейся в пределах заданных заказчиком значений $T_{RECONF}^{доп} = 10^{-2}$ с, можно сделать вывод о том, что $P_{СК}\left(T_{RECONF}\right) \to 1$.

4.3.2. Расчет вероятности угрозы нарушения конфиденциальности информации за счет формирования некорректной конфигурации мобильного абонентского устройства

Формирование некорректной конфигурации и, соответственно, профиля защиты МАУ возможно вследствие неправильных настроек политики безопасности, а также неточного определения уровня защищенности помещения, в котором находится пользователь МАУ – возникновении ошибок 2-го рода. Первый случай неправильных настроек политики безопасности выносится за рамки рассмотрения данной работы, поэтому для вычисления оценки вероятности утечки информации за счет некорректной конфигурации и профиля защиты МАУ будет использоваться значение ошибки 2-го рода при определения уровня защищенности помещения, в котором находится пользователь МАУ.

Результаты исследования эффективности определения уровня защищенности помещения численным методом Монте-Карло при использовании различных технологий определения местоположения представлены в таблице 4.9. В таблице: П – прототип, С – разработанная система.

Результаты получены при оптимальных параметрах подсистемы определения местоположения МАУ, выявленные в процессе предварительного имитационного моделирования.

Как видно из анализа таблицы, вне зависимости от технологии определения местоположения оценка эффективности определения уровня защищенности в виде ошибки 2-го рода не превышает 1 % при заданном критерии принятия решения. Однако при данном критерии высокие значения имеет ошибка 1-го рода.

Графическая иллюстрация результатов имитационного моделирования представлена на рисунке 4.18.

Таблица 4.9 – Результаты исследования эффективности определения уровня защищенности численным методом Монте-Карло при использовании различных технологий определения местоположения и их комбинаций

№ п/п	Метод	Правильно		Ошибка 1-го рода		Ошибка 2-го рода	
		П	С	П	С	П	С
1.	Трилатерация	72,104	16,779	5,325	81,614	22,569	0,906
2.	k-ближайших соседей	76,881	14,333	9,247	84,447	13,871	0,919
3.	Байесовский подход	75,572	11,153	17,726	87,786	6,700	0,906
4.	1,2	71,934	6,255	8,982	93,225	19,083	0,519
5.	1,3	72,069	8,349	9,615	90,997	18,314	0,653
6.	2,3	75,728	15,055	10,44	82,88	13,831	2,064
7.	1,2,3	76,327	8,727	7,938	90,235	15,786	1,037

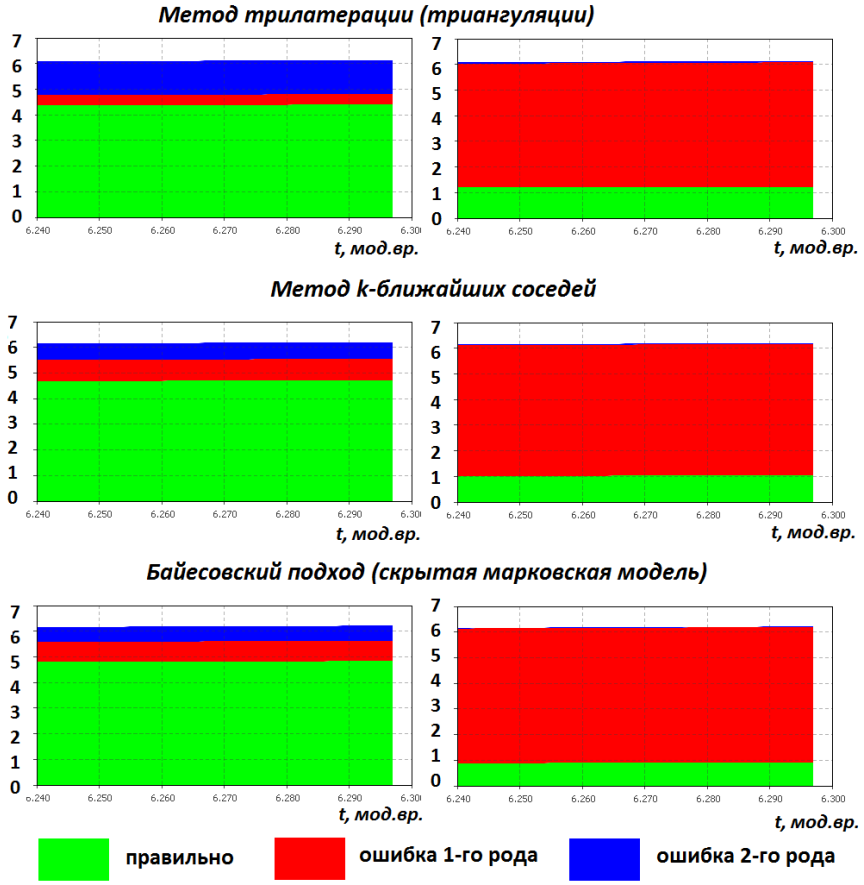


Рисунок 4.18 – Результаты имитационного моделирования исследования эффективности определения уровня защищенности помещения численным методом Монте-Карло

Из анализа таблицы 4.9 и результатов имитационного моделирования на рисунке 4.18 видно, что оценка вероятности утечки информации за счет формирования некорректной конфигурации мобильного устройств $P\left(CONF \subset CONF^{\text{доп}}\right) = P\left[P_{\beta}\left(\tilde{L}_{Room} > L_{Room}\right) \le P_{\beta}^{\text{доп}} \right]$ при $P_{\beta}^{\text{доп}} = 0,01$ находится в пределах допустимых значений.

4.3.3. Расчет ресурсоемкости технических решений по предоставлению услуг для прототипа и предложенной системы управления безопасностью мобильных абонентских устройств

Ресурсоемкость процесса защиты информации [7] при эксплуатации МАУ может быть определена, исходя из выражения:

$$\begin{aligned} RES_{\text{ЗИМАУ}} &= K_{\text{ИВР}} \cdot C_{\text{ВР}} + K_{\text{ИТР}} \cdot C_{\text{ТР}} + K_{\text{ИСУ}} \cdot C_{\text{СУМАУ}} + \\ &+ K_{\text{ИСОМ}} \cdot C_{\text{СОМ}} + \left(\sum_{i=1}^{N_{\text{МАУ}}} C_{\text{МАУ}_i} \right) \cdot N_{\text{Польз}} \end{aligned}, \qquad (4.6)$$

где $K_{\text{ИВР}}$ – коэффициент использования вычислительных ресурсов; $C_{\text{ВР}}$ – стоимость вычислительных ресурсов; $K_{\text{ИТР}}$ – коэффициент использования телекоммуникационных ресурсов; $C_{\text{ТР}}$ – стоимость телекоммуникационных ресурсов; $K_{\text{ИСУ}}$ – коэффициент использования системы управления безопасностью МАУ; $C_{\text{СУМАУ}}$ – стоимость системы управления безопасностью МАУ; $K_{\text{ИСОМ}}$ – коэффициент использования системы определения местоположения МАУ; $C_{\text{СОМ}}$ – стоимость системы определения местоположения МАУ ; $C_{\text{МАУ}_i}$ – стоимость i-го МАУ, необходимого для доступа к услугам; $N_{\text{МАУ}}$ – количеством МАУ, необходимых для доступа ко всему перечню услуг; $N_{\text{Польз}}$ – количество пользователей МАУ.

Анализ открытых источников информации и средней стоимости защищенных мобильных технических решений, а также средняя стоимость проектирования и развертывания защищенной БСПД и серверной составляющей, выполняющей функции ЦУИБ, позволил выявить зависимость между затратами и количе-

ством пользователей МАУ для прототипа и разработанной системы управления безопасностью МАУ. График данной зависимости представлен на рисунке 4.19.

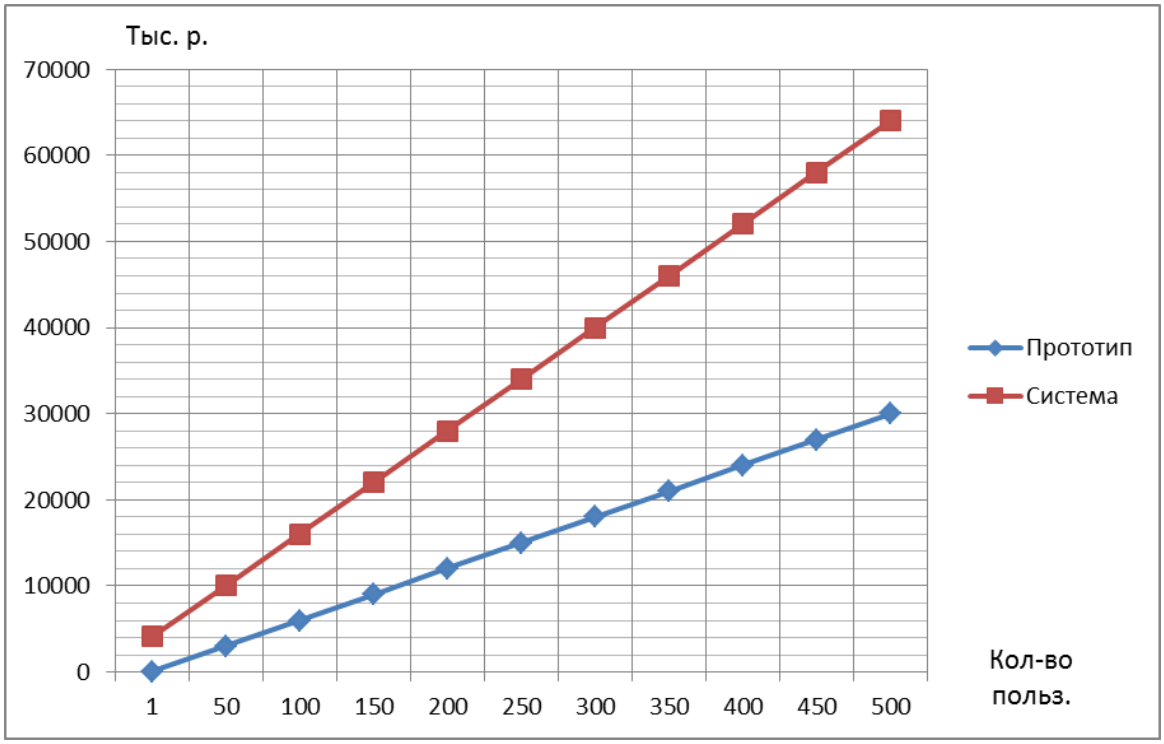


Рисунок 4.19 – График зависимости ресурсоемкости технических решений по предоставлению услуг для прототипа и предложенной системы управления безопасностью МАУ от количества пользователей МАУ

Анализа рисунка показывает, что изначально ресурсоемкость предлагаемого технического решения превышает аналогичный показатель для прототипа на величину затрат на систему управления и систему определения местоположения $K_{\text{ИСУ}} \cdot C_{\text{СУМАУ}} + K_{\text{ИСОМ}} \cdot C_{\text{СОМ}}$, при этом стоимость управляемого МАУ также не позволяет получить экономический эффект вне зависимости от количества пользователей МАУ.

4.3.4. Расчет своевременности доступа к услугам и информации с использованием мобильных абонентских устройств

Своевременность обработки запросов на доступ к услугам оценивалась в соответствии со стандартом [18]. Вероятность предоставления информации или услуг $P_{ДИ}(T_{ДИ})$ за заданное время $T_{ДИ}^{зад}$ будет определяться с помощью табулированной неполной гамма-функции [18]:

$$P_{ДИ}^{У}(T_{ДИ}) = \int_0^{\theta} exp(-\tau)\cdot\tau^{\gamma}\, d\tau / \Gamma(\gamma), \qquad (4.7)$$

где $\Gamma(\gamma) = \int_0^{\infty} exp(-\tau)\cdot\tau^{\gamma}\, d\tau$ – гамма функция; $\gamma = \frac{T_{полн}}{\sqrt{T_2 - T_{полн}}}$; $\theta = T_{ДИ}^{зад}\cdot\frac{\gamma}{T_{полн}}^2$; $T_{полн}$ и T_2 – рассчитываемые соответственно среднее время и 2-й момент времени реакции системы при обработке запросов системе (полного времени пребывания на обработке с учетом ожидания в очереди), $T_{ДИ}^{зад}$ – заданное время (предельно допустимое) для обработки запроса на доступ к информации (услугам).

В соответствие с выражением (4.4) рассчитанное временем, требующееся для переконфигурации МАУ составляет $T_{RECONF} = 4{,}778019376\cdot10^{-3}$ с. Соответствующее ему значение вероятности своевременности обработки запроса, полученное с помощью табулированной неполной гамма-функции равно

$$P_{ДИ}^{У}(T_{ДИ}) = \Gamma(\gamma) = \Gamma\left(\frac{T_{RECONF}}{\sqrt{D[T_{RECONF}] + T_{RECONF}^2}}\right) = \Gamma(1{,}033804) = 0{,}9983.$$

Таким образом, при одинаковых условиях получения доступа к услугам для разрабатываемой системы и ее прототипа в условиях, МАУ в разрабатываемой системе необходимо осуществить реконфигурацию, дополнительно затратив на это время, равное $T_{RECONF} = 4{,}778019376\cdot10^{-3}$ с.

4.3.5. Оценка степени достижения цели диссертационного исследования

Целью диссертационного исследования является повышение вероятности обеспечения безопасности информации при доступе к инфокоммуникационным услугам и информации в корпоративных сетях с разными требованиями по защищенности при использовании единого МАУ. Результативность процесса [45] оценивается с помощью вероятности обеспечения безопасности информации при доступе к услугам с использованием МАУ согласно выражению (1.4). Используя выражения (1.4), (1.5), (1.7)-(1.11) и принятых ограничений и допущений ($P_{\text{ЦИ}} \to 1$, $P_{\text{ПрЗ}} \to 0$, $P_{\text{СК}}\left(T_{RECONF}\right) \to 1$), получим итоговое выражение для оценивания результативности процесса защиты информации при эксплуатации МАУ:

$$P_{\text{БИ}}\left(T\right) = \left(1 - P\left[\beta\left(\tilde{L}_{Room} > L_{Room}\right) \le \beta^{\text{доп}}\right]\right) \cdot \frac{N_{\text{ДУ}}}{N_{\text{У}}} \cdot P_{\text{ДИ}}^{\text{У}}(T_{\text{ДИ}}). \qquad (4.8)$$

Значения вероятности правильной переконфигурации управляемого МАУ $P\left(CONF \subset CONF^{\text{доп}}\right) = P\left[P_{\beta}\left(\tilde{L}_{Room} > L_{Room}\right) \le P_{\beta}^{\text{доп}}\right]$ представлены в таблице 4.9. Для системы-прототипа данный показатель принят равным единице, поскольку МАУ системы прототипа неуправляемые. Сравнительный анализ количества доступных услуг для МАУ разрабатываемой системы и прототипа представлен на рисунке 1.2. На основании представленных данных получена оценка степени достижения цели исследования, представленная на рисунке 4.20.

В качестве прототипа оценивалась система доступа к услугам, основанная на типовых защищенных МАУ с количеством предоставляемых услуг, равным 5, и системой из организационно-техническим мер по защите информации, обеспечивающих требования по информационной безопасности.

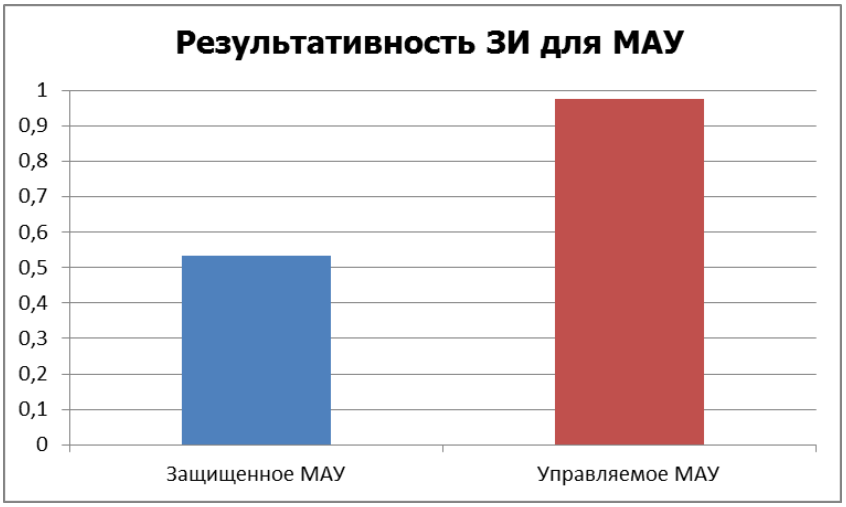


Рисунок 4.20 – Оценка степени достижения результатов диссертационного исследования

Получаемый эффект (нормированный на логарифмической шкале) при внедрении разработанной системы управления МАУ с учетом выражений (1.3), (1.13), (4.8) может быть оценен как

$$Э = \frac{\left|\lg\left(\frac{REZ}{RES}\right)\right|}{\max\left[\left|\lg\left(\frac{REZ}{RES}\right)\right|\right]}. \qquad (4.9)$$

Численные значения ресурсоемкости RES представлены на рисунке 4.19. С учетом выражения (4.9) и данных численных значений, а также в зависимости от количество пользователей МАУ были получены оценки получаемого эффекта от внедрения разработанной системы управления безопасностью МАУ и управляемых МАУ по сравнению с применяемым в настоящее время прототипом. Сравнительный анализ получаемых эффектов представлен на рисунке 4.21. Численные значения представлены в таблице 4.10.

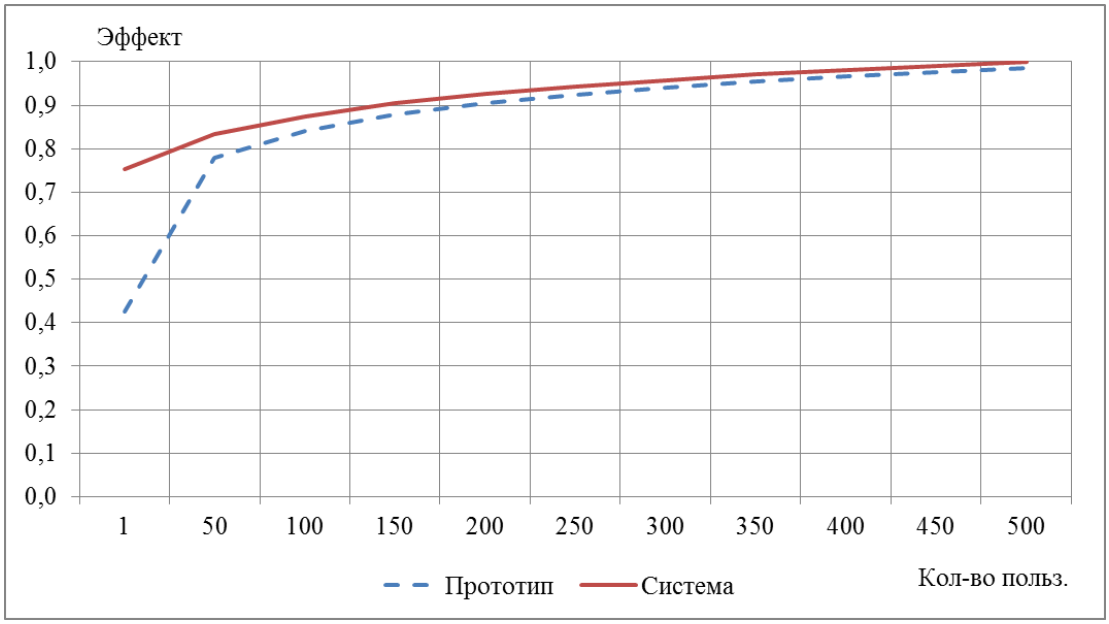


Рисунок 4.21 – Сравнительный анализ получаемого эффекта для прототипа и разработанной системы

Таблица 4.10 – Расчет численных значений эффектов от внедрения разработанной системы управления безопасностью МАУ и управляемых МАУ по сравнению с прототипом и в зависимости от количества пользователей МАУ (П – прототип, С – разработанная система)

Количество пользователей		1	50	100	150	200	250	300	350	400	450	500
Общая стои-мость, тыс. руб.	П	60	3000	6000	9000	12000	15000	18000	21000	24000	27000	30000
	С	4120	10000	16000	22000	28000	34000	40000	46000	52000	58000	64000
Эффект	П	0,00887	0,00018	0,00009	0,00006	0,00004	0,00004	0,00003	0,00003	0,00002	0,00002	0,00002
	С	0,00024	0,00010	0,00006	0,00004	0,00003	0,00003	0,00002	0,00002	0,00002	0,00002	0,00002
Эффект на лог-шкале	П	-2,052	-3,751	-4,052	-4,228	-4,353	-4,450	-4,529	-4,596	-4,654	-4,706	-4,751
	С	-3,625	-4,010	-4,214	-4,353	-4,457	-4,542	-4,612	-4,673	-4,726	-4,774	-4,816
Норми-рованный эффект на лог-шкале	П	0,426	0,779	0,841	0,878	0,904	0,924	0,940	0,954	0,966	0,977	0,986
	С	0,753	0,833	0,875	0,904	0,925	0,943	0,958	0,970	0,981	0,991	1,000

Анализ рисунка 4.21 и показывает, что получаемый эффект для разработанной системы выше, чем для используемого в настоящее время прототипа. При этом необходимо отметить, что существенный вклад в получаемый эффект вносит повышения числа доступных пользователю МАУ услуг.

Выводы по четвертому разделу

1. Проведена группа экспериментов, позволяющих обосновать выбор оптимальных параметров подсистемы определения местоположения, использующих различные технологии определения местоположения, а также параметры подсистемы определения уровня защищенности помещения на основы вычисленного местоположения и метода Монте-Карло.

2. Обоснованы оптимальные параметры подсистем определения местоположения для заданной карты помещений:

1) метод трилатерации:

– количество точек доступа – 5;

– оптимальное расположение точек доступа так, как показано на рисунке 4.3;

2) метод k-ближайших соседей:

– число учитываемых ближайших "соседей" $k = 6$ или $k = 9$;

– шаг сетки карты сигнального пространства $h = 1,5x1,5$;

– количество точек доступа – 5;

– оптимальное расположение точек доступа так, как показано на рисунке 4.3;

3) метод на основе байесовского подхода:

– число учитываемых ближайших "соседей" $k = 3$;

– шаг сетки карты сигнального пространства $h = 1,5x1,5$;

– количество измерений в каждой точке сигнального пространства с известными координатами $M \geq 30$;

– количество точек доступа – 5;

– расположение точек доступа оптимально для карты, изображенной на рисунке 4.3.

3. Наиболее точным методом определения местоположения является метод, основанный на байесовском подходе в совокупности с методом Монте-Карло.

4. Оптимальными параметрами для метода Монте-Карло при определении уровня защищенности помещения являются:

– количество испытаний $M = 1000$;

– эмпирический закон распределения вероятностей.

5. С помощью параметра порога принятия решения можно регулировать величину ошибок 1-го и 2-го рода при определении уровня защищенности помещения. При этом выполнение условия $P_\beta\left(\tilde{L}_{Room} > L_{Room}\right) \le P_\beta^{\text{доп}}$ в случае, когда $P_\beta^{\text{доп}} = 0,01$, достижимо при задании граничных параметров подсистемы определения местоположения.

6. Разработаны научно-технические предложения по составу и месту разработанной системы управления безопасностью МАУ к услугам корпоративных сетей с разными требованиями по защищенности.

7. Осуществлена комплексная оценка эффективности разработанных предложений с получением численных значений для оценки времени, необходимой для смены конфигурации МАУ, вероятности угрозы нарушения конфиденциальности при использовании управляемых МАУ, ресурсоемкости предложенной системы управления безопасностью МАУ, своевременности доступа к услугам при использовании управляемых МАУ.

8. Получена численная оценка степени достижения цели диссертационного исследования, позволяющая утверждать то, что цель достигнута.

ЗАКЛЮЧЕНИЕ

В диссертационной работе получено решение актуальной задачи по разработке алгоритма и основанной на нем системы управления безопасностью МАУ, базирующиеся на предложенной формальной модели безопасности МАУ, в совокупности позволяющие повысить вероятность обеспечения безопасности информации при доступе к инфокоммуникационным услугам и информации корпоративных сетей с разными требованиями по защищенности при использовании единого МАУ за счет учета атрибутов доступа, включая местоположения МАУ, требований по качеству предоставляемых услуг, а также политик безопасности защищенных корпоративных сетей.

Новизна предлагаемого подхода заключается в разработке и обосновании корректности формальной модели безопасности МАУ, отличающейся от известных учетом оценки его местонахождения в специальном помещении, других атрибутов доступа, а также реализацией требований мандатной и ролевой политик безопасности в корпоративных сетях с разными требованиями в отношении единого МАУ и разработке на базе данной модели нового алгоритма управления безопасностью МАУ, отличающегося от известных определением оптимальной, с точки зрения обеспечения конфиденциальности информации и качества предоставляемых пользователю услуг, программно-аппаратной конфигурации МАУ.

В рамках проведения исследований были получены следующие результаты:

1) проведен анализ состояния научных исследований и технических решений в области защиты информации при использовании МАУ, выявлены недостатки современных формальных моделей безопасности компьютерных систем применительно к обеспечению безопасности информации при использовании МАУ, включая существующие технические и программно-аппаратные решения; для решения задачи удаленного управления, а также сопряжения контуров обработки информации с разными требованиями по защищенности в современных МАУ предлагается использовать агентно-ориентированный подход, являющийся эле-

ментом искусственного интеллекта и построенный на основе клиент-серверной архитектуры;

2) разработана модель безопасности МАУ, отличающаяся от известных учетом его местонахождения в корпоративных сетях с разными требованиями по защищенности; обоснован выбор технологий, на основе которых целесообразно построение системы определения местоположения МАУ, а также предложен подход, позволяющий повысить достоверность определения местонахождения МАУ в специальных помещениях; осуществлена апробация модели с помощью имитационного моделирования, а также проведена всесторонняя оценка ее качества, включающая в себя проверку адекватности, чувствительности и устойчивости; получены оценки параметров частных моделей, влияющих на достоверность определения местоположения МАУ;

3) разработан алгоритм управления безопасностью МАУ, учитывающий атрибуты доступа мобильных пользователей; описана оптимизационная задача, решаемая в алгоритме и охарактеризованная как задача многокритериальной оптимизации целочисленного динамического программирования; представлено описание цикла управления конфигурацией МАУ с уравнениями состояния и наблюдения, обоснованием цели управления; описаны основные процедуры, входящие в состав алгоритма; исследованы основные свойства алгоритма и его процедур, включая временную сложность, сложность по памяти и точность. Получены их численные оценки, а также представлен численный пример работы алгоритма;

4) сформированы научно-технические предложения по практической реализации системы управления безопасностью МАУ в корпоративных сетях с разными требованиями по защищенности; проведена группа экспериментов и обоснован выбор оптимальных параметров подсистемы определения местоположения; осуществлена комплексная оценка эффективности разработанных предложений с получением численных значений для оценки времени, необходимой для смены конфигурации МАУ, вероятности угрозы нарушения конфиденциальности при использовании управляемых МАУ, ресурсоемкости предложенной системы управления безопасностью МАУ, своевременности доступа к услугам; получена

численная оценка степени достижения цели диссертационного исследования, позволяющая утверждать то, что цель достигнута.

Диссертация соответствует пунктам "2. Методы, аппаратно-программные и организационные средства защиты систем (объектов) формирования и предоставления пользователям информационных ресурсов различного вида.", "8. Модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем.", "13. Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности." паспорта научной специальности 05.13.19 "Методы и системы защиты информации, информационная безопасность" (технические науки).

Направлением дальнейших исследований автор считает

– исследование перспективных технологий определения местоположение пользователей МАУ в помещениях внутри здания с целью снижения ошибок;

– исследование технологий агентно-ориентированного подхода для оптимизации информационного взаимодействия контроллеров беспроводных сетей по передаче управляющей информации;

– совершенствование подходов по управлению конфигурацией современных мобильных устройств с целью создания возможности реализации разработанных подходов по управлению доступом применительно к услугам, использующим конфиденциальные сведения.

СПИСОК СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ

АПМДЗ	–	аппаратно-программный модуль доверенной загрузки
АРМ	–	автоматизированное рабочее место
АС	–	автоматизированная система
БСПД	–	беспроводная сеть передачи данных
ВОЛС	–	волоконно-оптическая линия связи
ГЛОНАСС	–	глобальная навигационная спутниковая система
ЗБ	–	задание по безопасности
ЗКС	–	защищенная корпоративная сеть
ЗИ	–	защита информации
ИБ	–	информационная безопасность
ИПС	–	изолированная программная среда
КС	–	компьютерная система
КСЗИ	–	криптографические средства защиты информации
МАУ	–	мобильное абонентское устройство
ОС	–	операционная система
ПЗ	–	профиль защиты
ПЗУ	–	постоянное запоминающее устройство
ПО	–	программное обеспечение
ПЭВМ	–	персональная электронная вычислительная машина
СВТ	–	средства вычислительной техники
СЗИ	–	средство защиты информации
СКЗИ	–	система криптографической защиты информации
СКО	–	среднеквадратическое отклонение
СУБД	–	систему управление базой данных
СШП	–	сверхширокополосный (сигнал)
ТС	–	техническое средство

ТКУИ	–	технический канал утечки информации
УКВ	–	ультракороткие волны
МАУ	–	универсальное мобильное абонентское устройство
ФГУП	–	Федеральное государственное унитарное предприятие
ФСТЭК	–	Федеральная служба по техническому и экспортному контролю Российской Федерации
ЦУИБ	–	центр управления информационной безопасностью
ЭВТ	–	электронная вычислительная техника
ACK	–	Acknowledge
BYOD	–	Bring Your Own Device
CCA	–	Channel Clearance Algorithm
CTS	–	Clear To Send
CSMA/CA	–	Carrier Sense Multiple Access / Collision Avoidance
IEEE	–	Institute of Electrical and Electronics Engineers
GPS	–	Global Positioning System
GSM	–	Global System for Mobile Communications
LTE	–	Long-Term Evolution
MAC	–	Media Access Control
MAM	–	Mobile Application Management
MDM	–	Mobile Device Management
MIM	–	Mobile Information Management
OFDM	–	Orthogonal Frequency Division Multiplexing
POA	–	Phase of Arrival
RFID	–	Radio Frequency IDentification
RSP	–	Received Signal Phase
RSS	–	Received Signal Strength
RSSI	–	Received Signal Strength Indicator
RTS	–	Ready To Send
SoC	–	System-on-Chip

SSO	–	Single Sign-On
TDOA	–	Time Difference Of Arrival

СПИСОК ЛИТЕРАТУРЫ

1. Амосов, А. А. Вычислительные методы для инженеров: Учеб. пособие / А. А. Амосов, Ю. А. Дубинский, Н. В. Копченова. – Москва : Высш. шк., 1994. – 544 с.

2. Аппаратура 605 / ОАО "Концерн "Автоматика" [Электронный ресурс] : Электрон. дан. – Москва, 2015. Режим доступа: http://oao-ka.ru/Vremennyj_katalog/Zacshicshennye_telefonnye_apparaty/Apparatura_605.htm. – Дата обращения: 29.05.2015 г.

3. Артамонов, В. А. Безопасность мобильных устройств, систем и приложений // Проект ИТ-защита [Электронный ресурс] / Режим доступа: http://itzashita.ru/wp-content/uploads/2015/04/Bezop_mobil_Artamonov.pdf. – Дата обращения: 04.06.2015 г.

4. Бахвалов, Н.С. Численные методы: учеб. пособие для студ. физ.-мат. спец. вузов / Н. С. Бахвалов, Н. П. Жидков, Г. М. Кобельков. – Изд. 3-е. – Москва : БИНОМ. Лаборатория знаний, 2007. – 637 с.

5. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий // Руководящий документ (ГОСТ Р ИСО/МЭК 15408). – Москва : Гостехкомиссия России, 2002. – Ч. 1–3.

6. Белько, И. В. Теория вероятностей и математическая статистика. Примеры и задачи : учеб. пос. / И. В. Белько, Г. П. Свирид под. ред. К. К. Кузьмича. – 2-е изд., стер. – Москва : Новое издание, 2004. – 251 с.

7. Бочков, М. В. Адаптивная защита информации от несанкционированного доступа в вычислительных сетях / М. В. Бочков, С. Н. Бушуев, В. А. Логинов, И. Б. Саенко. – Санкт-Петербург : ВАС, 2005. – 172 с.

8. Бочков, М. В. Проектирование автоматизированных систем обработки информации и управления: Курс лекций / М. В. Бочков, О. В. Тараканов. – Орел: Академия ФАПСИ, 2002. – 282 с.

9. Вишнякова, О. А. Математическая модель обнаружения точки беспроводного доступа по измерениям можности излучения разнесенными наблюдателями / О. А. Вишнякова, Д. Н. Лавров, С. Ю. Лаврова // Математические структуры и моделирование / Ом. гос. ун-т. Фак. компьютер. наук. – Омск : Изд-во ОмГУ. – 2013. – № 2(28). – С.49–59.

10. Вопросы безопасности мобильных устройств / А. Г. Бельтов, И. Ю. Жуков, А. В. Новицкий, Д. М. Михайлов, А. В. Стариковский // Безопасность информационных технологий Москва : Всероссийский научно-исследовательский институт проблем вычислительной техники и информатизации, 2012. – С. 5–7.

11. Ворошилин, Е. П. Моделирование процессов и явлений в системах связи : методическое пособие для самостоятельной работы магистров направления 210700.68 "Инфокоммуникационные технологии и системы связи" / Е. П. Ворошили // ТУСУР, 2012.

12. Выборнов, О. В. Прогнозирование потенциальной нагрузки секторов сетей широкополосного доступа на основе анализа отношения сигнал/помеха с использованием геоинформационных технологий / О .В. Выборнов, А. М. Измайлов, С. В. Козлов, В Н. Лаврушев, Е. А. Спирина // Вестник Казанского государственного технического университета им. А. Н. Туполева. – 2013. – Выпуск № 4. – С. 130–135.

13. Выборнов, О. В. Тестирование ЭМС оборудования стандарта 802.11n фирмы InfiNet / О. В. Выборнов, А. М. Измайлов, С. В. Козлов, Е. А. Спирина // Вестник КГТУ им. А. Н. Туполева. – 2012. – Выпуск № 2 (68). – С. 160–163.

14. Голдсмит, А. Беспроводные коммуникации. Москва : Техносфера, 2011. 904 с.

15. ГОСТ Р 50922–2006. Защита информации. Основные термины и определения. – Введ. 2006.12.27. – Москва : Федеральное агентство по техническому регулированию и метрологии, 2006. – 16 с. – (Национальный стандарт Российской Федерации).

16. ГОСТ Р 51275–2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. – Введ.

2006.12.27. – Москва : Федеральное агентство по техническому регулированию и метрологии, 2007. – 8 с. – (Национальный стандарт Российской Федерации).

17. ГОСТ Р 53114–2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. – Введ. 2006.12.27. – Москва : Федеральное агентство по техническому регулированию и метрологии, 2006. – 12 с. – (Национальный стандарт Российской Федерации).

18. ГОСТ РВ 51987–2002. Информационная технология. Комплекс стандартов на автоматизированные системы. Типовые требования и показатели качества функционирования информационных систем. Общие положения. – Введ. 2001. – Москва : ИПК Издательство стандартов, 2002. – 60 с. – (Государственный стандарт Российской Федерации).

19. ГОСТ Р ИСО 7498-2–99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. – Введ. 1999.03.18. – Москва : ИПК Издательство стандартов, 1999. – 39 с. – (Государственный стандарт Российской Федерации).

20. ГОСТ Р ИСО/МЭК 15408-1–2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. – Введ. 01.12.2013. – Москва : ФГУП "СТАНДАРТИНФОРМ", 2014. – 56 с. – (Государственный стандарт Российской Федерации).

21. ГОСТ Р ИСО/МЭК 15408-2–2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности. – Введ. 01.09.2014. – Москва : ФГУП "СТАНДАРТИНФОРМ", 2014. – 328 с. – (Государственный стандарт Российской Федерации).

22. ГОСТ Р ИСО/МЭК 15408-3–2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности. – Введ. 01.09.2014. – Москва : ФГУП "СТАНДАРТИНФОРМ", 2014. – 150 с. – (Государственный стандарт Российской Федерации).

23. Груздев, С. Л. Проблемы доверия к импортной электронике на базе ARM-процессоров / С. Л. Груздев // Форум "Технологии безопасности". Красногорск. 7-9 февраля 2017 года : материалы [Электронный ресурс]: Электрон. дан. – Красногорск, 2017. Режим доступа: http://new.groteck.ru/images/catalog/46978/5cf0f9ab4188375622ef14b54f1b8bfe.pdf. – Дата обращения: 19.05.2017 г.

24. Грушко, А. А. Теоретические основы защиты информации / А. А. Грушко, Е. Е. Тимонина. – Москва : Издательство Агентсва "Яхтсмен", 1996. – 192 с.

25. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. – 2-е изд., испр. и доп. – Москва : Горячая линия-Телеком, 2013. – 338 с.: ил. ISBN 978-5-9912-0328-9.

26. Девянин, П. Н. Теоретические основы компьютерной безопасности : Учеб. пособие для вузов / П. Н. Девянин, О. О., Михальский, Д. И. Правиков, А. Ю. Щербаков. – Москва : Радио и связь, 2000. –192.

27. Десницкий, В. А. Конфигурирование безопасных встроенных устройств с учетом показателей ресурсопотребления : автореф. дис. ... канд. техн.. наук : 05.13.19 / Десницкий Василий Алексеевич ; [Санкт-Петербургский ин-т информатики и автоматизации РАН]. – Санкт-Петербург, 2013. – 22 с. – Библиогр.: с. 21–22.

28. Заяц, А. Обзор и тестирование смартфона Caesar A9600, а также знакомство с MT6589 - четырехядерной SoC MediaTek для бюджетных решений [Электронный ресурс] / Режим доступа: http://ixbt.com/md/pda/. – Дата обращения: 03.03.2014 г.

29. Зегжда, Д. П. Основы безопасности информационных систем / Д. П. Зегжда, А. М. Ивашко. – Москва : Горячая линия – Телеком, 2000. – 452 с.

30. Илибман, В. Безопасность на основе идентификации Cisco Secure ACS / В. Илибман : Презентация доклада, 2009. – 53 с.

31. Инструмент имитационного моделирования AnyLogic [Электронный ресурс] : сайт / The AnyLogic Company. – Санкт-Петербург, 1991– . – Режим доступа: http://www.anylogic.ru/overview. – Дата обращения: 11.12.2013 г.

32. КАМИ-Терминал / Научно-технический центр КАМИ [Электронный ресурс] : Электрон. дан. – Москва, 2015. Режим доступа: http://www.kami.ru/Solutions/КАМИ-Терминал. – Дата обращения: 29.05.2015 г.

33. Колегов, Д. Н. Построение иерархического ролевого управления доступом // Математические основы компьютерной безопасности. – 2012. – № 3 (17). – С. 69–76.

34. Колмогоров, А.Н. Теория информации и теория алгоритмов. – Москва : Наука, 1987. – 303 с.

35. Континент Т-10 / Код безопасности [Электронный ресурс] : Электрон. дан. – Москва, 2015. Режим доступа: http://securitycode.ru/products/kontinent_t_10/. – Дата обращения: 29.05.2015 г.

36. Крипто БД: защита баз данных Oracle // ООО "Алладин Р.Д." [Электронный ресурс] / Режим доступа: https://www.aladdin-rd.ru/catalog/cryptobd/. – Дата обращения: 23.06.2017 г.

37. Майн, Х. Марковские процессы принятия решений / Х. Майн, С. Осаки. Москва : Наука, 1977. – 176 с.

38. Малышев, В. В. Методы оптимизации в задачах системного анализа и управления : Учебное пособие. – Москва : Изд-во МАИ-ПРИНТ, 2010. – 440 с.: ил. ISBN 978-5-7035-2179-2.

39. Маркин, Д. О. Автоматизированная система оценки защищенности удаленного доступа на основе данных о местоположении / Д. О. Маркин, Л. К. Саморцев // Информационная безопасность и защита персональных данных: Проблемы и пути их решения [Текст]+[Электронный ресурс]: материалы VI Межрегиональной научно-практической конференции / под ред. О. М. Голембиовской. – Брянск: БГТУ,2014. – С. 81–85. ISBN 978-5-89838-751-8.

40. Маркин, Д. О. Автоматизированная система оценки защищенности удаленного доступа на основе модели поведения пользователя мобильного устройства / Д. О. Маркин, А. А. Смыкалов // Информационная безопасность и защита персональных данных: Проблемы и пути их решения [Текст]+[Электронный ре-

сурс]: материалы VI Межрегиональной научно-практической конференции / под ред. О.М. Голембиовской. – Брянск: БГТУ,2014. – С. 75–81.

41. Маркин, Д. О. Алгоритм управления программно-аппаратной конфигурацией защищенного мобильного абонентского устройства / Д. О. Маркин, В. В. Комашинский, А. А. Двилянский // Промышленные АСУ и контроллеры. – 2016. – № 9. – С. 39–50.

42. Маркин, Д. О. Имитационное моделирование определения местоположения пользователей мобильных устройств внутри помещений / Д. О. Маркин, В. В. Комашинский // Информационная безопасность и защита персональных данных. Проблемы и пути их решения [Текст]+[Электронный ресурс]: материалы VII Межрегиональной научно-практическая конференция / под ред. О. М. Голембиовской. – Брянск: БГТУ, 2015. – С. 109–115.

43. Маркин, Д. О. Исследование эффективности алгоритмов определения местоположения мобильных устройств внутри помещений / Д. О. Маркин // Вестник РГРТУ. – 2015. – № 54-1. – С. 32–39.

44. Маркин, Д. О. Методика обнаружения и способы противодействия распределенной атаке типа "отказ в обслуживании", основанной на использовании SEO-технологий / Д. О. Маркин, М. А. Сазонов // Информация и безопасность. – 2014. – № 2 (7) – С.208–211.

45. Маркин, Д. О. Методика оценки эффективности защиты информации при эксплуатации мобильных абонентских устройств в корпоративных сетях с разными требованиями по защищенности / Д. О. Маркин, В. В. Комашинский, И. А. Сенотрусов // Вопросы кибербезопасности. – 2017. – № 4 (22). – С. 21–31.

46. Маркин, Д. О. Модель состояний мобильного абонентского устройства в помещениях с разными требованиями по защищенности / Д. О. Маркин, В. В. Комашинский, А. А. Двилянский // Промышленные АСУ и контроллеры. – 2016. – № 10. – С. 40–51.

47. Маркин, Д. О. Модель управления профилем защиты мобильного устройства при доступе к услугам с разным уровнем конфиденциальности /

Д. О. Маркин, В. В. Комашинский, И. Ю. Баранов // Информационные технологии. – 2015. – № 9 (21). – С. 611–618.

48. Маркин, Д.О. Модель доступа к информационным системам / Д. О. Маркин, М. А. Сазонов // Телекоммуникации. – 2013. – № 9. – С. 27–31.

49. Маркин, Д.О. Модель и алгоритм адаптивного управления профилем защиты мобильного устройства / Д. О. Маркин, В. В. Комашинский // XII Всероссийское совещание по проблемам управления ВСПУ-2014. Москва, 16-19 июня 2014 г. : Труды. [Электронный ресурс] Москва : Институт проблем управления им. В. А. Трапезникова РАН, 2014. 9616 с. Электрон. текстовые дан. (1074 файл.: 537 МБ). 1 электрон. опт. диск (DVD-ROM). Файл 7449. ISBN 978-5-91450-151-5. Номер государственной регистрации: 0321401153.

50. Маркин, Д. О. Модель определения местоположения пользователей мобильных устройств внутри помещений на основе сигналов беспроводной сети доступа / Д. О. Маркин, В. В. Комашинский // Перспективные информационные технологии (ПИТ 2015), Том 2: труды Международной научно-технической конференции / под ред. С.А. Прохорова. – Самара: Издательство Самарского научного центра РАН, 2015. – С. 305–309. ISBN 978-5-93424-735-6.

51. Маркин, Д. О. Модель системы определения местоположения мобильного устройства на основе метода статистических испытаний / Д. О. Маркин, С. М. Макеев // Известия Тульского государственного университета. Технические науки. – 2016. – № 2. – С. 150–165.

52. Маркин, Д. О. Практические аспекты реализации управления функциональностью мобильных устройств на базе операционной системы Android // Д. О. Маркин, А. Н. Разумов // Информационная безопасность и защита персональных данных. Проблемы и пути их решения: Материалы VIII Всероссийской научно-практической конференции [Текст] + [Электронный ресурс] / под ред. О.М. Голембиовской, М.Ю.Рытова. – Брянск: БГТУ, 2016. – С. 105–110. ISBN 978-5-89838-886-10.

53. Маркин, Д. О. Система удаленного управления функциональностью мобильного абонентского устройства / Д. О. Маркин, А. Н. Разумов // Перспектив-

ные информационные технологии (ПИТ 2016): труды Международной научно-технической конференции / под ред. С.А. Прохорова. – Самара: Издательство Самарского научного центра РАН, 2016. – С. 322–326. ISBN 978-5-93424-758-5.

54. Мобильное защищенное автоматизированное рабочее место доступа в сеть Интернет / ФГУП "НТЦ "АТЛАС"" [Электронный ресурс] : Электрон. дан. – Москва, 2015. Режим доступа: http://web.stcnet.ru/products_iid_27.htm. – Дата обращения: 29.05.2015 г.

55. Мобильный вычислительный комплекс "ИНФОПРО" МВК-2 / ЗАО "Инфопро" [Электронный ресурс] : Электрон. дан. – Москва, 2015. Режим доступа: http://www.infopro.ru/vt.php?id=48. – Дата обращения: 29.05.2015 г.

56. Об информации, информационных технологиях и о защите информации : федер. закон от 27 июля 2006 г. № 149-ФЗ // Информационно-правовая система "Законодательство России" [Электронный ресурс] / Официальный интернет-портал правовой информации "Государственная система правовой информации". – Последнее обновление 05.05.2015 г.

57. Однонаправленный шлюз "Атликс-Шлюз-К" / ФГУП "НТЦ "АТЛАС"" [Электронный ресурс] : Электрон. дан. – Москва, 2015. Режим доступа: http://web.stcnet.ru/products_iid_26.htm. – Дата обращения: 29.05.2015 г.

58. Озарнов, И. Интеграция сервисов идентификации и контроля доступа. Решение Cisco Identity Services Engine (ISE) / И. Озарнов, Г. Симонов : Презентация доклада, 2012. – 47 с.

59. О государственной тайне : федер. закон от 21 июня 1993 г. № 5485-I // Информационно-правовая система "Законодательство России" [Электронный ресурс] / Официальный интернет-портал правовой информации "Государственная система правовой информации". – Последнее обновление 05.05.2015.

60. Пат. 2503059 Российская Федерация : МПК G06F 15/173, H04L 29/12. Способ удаленного мониторинга и управления информационной безопасностью сетевого взаимодействия на основе использования системы доменных имен / Д. О. Маркин, М. С. Аксаментов ; заявитель и патентообладатель Академия ФСО Рос-

сии. - № 2012123556 ; заявл. 06.06.2012 ; опубл. 27.12.2013, Бюл. № 36. – 16 с. : ил.

61. Пат. 2530691 Российская Федерация : МПК G06F11/00; H04L9/08. Способ защищенного удаленного доступа к информационным ресурсам / Д. О. Маркин, Д. Е. Шугуров [и др.] ; заявитель и патентообладатель Академия ФСО России. - № 2013113592; заявл. 26.03.2013; опубл. 10.10.2014, Бюл. № 28. – 13 с. : ил.

62. Пат. 2546236 Российская Федерация : МПК G06F11/00; H04L9/08. Способ анализа информационного потока и определения состояния защищенности сети на основе адаптивного прогнозирования и устройство для его осуществления / Д.О. Маркин, С. В. Гребенев, В. Ю. Сергеенков, А. А. Кузькин ; заявитель и патентообладатель Академия ФСО России. - № 2013136682; заявл. 05.08.2013; опубл. 10.04.2015, Бюл. № 10 – 29 с. : ил.

63. Петрова, Е. А. Оценка гарантированной информационной скорости передачи в сетях широкополосного радиодоступа с учетом внутрисистемных помех [Электронный ресурс] / Е. А. Петрова // Журнал Радиоэлектроники. – 2014. – № 10.

64. Петухов, Г. Б. Основы теории эффективности целенаправленных процессов. Ч. 1. Методология, методы, модели. – МО СССР, 1989. – 660 с.

65. Положинцев, Б. И. Теория вероятностей и математическая статистика. Введение в математическую статистику: Учебное пособие. – Санкт-Петербург : Изд-во Политехн. ун-та, 2010.– 95 с.

66. Пролетарский, А. В. Организация беспроводных сетей / А. В. Пролетарский, И. В. Баскаков, Р. А. Федотов, А. В. Бойков, Д. Н. Чирков, В. А. Платонов / Под ред. К. А. Пупкова. Москва : Техносфера, 2011. – 181 с.

67. Р. 50.1.033–2001. Прикладная статистика. Правила проверки согласия опытного распределения с теоретическим. Часть 1. Критерии типа хи-квадрат. – Введ. 2001. – Москва : ФГУП "Стандартинформ". – 87 с. (Рекомендации по стандартизации).

68. Рабинер, Л. Р. Скрытые Марковские модели и их применение в избранных приложениях при распознавании речи: Обзор. // ТИЭР – Москва : Наука, 1989. – Выпуск 2. – Том 77. – С. 86–102.

69. Развитие интернета в регионах России. Весна 2014 / "Яндекс" [Электронный ресурс] : Электрон. дан. – Москва, 2014. Режим доступа: http://download.yandex.ru/company/ya_internet_regions_2014.pdf. – Дата обращения: 31.10.2014.

70. Рекомендация МСЭ-Т E.802. Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы. Качество услуг электросвязи: концепции, модели, цели и планирование надежности работы. – Термины и определения, связанные с качеством услуг электросвязи. Принципы и методики определения и применения параметров QoS. – Введ. 2007.02.08. – Сектор стандартизации электросвязи МСЭ, 2007.

71. Российский рынок мобильной коммерции (M-commerce) 2014 / РБК [Электронный ресурс] : Электрон. дан. – Москва, 2014. Режим доступа: http://marketing.rbc.ru/download/research/562949989322122.shtml. – Дата обращения: 10.04.2015 г.

72. Руководящий документ. Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности Гостехкомиссия России // ФСТЭК России [Электронный ресурс] : сайт. – Электрон. дан. – Москва, 2003 – Режим доступа: http://fstec.ru/component/attachments/download/314. – Дата обращения 20.05.2015 г.

73. Салех, Х. М. Мобильные системы предоставления информационных сервисом позиционирования объектов : автореф. дис. ... канд. техн. наук : 05.13.01 / Салех Хади Мухаммед; [Владимирский гос. ун-т]. – Владимир, 2013. – 20 с. – Библиогр.: с. 19–20

74. Свидетельство о государственной регистрации программы для ЭВМ № 2013612870 Российская Федерация : DNS-коммутатор / Д. О. Маркин; заявл. 09.01.2013; зарегистрировано в Реестре программ для ЭВМ 14.03.2013 г.

75. Свидетельство о государственной регистрации программы для ЭВМ № 2013615947 Российская Федерация. Автоматизированная система оценки вероятности отказа в обслуживании запросов пользователей при построении сети как системы массового обслуживания / [Д. О. Маркин, Д. Е. Шугуров, А. Н. Цибуля и др.] ; заявл. 06.03.2013; зарегистрировано в Реестре программ для ЭВМ 24.09.2013 г.

76. Свидетельство о государственной регистрации программы для ЭВМ № 2013618388 Российская Федерация. Анализатор контекста доступа мобильного устройства / Д. О. Маркин, С. В. Шекшуев, В. В. Комашинский ; заявл. 19.07.2013; зарегистрировано в Реестре программ для ЭВМ 06.09.2013 г.

77. Свидетельство о государственной регистрации программы для ЭВМ № 2014617119 Российская Федерация. Автоматизированная система оценки параметров защищенности удаленного доступа к услугам защищенной корпоративной сети пользователя мобильного устройства / Д. О. Маркин, Л. К. Саморцев, А. А. Смыкалов ; заявл. 21.05.2014; зарегистрировано в Реестре программ для ЭВМ 11.07.2014 г.

78. Свидетельство о государственной регистрации программы для ЭВМ № 2014617940 Российская Федерация. Автоматизированная система мониторинга и управления информационной безопасностью сетевого трафика при доступе к услугам информационных сервисов, использующих систему доменных имен / Д. О. Маркин, И. М. Кудинов, Е. В. Лебеденко ; заявл. 10.06.2014; зарегистрировано в Реестре программ для ЭВМ 06.08.2014 г.

79. Свидетельство о государственной регистрации программы для ЭВМ № 2015615631 Российская Федерация. Автоматизированная система определения местоположения пользователей мобильных устройств внутри здания на основе сигналов беспроводной сети / Д. О. Маркин, Н. И. Биркун, А. О. Зозуля ; заявл. 24.03.2015; зарегистрировано в Реестре программ для ЭВМ 21.05.2015 г.

80. Свидетельство о государственной регистрации программы для ЭВМ № 20166111210 Российская Федерация. Программный агент удаленного управления функциональностью мобильного абонентского устройства / Маркин Д. О., Ра-

зумов А. Н., Сенотрусов И. А. ; заявл. 06.11.2015; зарегистрировано в Реестре программ для ЭВМ 27.01.2016 г.

81. Сидак, А. А. Мобильные устройства в информационных системах и угрозы безопасности информации. Взаимосвязи /А. А. Сидак, А. В. Ильин, А. В. Кубарев, // Вопросы кибербезопасности. – 2014. – № 3 (4). – С. 29–34.

82. Система однонаправленной передачи данных ДИ-ОД / АО ЦНИИ ЭИСУ [Электронный ресурс] : Электрон. дан. – Москва, 2015. Режим доступа: http://cniieisu.ru/index.php/produsti-i-uslugi/17-produkciya/apparatnoe-obespechenie/odnonapravlennyj-informatsionnyj-shlyuz-di-od. – Дата обращения: 29.05.2015 г.

83. Специализированный терминал мобильной связи (СТМС) "Сапфир-К" / НИИ Автоматики Сапфир-К [Электронный ресурс] : Электрон. дан. – Москва, 2015. Режим доступа: http://niia.ru/document/sapfir.htm. – Дата обращения: 29.05.2015 г.

84. Специальный микросотовый телефон М-549М / ФГУП "НТЦ "АТЛАС"" [Электронный ресурс] : Электрон. дан. – Москва, 2015. Режим доступа: http://web.stcnet.ru/products_iid_24.htm. – Дата обращения: 29.05.2015 г.

85. Специальный сотовый телефон SMP-АТЛАС/2 / ФГУП "НТЦ "АТЛАС"" [Электронный ресурс] : Электрон. дан. – Москва, 2015. Режим доступа: http://web.stcnet.ru/products_iid_17.htm. – Дата обращения: 29.05.2015 г.

86. Статистические методы обработки результатов наблюдений : учеб. для вузов / под ред. докт. техн. наук проф. Юсупова Р. М. – Москва : Мин. Обороны СВСР, 1984. – 687 с

87. Стратонович Р. Л. Условные марковские процессы и их применение к теории оптимального управления. Изд. МГУ. 1965 г. – 319 с.

88. Талисман 395 – защищённый телефон стандарта GSM / СовТехКом Информационная безопасность [Электронный ресурс] : Электрон. дан. – Москва, 2015. Режим доступа: http://www.sovtechcom.ru/product/talisman-395.html. – Дата обращения: 29.05.2015 г.

89. Теория электрической связи : учебник для вузов / А. Г. Зюко, Д. Д. Кловский, В. И. Коржик, М. В. Назаров ; под ред. Д. Д. Кловского. – Москва : Радио и связь, 1999. – 432 с. : 204 ил.

90. Хаккарайнен, А. Как защититься от мобильных угроз // Computer World Россия. – 2007. – № 24. – С. 32–34.

91. Хорев, А. А. Техническая защита информации: учеб. пособие для студентов вузов / А. А. Хорев. – В 3 т. Т. 1 : Технические каналы утечки информации. – Москва : НПЦ "Аналитика", 2008. – 436 с.

92. Хорев, А. А. Технические каналы утечки информации, обрабатываемой средствами вычислительной техники / А. А. Хорев // Специальная техника. – 2010. – С. 39–56.

93. Хрусталев, Д.А. Мобильные телефоны Siemens. Принципы устройства и ремонт [Текст] / Д. А. Хрусталев. - Москва : Изумруд, 2004. – 256 с.

94. Чернов, Д. В. О моделях логического управления доступом на основе атрибутов // Математические основы компьютерной безопасности. – 2012. – № 3 (17). – С. 79–82.

95. Шутый, Р.С. Модифицированный протокол "Передача бита на хранение" для канала с изменяемой вероятностью ошибки / В. А. Яковлев, Р. С. Шутый // Проблемы информационной безопасности. Компьютерные системы. – 2008. – № 1. – С. 88–95.

96. Шутый, Р.С. Протокол "Забывчивая передача" с использованием интерактивного хэширования / В. А. Яковлев, Р. С. Шутый // Методы и техн. сред-ства обеспечения безопасности информации: Материалы XVII Общерос. НТК. – Санкт-Петербург.: Изд-во СПбГПУ, 2008. – С. 74–75.

97. Щербаков, А. Ю. Введение в теорию и практику компьютерной безопасности. – Москва : Издатель Молгачева С. В., 2001. – 352 с.

98. Эшби, У.Р. Введение в кибернетику: Пер. с англ. – Москва : Изд-во иностран-ной литературы, 1959. – 432 с.

99. A Survey of Indoor Positioning Systems and Algorithms / Klaithem Al Nuaimi // International Conference on Innovations in Informational Technology, – 2011. – Vol.11. – P.185–190.

100. Al-Muhtadi, J. Context and location-aware encryption for pervasive computing environments / J. Al-Muhtadi, R. Hill, R. Campbell, M.D. Mickunas // In: PERCOMW ’06: Proc. of the 4thAnnual IEEE Intl. Conf. on Pervasive Comput. and Commun.Workshops, 2006. – P. 283–289.

101. An Indoor Positioning Technique Based on Fuzzy Logic / Chih-Yung Chen, Jen-Pin Yang, Guang-Jeng Tseng, Yi-Huan Wu, Rey-Chue Hwang // IMECS : Proceedings of the International MultiConference of Engineers and Computer Scientists (17-19 March, 2010, Hong Kong). Hong Kong, 2010. – Vol. 2.

102. Ardagna, C. A. Supporting location-based conditions in access control policies / C. A. Ardagna, M. Cremonini, E. Damiani, S. De Capitani di Vimercati, P. Samarati // In Proceedings of the ACM Symposium on Information, Computer and Communications Security, Taipei, Taiwan, March 2006. – P. 212–222.

103. Bahl, P. RADAR: An in-building RF-based user location and tracking system / P. Bahl, V. N. Padmanabhan : Proc. IEEE INFOCOM 2000, Mar.. – 2000. – Vol. 2. – P. 775–784.

104. Bahl, P. Enhancements to the RADAR user location and tracking system / P. Bahl, V. N. Padmanabhan Microsoft Corp., Tech. Rep. MSR-TR-2000–12, Feb. 2000.

105. Battiti, R. Location-aware computing:A neural network model for determining location in wireless LANs / R. Battiti, T. L. Nhat, A.Villani : Tech. Rep. DIT-02–0083, 2002.

106. Bell, D.E. Secure Computer Systems: Unified Exposition and Multics Interpretation. – Bedford, Mass.: MITRE Corp., 1976. – MTR-2997 Rev.1.

107. Brunato, M. Statistical learning theory for location fingerprinting in wireless LANs / M. Brunato, R. Battiti : Comput. Netw. – 2005. – V. 47. – P. 825–845.

108. Google Tango Project / Google Inc. [Электронный ресурс] : Электрон. дан. – 2016. Режим доступа: https://get.google.com/tango/. – Дата обращения: 30.06.2016.

109. Gwon, Y. Error characteristic and calibaration-free techniques for wireless LAN-based location estimation / Y. Gwon, R. Jain // in Proc. MobiWac'04, Philadelphia, PA, Oct. 1, 2004. – P. 2–9.

110. Hansen, F. SRBAC: A Spacial Role-Based Access Control Model for Mobile Systems / F. Hansen, V. Oleshchuk // In: Proceedings of the 8th Nordic workshop secure IT systems (NORDSEC). – 2003. – P. 129–141.

111. Harrison, M. Protection in operation systems / M. Harrison, W. Ruzzo, J. Ulman // Communication of ACM. – 1976. – № 19 (8). – P. 461–471.

112. Hashemi, H. The Indoor Radio Propagation Channel // Proceedings of the IEEE. – 1993. – Vol. 81. – No. 7. – P. 943–968.

113. HELIOS ProfyShield LT-A330–1s / Группа компаний "Гелиос" [Электронный ресурс] : Электрон. дан. – Москва, 2015. Режим доступа: http://www.hbc.ru/solutions/security/secured_terminal/. – Дата обращения: 29.05.2015 г.

114. Hewitt, C. A Universal Modular ACTOR Formalism for Artificial Intelligence / C. Hewitt, P. Bishop, R. Steiger // Proc. of the Third Int. Joint Conf. on AI (IJCAI-73). – Stanford, CA: Stanford University: 1973. – P. 235–245.

115. Hur, J. Attribute-based access control with efficient revocation in data outsourcing systems / J. Hur, D.K. Noh // IEEE Trans. Parallel Distrib. Syst. – 2011. № 22 (7). – P. 1214–1221.

116. Hybrid WSN and RFID indoor positioning and tracking system / Zhoubing Xiong1, Zhenyu Song1, Andrea Scalera2, Enrico Ferrera2, Francesco Sottile2, Paolo Brizzi2, Riccardo Tomasi2, Maurizio A Spirito2 // EURASIP Journal on Embedded Systems [Электронный ресурс] / Режим доступа: http://jes.eurasipjournals.com/content/2013/1/6. – 2013. – Дата обращения: 12.02.2014 г.

117. IEEE 802.11, The Working Group Setting the Standards for Wireless / The Institute of Electrical and Electronics Engineers : Электрон. дан. – 2015. Режим доступа: http://www.ieee802.org/11/. – Дата обращения: 09.09.2015 г.

118. Indrakshi, Ray LRBAC: A Location-Aware Role-Based Access Control Model [Электронный ресурс] / Indrakshi Ray, Mahendra Kumar, and Lijun Yu. – Электрон. текстовые данные, Proceedings of the 2nd International Conference on Information Systems Security, Kolkata, India, December 2006. – Режим доступа: http://www.cs.colostate.edu/~lijun/ICISS06.pdf. – Дата обращения: 18.11.2014 г.

119. ITU-R P.1238-7 Propagation data and prediction methods for the planning of indoor radio communication systems and the radio local area networks in the frequency range 900 MHz to 100 GHz. Geneva: ITU-R Recommendations, 2001.

120. Koyuncu, H. A Survey of Indoor Positioning and Object Locating Systems / Hakan Koyuncu, Shuang Hua Yang // IJCSNS International Journal of Computer Science and Network Security, 2011. – Vol. 10. – № 5. – P.121–128.

121. Kulkarni, D. Context-aware role-based access control in pervasive computing systems / D. Kulkarni, A. Tripathi // In: SACMAT ’08:Proceedings of the 13th ACM symposium on Access control models and technologies, New York, NY, USA, ACM, 2008. – P. 113–122.

122. Lampson, B. Authentication in distributed systems: Theory and practice / B. Lampson, M. Abadi, M. Burrows, E. Wobber // ACM Transactions on Computer Systems. – 1992. – № 10(4). – P. 265–310.

123. Lampson, B. Protection // ACM Oper. Syst. Rev. 8, 1. – P.18–24.

124. Medeisis, A. Fine tuning of the Okumura-Hata propagation prediction model using the minimum squares method and fuzzy logic approach // Fifteenth International Wroclaw Symposium and Exhibition on Electromagnetic Compatibility, EMC 2000. – P. 619–623.

125. Metropolis, N. The Monte Carlo Method / N. Metropolis, S. Ulam // Journal of the American Statistical Association. – 1949. – № 247. – P. 335–341.

126. Practical robust localization over large-scale 802.11 wireless networks / [A. Haeberlen, etc.] // in Proc. 10th ACM Int. Conf. Mobile Comput. Netw., Philadelphia, PA, Sep. 26–Oct. 1, 2004. – P. 70–84.

127. Propagation prediction models // COST 231 Final Rep. – Ch. 4. – P. 17–21.

128. Prasithsangaree, P. On indoor position with wireless LANs / P. Prasithsangaree, P. Krishnamurthi, P. K. Chrysanthis // in Proc. IEEE Int. Symp. Pers. Indoor, Mobile Radio Commun., Sep. 2002. – Vol. 2. – P. 720–724.

129. Ranganathan, A. MiddleWhere: A Middleware for Location Awareness in Ubiquitous Computing Applications. / A. Ranganathan, J. Al-Muhtadi, S. Chetan, R. Campbell, M.D. Mickunas : Jacobsen, H.-A. (ed.) Middleware 2004. LNCS. – 2004. – Vol. 3231. – P. 397–416.

130. Real Time Location System (RTLS) RFID-over-Wi-Fi Technology | Ekahau / Inc. Ekahau // Ekahau [Электронный ресурс] : сайт. – Электрон. дан. – 2014. Режим доступа: http://www.ekahau.com/real-time-location-system/technology. – Дата обращения: 05.09.2014 г.

131. Rice, S. O. Mathematical analysis of Random Noise / Bell System Technical Journal. – Vol. 23 (1944). – Vol. 24 (1945).

132. Robotics-based location sensing using wireless Ethernet / A. M. Ladd, K. E. Bekris, A. Rudys, G. Marceau, L. E. Kavraki, D. S. Wallach // In Proceedings of The Eighth ACM International Conference on Mobile Computing and Networking (MOBICOM), Atlanta, GA, Sept. 2002. – P. 189–204.

133. Rocha, C.C. A2BeST: An Adaptive Authentication Service Based on Mobile User`s Behavior Spatio-Temporal Context / Cristiano C. Rocha, Joao Carlos D. Lima, M.A.R. Dantas : IEEE Press. – 2011. – № 11. – P. 771–774.

134. Saunders, S. R. Antennas and Propagation for Wireless Communication Systems // New York, NY: Wiley. – 1999.

135. Sandhu, R. S. Access Control: Principles and Practice / R. Sandhu, P. Samarati // IEEE Communications. – 1994. – Vol.32, № 9. – P.40–49.

136. Sandhu, R. S. Lattice-Based Access Control Models / IEEE Computer. – 1993. – № 26(11). – P. 9–19.

137. Sandhu, R. S. Role-Based Access Control, Advanced in Computer // Academic Press. – 1998. – Vol 46.

138. Sandhu, R. S. Role hierarchies and constraints for lattice-based access controls // Proceedings of the Fourth European Symposium on Research in Computer Se-

curity (ESO-RICS96), E. Bertino, Ed. Springer-Verlag, New York. – 1996. – Vol. 1146. P. 65–79

139. Sandhu, R. S. Rationale for the RBAC96 family of access control models // Proceeding of the 1st ACM Workshop on Role-Based Access Control. – ACM, 1997.

140. Seidel, S. Y. 914 MHz path loss prediction Model for Indoor Wireless Communication in Multi-floored buildings / S. Y. Seidel, T. S. Rapport // IEEE Communication Magazine, April, 1998.

141. Scholten, H. Context Based Access Control / H. Scholten, P. Valkenburg, D. De Vreeze // Everett BV : Neterlands. – 2007. – 22 p.

142. Survey of Wireless Indoor Positioning Techniques and Systems / Hui Liu [etc.] // IEEE Transactions on systems, man, and cybernetics, part C : Applications and reviews. – 2007. – Vol.37. – No. 6. – P. 1067–1080.

143. Tekinay, S. Performance benchmarking for wireless location systems / S. Tekinay, E. Chao, and R. Richton // IEEE Commun. Mag. – 1998. – Vol. 36. – No. 4. – P. 72–76.

144. Trusted Computer System Evaluation Criteria. – US Department of Defense, 1985. – CSC-STD-001-83.

145. Using Wireless Ethernet For Localization / [A. M. Ladd, etc.] // in Proc. 2002 IEEE/RJS Int. Conf. Intell. Robots Syst. – 2002. – Vol. 1. – P. 402–408.

146. ViPNet Client для iOS и Android / ОАО "ИнфоТеКС" [Электронный ресурс] : Электрон. дан. – Москва, 2015. Режим доступа: http://infotecs.ru/products/catalog.php?SECTION_ID=&ELEMENT_ID=2870. – Дата обращения: 29.05.2015 г.

147. ViPNet Terminal / ОАО "ИнфоТеКС" [Электронный ресурс] : Электрон. дан. – Москва, 2015. Режим доступа: http://infotecs.ru/products/catalog.php?SECTION_ID=&ELEMENT_ID=5521. – Дата обращения: 29.05.2015 г.

148. Xin Jin RABAC: Role-Centric Attribute-Based Access Control / Xin Jin, Ravi Sandhu, Ram Krishnan // In MMM-ACNS. – 2012.

149. Youssef, M. WLAN location determination via clustering and probability distributions / M. Youssef, A. Agrawala, A. Udaya Shankar : IEEE Int. Conf. Pervasive Comput. Commun. – 2003. – P. 143–151.

150. Youssef, M. Handling samples correlation in the Horus system : IEEE INFOCOM 2004, Hong Kong. – 2004. – Vol. 2. – P. 1023–1031.

ПРИЛОЖЕНИЕ А

к стр. 98

Технологии определения местоположения мобильного абонентского устройства внутри здания на основе использования беспроводных сетей передачи данных

Сравнительный анализ точности методов трилатерации (триангуляции) [9, 109]; k-ближайших соседей [103, 104]; байесовского подхода [132] представлен на рисунке А.1.

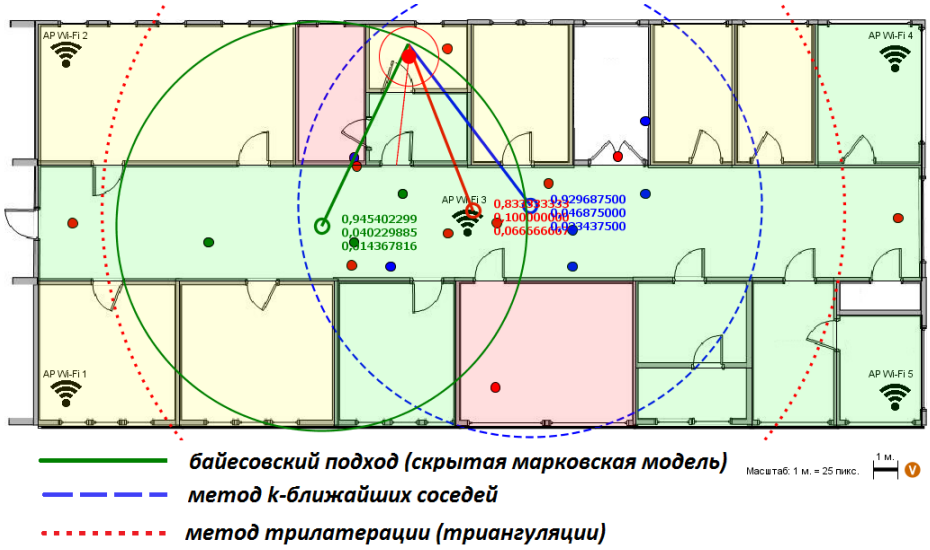


Рисунок А.1 – Сравнительный анализ точности исследуемых технологий определения местоположения

Сравнительный анализ распределения вероятности и плотности распределения ошибки измерений местоположения для исследуемых технологий приведены на рисунках А.2 и А.3.

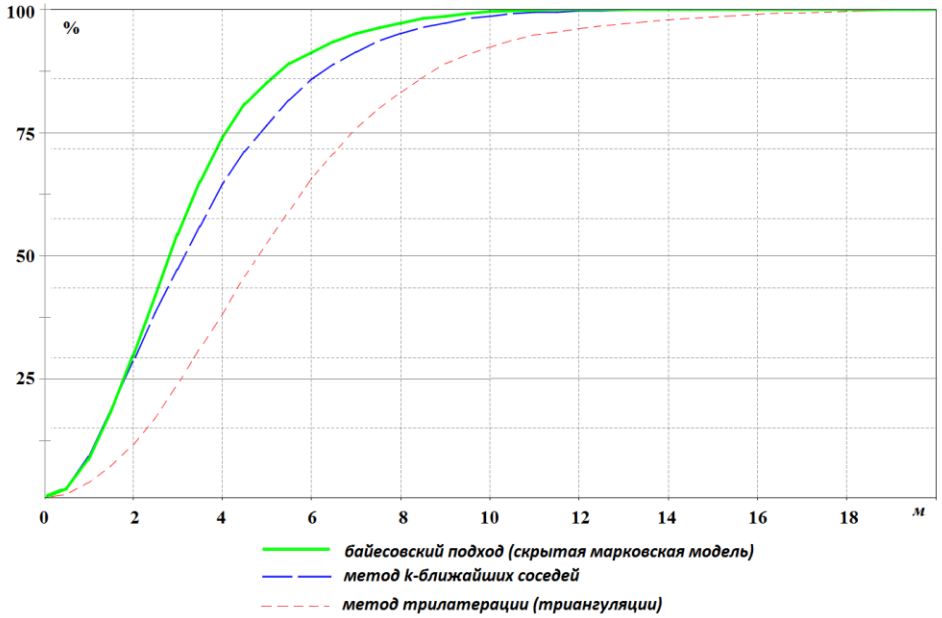
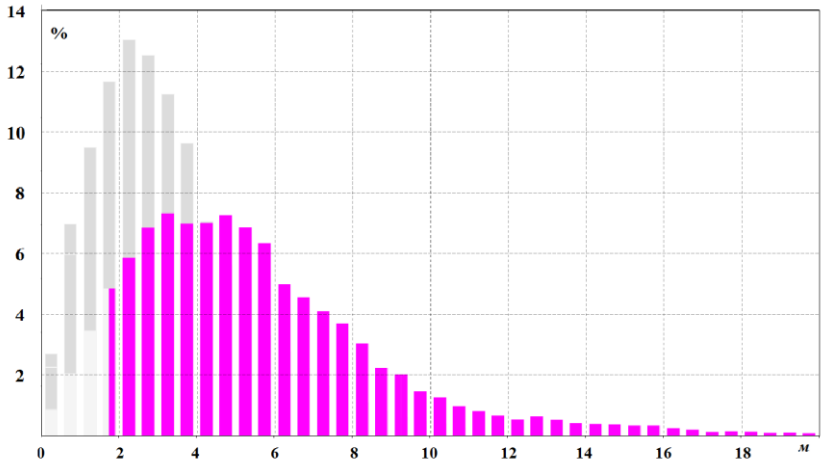
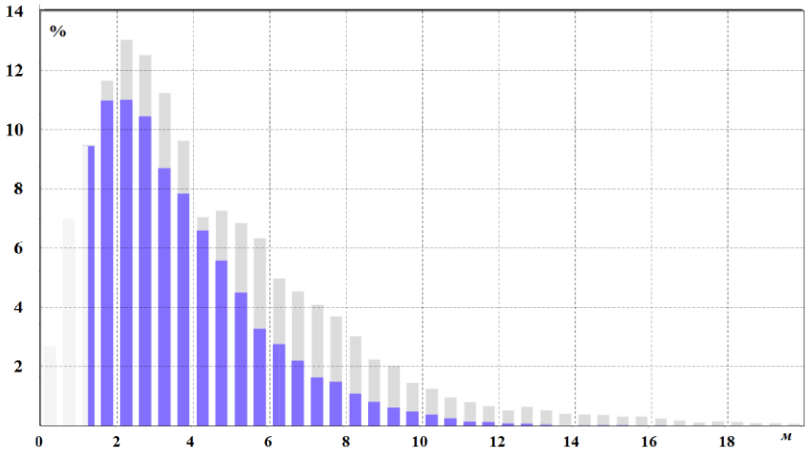


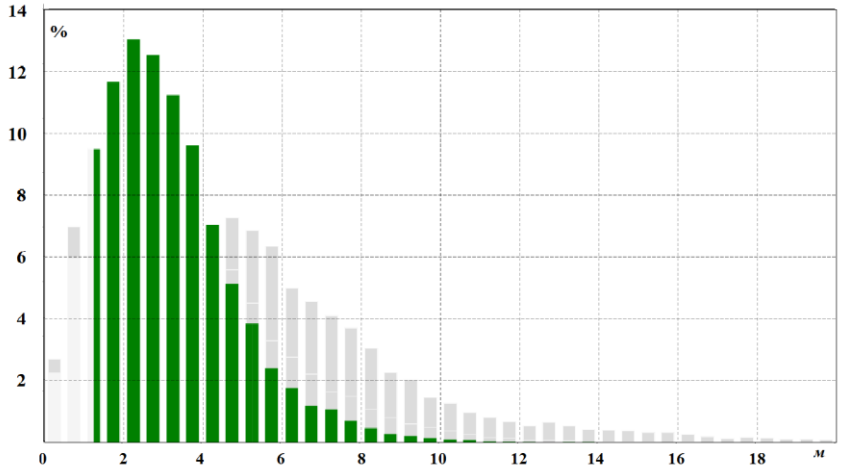
Рисунок А.2 – Сравнительный анализ функции распределения ошибки измерений местоположения для исследуемых способов



а)



б)



в)

Рисунок А.3 – Сравнительный анализ плотностей распределения ошибки измерений местоположения: а) трилатерация; б) метод k-ближайших соседей; в) байесовский подход

Данные методы отличаются по точности, трудоемкости и необходимой для их функционирования производительности вычислительных средств. Целесообразность применения того или иного метода зависит от конкретных условий эксплуатации.

Элементом системы определения местоположения является **описательная модель беспроводной сети передачи данных**, включающая в себя информацию о составе и местоположении точек доступа:

$$AP = \left\{ AP_i = \left(x_i, y_i \right) \right\}, i = \overline{1, N_{AP}}, \quad \text{(A.1)}$$

где $\left(x_i, y_i \right)$ – координаты i-й точки доступа; N_{AP} – количество точек доступа.

Описательная модель сигнального пространства здания необходима в случае использования технологий, использующих метод анализа карт и технологии машинного обучения. К таким методам относятся метод k-ближайших соседей [103, 104], байесовский подход (скрытых марковских моделей) [132] и другие.

В общем виде модель сигнального пространства можно представить как

$$MAP_{P_t} = \left\{ \left(x_i, y_i \right), \lambda_{P_t} \right\}, i = \overline{1, N_{MAP}}, \quad \text{(A.2)}$$

где (x_i, y_i) – координаты i-й точки измерений уровня сигнала МАУ; N_{MAP} – количество точек измерения; λ_{P_t} – статистика (для метода k-ближайших соседей – только уровень сигнала) измерений уровня сигнала.

Рассмотрим более детально исследуемые технологии определения местоположения МАУ в помещениях.

Метод трилатерации

Метод трилатерации (триангуляции) сигнала МАУ, принимаемого несколькими точками доступа БСПД [9, 109], базируется на принципах радиолокации. Для его реализации необходимо не менее трех разнесенных в пространстве измерителей уровня сигнала беспроводного модуля МАУ. При наличии достаточного количества измерителей для определения местоположения МАУ необходимо решить систему уравнений:

$$\begin{cases} (x-x_1)^2 + (y-y_1)^2 = R_1^2 \\ (x-x_2)^2 + (y-y_2)^2 = R_2^2 \\ \dots \\ (x-x_n)^2 + (y-y_n)^2 = R_n^2 \end{cases}, \quad \text{(A.3)}$$

где (x, y) – координаты МАУ; (x_i, y_i), $i = \overline{1,n}$ – координаты точек доступа БСПД, а n – их количество; R_i – оценки расстояния от точек доступа до МАУ.

Для вычисления расстояния до МАУ в работе [9] предложено использовать формулу потерь в свободном пространстве для идеальной изотропной антенны [66, стр. 72]:

$$\frac{P_t}{P_r} = \frac{(4\pi R)^2}{\lambda^2}, \quad \text{(A.4)}$$

где P_t – мощность сигнала передающей антенны; P_r – мощность сигнала, поступающего на антенну приемника; λ – длина волны несущей, определяемой выражением $\lambda = \frac{c}{f}$, где c – скорость света, а f – центральная частота несущей; R – расстояние, пройденное сигналом между двумя антеннами.

Тогда выражение для оценки расстояния примет вид:

$$R = \frac{\lambda}{4\pi} \cdot \sqrt{\frac{P_t G_t G_r}{P_r}} . \qquad (A.5)$$

Очевидно, что выражение (А.4) является значительно упрощенной моделью распространения радиосигналов внутри помещений, не учитывающей такие факторы [119] как:

– отражение от стен и полов;

– дифракция, рассеяние и поглощение радиоволн материалами стен, дверей, перегородок и других структурных элементов строения;

– многолучевый прием сигнала;

– помеховая обстановка.

Исследования, проведенные в работах [103, 104], показывают, что использование сложных моделей распространения сигналов в ряде случаев неэффективно. Так, например модель затуханий Рэлея [112] использует критическое предположение, что все сигналы, достигающие принимающего устройства, имеют одинаковую мощность, что на практике недостижимо. Кроме того, исследования показывают, что все сигналы, поступающие на приемник, имеют доминирующий компонент мощности от линии прямой видимости между приемником и передатчиком, а данная модель ее не учитывает.

Другая модель распределения Райса [131] учитывает мощность сигнала прямой видимости. Данная модель является частным случаем модели затухания Рэлея, но при этом для ее задания необходимо определить достаточно большое количество параметров, что на практике является проблематично [103].

Наиболее целесообразно для учета указанных факторов использовать такие модели распространения радиоволн как модель Ли [134], Хата [124, 134], Окамуры [124, 134], COST231-Хата [134], COST231-Уолфиш-Икегами [127], модифицированная модель Хата [127], поскольку они более адекватно учитывают условия распространения радиоволн внутри помещений. Для расчета затухания мощности сигнала МАУ в данной работе использовалось выражение COST231-Хата [134]:

$$\bar{L}_e = 46{,}3 + 33{,}9 \cdot \lg f - 13{,}82 \cdot \lg h_t - \left[(1{,}1 \cdot \lg f - 0{,}7) h_r - (1{,}56 \cdot \lg f - 0{,}8) \right] + \\ + (44{,}9 - 6{,}55 \cdot \lg h_t) \cdot \lg d + C, \quad \text{(A.6)}$$

где f – частота передатчика; h_t – высота антенны передатчика; h_r – высота антенны приемника; d – расстояние до передатчика МАУ; C – поправочный коэффициент, учитывающий пересеченность зоны распространения сигнала МАУ, а также выражение на основе стандарта ITU-R P.1238-7 [119]:

$$L = 20 \cdot \lg f + N \cdot \lg d + P_f(n) - 28, \quad \text{(A.7)}$$

где f – частота передатчика (МГц); N – дистанционный коэффициент потерь мощности; d – расстояние до передатчика МАУ; $P_f(n)$ – коэффициент потерь за счет прохождения сигнала через пол (дБ); n – количество этажей.

В качестве компромисса могут быть использованы модели распространения сигналов, учитывающих поглощение сигналов материалами стен и других конструктивных элементов здания, предложенные в работах [14, 103, 140]:

$$P(d)[\text{дБм}] = P(d_0)[\text{дБм}] - 10n \log\left(\frac{d}{d_0}\right) - \begin{cases} n \cdot WAF, nW < C \\ C \cdot WAF, nW \geq C \end{cases}, \quad \text{(A.8)}$$

где n – количество стен (этажей); $P(d_0)$ – мощность сигнала в начальной точке, а $P(d)$ – в точку приема; C – максимальное количество препятствий (стен, перегородок, этажей); WAF – коэффициент затухания радиоволн, проходящих через препятствие. Очевидно, что при использовании данной модели для каждого отдельно взятого помещения необходимо задавать массив величин, определяющих параметры затухания, что существенно усложнит систему определения местоположения.

Поскольку предполагается, что используются доверенные МАУ, а также доверенная сеть точек доступа БСПД, то параметры P_t, P_r, G_t, G_r, f известны. Для вычисления координат МАУ на основе выражения (А.3) необходимо попарно вычислить точки пересечения окружностей, радиусами которых являются вычисленные на основе выражения (А.4) расстояния до передатчика МАУ с известными

центрами в местах расположения точек доступа БСПД. Решение данной задачи основывается на аналитической геометрии и состоит из следующих этапов.

1) перенос системы координат сдвигом таким образом, чтобы центр первой окружности оказался в начале координат:

$$\begin{pmatrix} \bar{x} \\ \bar{y} \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} - \begin{pmatrix} x_1 \\ y_2 \end{pmatrix}; \tag{A.9}$$

2) преобразование в новой системе координат к виду:

$$\begin{cases} \bar{x}^2 + \bar{y}^2 = R_1^2 \\ \left(\bar{x} - \bar{x}_2\right)^2 + \left(\bar{y} - \bar{y}_2\right)^2 = R_2^2 \end{cases}, \tag{A.10}$$

где $\bar{x}_2 = x_2 - x_1$ и $\bar{y}_2 = y_2 - y_1$;

3) поворот системы координат таким образом, чтобы центр второй окружности оказался на оси абсцисс:

$$\begin{pmatrix} \bar{\bar{x}} \\ \bar{\bar{y}} \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix} \cdot \begin{pmatrix} \bar{x} \\ \bar{y} \end{pmatrix}, \tag{A.11}$$

где $\alpha = \cos\upsilon = \dfrac{\bar{x}^2}{\sqrt{\bar{x}^2 + \bar{y}^2}}$, $\beta = \sin\upsilon = \dfrac{\bar{y}^2}{\sqrt{\bar{x}^2 + \bar{y}^2}}$, υ – угол поворота;

4) решение системы уравнений с двумя неизвестными:

$$\begin{cases} \bar{\bar{x}}^2 + \bar{\bar{y}}^2 = R_1^2 \\ \left(\bar{\bar{x}} - \sqrt{\bar{x}_2^2 + \bar{y}_2^2}\right)^2 + \bar{\bar{y}}^2 = R_2^2 \end{cases}. \tag{A.12}$$

Вследствие того, что реальные уровни сигналов всегда отличаются от идеальных, то возможны несколько вариантов расположения окружностей друг относительно друга.

Вариант 1. Окружности не пересекаются: $R_1 + R_2 > \sqrt{\left(x_2 - x_1\right)^2 + \left(y_2 - y_1\right)^2}$ или $\left|R_1 + R_2\right| > \sqrt{\left(x_2 - x_1\right)^2 + \left(y_2 - y_1\right)^2}$.

Вариант 2. Окружности пересекаются в одной или двух точках: $R_1 + R_2 \le \sqrt{\left(x_2 - x_1\right)^2 + \left(y_2 - y_1\right)^2}$

В первом варианте формально решений нет, поскольку система уравнений несовместна, поэтому в качестве точек пересечения выбирается точка, лежащая в центре прямой, соединяющей центры окружности. В этом случае в преобразованной системе координат решением будут точки:

$$\overline{\overline{x}}_{1,2} = \pm R_2,\ \overline{\overline{x}}_{3,4} = \sqrt{\overline{x}_2^2 + \overline{y}_2^2} \pm R_2. \qquad \text{(A.13)}$$

Далее, необходимо найти индексы, для которых расстояние минимально и вычислить начальное приближение:

$$(k,l) = \arg\min_{\substack{k\in\{1,2\}\\ l\in\{3,4\}}} \left|\overline{x}_k - \overline{x}_l\right|, \qquad \text{(A.14)}$$

$$\overline{\overline{x}} = \frac{\overline{\overline{x}}_l + \overline{\overline{x}}_k}{2}, \qquad \text{(A.15)}$$

$$\overline{\overline{y}} = 0. \qquad \text{(A.16)}$$

Во втором варианте точки пересечения определяются выражениями:

$$\overline{\overline{x}} = \frac{R_1^2 - R_2^2 + \overline{x}_2^2 + \overline{y}_2^2}{2\cdot\sqrt{\overline{x}_2^2 + \overline{y}_2^2}}, \qquad \text{(A.17)}$$

$$\overline{\overline{y}} = \pm\sqrt{R_1^2 - \overline{\overline{x}}^2}. \qquad \text{(A.18)}$$

Полученные координаты точки с помощью обратных преобразований приводятся к исходной системе координат, и затем находится средняя точка, являющая искомой. В случаях, когда точек доступа больше двух, расчеты осуществляются попарно для всех пар точек доступа. Геометрическая интерпретация данного метода для случая с тремя точками доступа представлена на рисунке А.4.

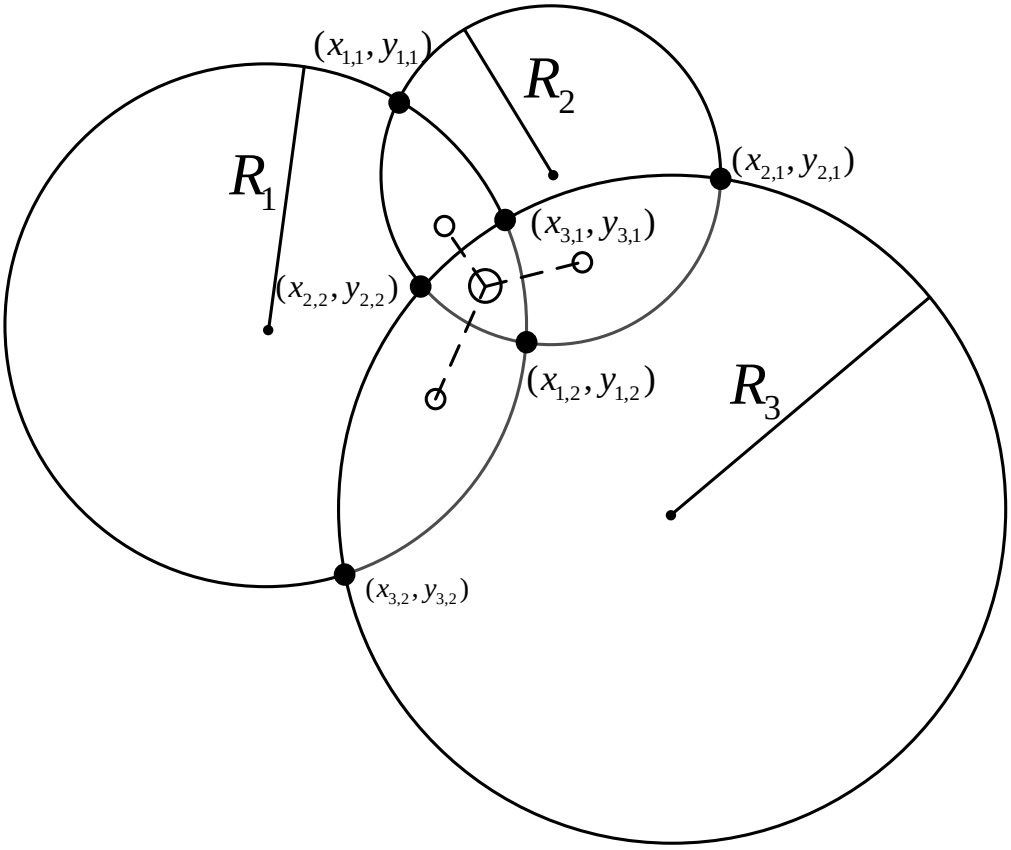


Рисунок А.4 – Геометрическая интерпретация метода трилатерации при определении местоположения

Выражение для искомой точки $(\tilde{x}_{tr}, \tilde{y}_{tr})$ вычисляемого местоположения пользователя МАУ:

$$\tilde{x}_{tr} = \frac{1}{2 \cdot N_{AP}} \cdot \sum_{i=1}^{N_{AP}} \sum_{j=1}^{2} x_{i,j} \, , \tilde{y}_{tr} = \frac{1}{2 \cdot N_{AP}} \cdot \sum_{i=1}^{N_{AP}} \sum_{j=1}^{2} y_{i,j} \, . \qquad \text{(A.19)}$$

Метод *k*-ближайших соседей

Метод k-ближайших соседей по определению местоположения МАУ является одним из методов интеллектуального анализа данных с обучением и с учителем. Предварительно необходимо составление карты измерений уровней сигнала (карта сигнального пространства) в разных точках с известными координатами, а также, возможно, известной ориентацией передающего устройства.

Обучающая выборка для такой карты сигнального пространства имеет вид:

$$X^{N_{kNN}} = \left\langle \left\{ \left(x_i, y_i \right), \upsilon_i \right\}, P_{r_i}^{RSS} \right\rangle, \tag{A.20}$$

где $\left(x_i, y_i \right)$ – координаты i-й точки карты сигнального пространства; υ_i – угол ориентации в пространстве МАУ; $P_{r_i}^{RSS}$ – уровень мощности принимаемого сигнала от МАУ; $i = \overline{1, N}_{kNN}$ – индекс точки измерений карты сигнального пространства, а N_{kNN} – их количество.

В качестве метрики для вычисления расстояния между текущими измерениями уровня сигнала и значениями, хранящимися в карте сигнального пространства, целесообразно использовать метрику Евклида:

$$d_{Evkl}\left(\tilde{P}_r^{RSS}, P_{r_i}^{RSS} \right) = \sqrt{\sum_{j=1}^{N_{AP}} \left(\tilde{P}_{r_j}^{RSS} - P_{r_{i,j}}^{RSS} \right)^2}, \tag{A.21}$$

где $\tilde{P}_r^{RSS} = \left\{ \tilde{P}_{r_j}^{RSS} \right\}, j = \overline{1, N}_{AP}$ – текущие измерения уровня сигнала N_{AP} точками доступа; $P_{r_i}^{RSS} = \left\{ P_{r_{i,j}}^{RSS} \right\}, j = \overline{1, N}_{AP}, i = \overline{1, N}_{kNN}$ – измерения уровня сигнала в i-й точке карты сигнального пространства N_{AP} точками доступа; N_{kNN} – количество точек сигнального пространства.

Также допустимо использовать метрику Манхэттена (метрика городских кварталов, метрика Миньковского, метрика такси):

$$d_{Mink_i}\left(\tilde{P}_r^{RSS}, P_{r_i}^{RSS} \right) = \left| \sum_{j=1}^{N_{AP}} \left(\tilde{P}_{r_j}^{RSS} - P_{r_{i,j}}^{RSS} \right) \right|. \tag{A.22}$$

Для произвольного местоположения МАУ $(\tilde{x}_{kNN}, \tilde{y}_{kNN})$ в соответствие с выбранной метрикой обучающая выборка упорядочивается в порядке возрастания расстояния от $\tilde{P}_r^{RSS}$ до $P_{r_i}^{RSS}$:

$$d_{Evkl}\left(\tilde{P}_r^{RSS}, P_{r_{1;u}}^{RSS} \right) \le d_{Evkl}\left(\tilde{P}_r^{RSS}, P_{r_{2;u}}^{RSS} \right) \le \ldots \le d_{Evkl}\left(\tilde{P}_r^{RSS}, P_{r_{N_{kNN};u}}^{RSS} \right), \tag{A.23}$$

где $P_{r_{i;u}}^{RSS}$, $i = \overline{1, N}_{kNN}$ – i-й сосед из обучающей выборки $X^{N_{kNN}}$.

Таким образом, каждый набор измерений $\tilde{P}_r^{RSS}$ порождает свою нумерацию упорядоченной выборки. Тогда в общем виде метод k-ближайших соседей можно представить в виде:

$$a_{kNN}(u=\tilde{P}_r^{RSS})=\arg\min_{x_i,y_i}\sum_{i=1}^{N_{kNN}}\left[d_{Evkl_i}\left(\tilde{P}_r^{RSS},P_{r_i}^{RSS}\right)\right]\cdot\omega(i,u), \qquad (A.24)$$

где $\omega(i,u)=[i\le k]$ – весовая функция, оценивающая степень важности i-го соседа. Тогда координаты $(\tilde{x}_{kNN},\tilde{y}_{kNN})$ местоположения МАУ будут определяться выражением

$$\tilde{x}_{kNN}=\frac{1}{k}\cdot\sum_{i=1}^{k}x_i\,,\ \tilde{y}_{kNN}=\frac{1}{k}\cdot\sum_{i=1}^{k}y_i\,. \qquad (A.25)$$

Метод на основе байесовского классификатора

В основе метода определения местоположения на базе байесовского подхода [132] также как и для метода k-ближайших соседей лежит карта сигнального пространства. Отличие заключается в том, что в каждой точке здания с известными координатами в карте сигнального пространства хранятся не данные об одном измерении уровня сигнала МАУ, а статистика измерений уровней сигналов. Многочисленные исследования [14, 50, 99, 103, 132] статистики измерений уровня сигнала БСПД в диапазонах 2,4-5 ГГц показывают, что уровень сигнала является стохастической величиной, зависящей от множества факторов, поэтому можно сделать обоснованное предположение, что учет статистики распределения уровня сигнала в каждой точке с известными координатами позволит более точно определить местоположение МАУ.

Для метода на основе байесовского подхода необходимо осуществить сбор статистики измерений уровня сигнала в каждой точке. Обучающая выборка для такой карты сигнального пространства имеет вид:

$$X^{N_{HMM}}=\left\langle(x_i,y_i),P_{r_i}\left[\lambda_i/(x_i,y_i)\right]\right\rangle,i=\overline{1,N}_{HMM}\,, \qquad (A.26)$$

где (x_i,y_i) – координаты i-й точки карты сигнального пространства; $P_{r_i}\left[\lambda_i/(x_i,y_i)\right]$ – условная вероятность получения измерений сигнала передатчика

МАУ со статистическим распределением λ_i в точке с координатами (x_i, y_i); N_{HMM} – количество точек сигнального пространства обучающей выборки.

Для использования байесовского подхода при определении местоположения МАУ процесс определения местоположения представляется в виде скрытой марковской модели:

$$\lambda = \{A, B, \pi\}, \qquad (A.27)$$

где $A = \{a_{ij}\}$ – матрица переходных вероятностей для "скрытых" состояний $s_i, i = \overline{1, N}_{HMM}$, где a_{ij} – вероятность перехода из i-го в j-е состояние, $i, j = \overline{1, N}_{HMM}$;

$S = \{s_i\}$ – множество состояний скрытой Марковской модели;

$s_i = (x_i, y_i)$ – i-е состояние скрытой Марковской модели;

(x_i, y_i) – координаты точки в здании;

N_{HMM} – количество точек сигнального пространства с известными координатами;

$B = \left\{P_r(o_j / s_i) = P_r\left[\lambda_j / (x_i, y_i)\right]\right\}$ – матрица функций условных распределений вероятностей наблюдения символов o_j при условии нахождения в состоянии s_i, где $i = \overline{1, N}_{HMM}$, $j = \overline{1, m}$, m – количество допустимых наблюдений;

$o_j = \left\{\left(b_1, P_{r_1}^{RSS}\right), \left(b_2, P_{r_2}^{RSS}\right), ..., \left(b_k, P_{r_k}^{RSS}\right)\right\}$ – j-е допустимое наблюдение;

b_k – номер k-й точки доступа, осуществляющей измерение уровня сигнала;

$P_{r_k}^{RSS}$ –уровень сигнала k-й точкой доступа беспроводной сети;

$\pi = \{\pi_i\}$, $i = \overline{1, N}_{HMM}$ – начальное распределение вероятностей состояний скрытой Марковской модели.

Для определения местоположения МАУ – наиболее вероятного состояния скрытой Марковской модели – используют выражение:

$$\pi'_i = \frac{\pi_i P_r\left(o_j / s_i\right)}{\sum_{k=1}^{N_{HMM}} \pi_k \cdot P_r\left(o_j / s_k\right)}. \qquad \text{(A.28)}$$

Тогда координаты наиболее вероятного местоположения МАУ можно получить, используя выражение:

$$\left(x_i, y_i\right) = \arg\max\left(\pi'_i\right). \qquad \text{(A.29)}$$

Поскольку значения условных вероятностей являются достаточно маленькими, то целесообразно использовать логарифмическую шкалу при определении вектора π'_i либо применять дополнительную обработку данных с нормированием:

$$\pi''_i = \left(\pi_1 + u_1\right) \cdot \left(\pi'_i + u_2\right), \qquad \text{(A.30)}$$

где u_1, u_2 – малые константы, необходимые для избегания обнуления значений вектора вероятностей состояний при вычислениях. Обнуление значений связанно с недостаточной разрядностью мантиссы чисел с плавающей точкой.

Проведенные исследования [43, 51] показали, что точность определения местоположения можно повысить, используя для определения местоположения МАУ k значений наиболее вероятных состояний. Иными словами, для вычисления координат предложено использовать первые k значений вектора вероятностей состояний скрытой Марковской модели. Тогда координаты $\left(\tilde{x}_{HMM}, \tilde{y}_{HMM}\right)$ местоположения МАУ будут определяться выражением

$$\tilde{x}_{HMM} = \frac{1}{k} \cdot \sum_{i=1}^{k} \arg\max_{x_i}\left(\pi'_i\right), \tilde{y}_{HMM} = \frac{1}{k} \cdot \sum_{i=1}^{k} \arg\max_{y_i}\left(\pi'_i\right). \qquad \text{(A.31)}$$

ПРИЛОЖЕНИЕ Б

к стр. 98

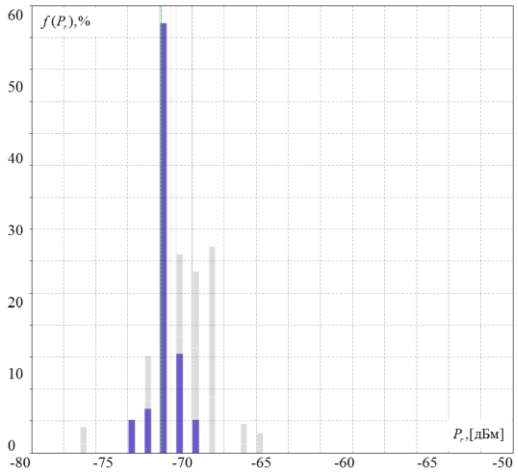
Результаты экспериментов по измерению колебаний уровня мощности сигналов базовых станций беспроводной сети передачи данных

Таблица Б.1 – Измерения колебаний уровня сигнала от базовых станций

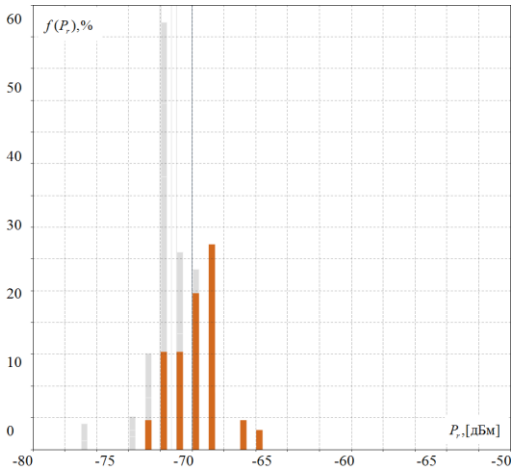
№ измерения	Положение 1			Положение 2			Положение 3			Положение 4		
	БС1, дБм	БС2, дБм	БС3, дБм	БС1, дБм	БС2, дБм	БС3, дБм	БС1, дБм	БС2, дБм	БС3, дБм	БС1, дБм	БС2, дБм	БС3, дБм
1	2	3	4	5	6	7	8	9	10	11	12	13
1	-72	-63	-63	-71	-59	-64	-72	-61	-66	-71	-57	-64
2	-72	-63	-64	-72	-63	-58	-72	-61	-70	-70	-56	-64
3	-71	-65	-63	-71	-55	-59	-70	-59	-69	-72	-57	-63
4	-72	-61	-63	-69	-59	-69	-71	-63	-66	-72	-57	-64
5	-72	-60	-64	-66	-59	-59	-73	-57	-70	-71	-55	-66
6	-72	-57	-63	-72	-59	-59	-72	-55	-67	-71	-56	-59
7	-72	-60	-63	-69	-64	-59	-72	-59	-64	-70	-56	-59
8	-72	-63	-63	-69	-57	-59	-70	-57	-66	-71	-55	-59
9	-72	-61	-64	-70	-57	-59	-72	-55	-61	-72	-57	-59
10	-72	-63	-64	-71	-58	-59	-72	-60	-65	-72	-59	-66
11	-72	-60	-64	-69	-63	-59	-72	-63	-63	-72	-57	-59
12	-72	-63	-63	-71	-59	-59	-73	-66	-67	-73	-56	-64
13	-72	-63	-64	-70	-57	-59	-72	-59	-70	-70	-58	-64
14	-71	-63	-63	-72	-57	-59	-72	-60	-69	-72	-55	-59
15	-74	-61	-63	-72	-58	-59	-72	-64	-66	-72	-57	-66
16	-72	-63	-64	-69	-59	-61	-72	-59	-70	-70	-56	-64
17	-71	-65	-63	-70	-65	-59	-72	-59	-67	-72	-59	-64
18	-72	-71	-63	-69	-64	-67	-73	-59	-66	-72	-58	-64
19	-71	-59	-61	-70	-63	-59	-70	-59	-66	-70	-54	-66
20	-72	-57	-64	-70	-65	-59	-72	-57	-70	-71	-55	-59
21	-72	-57	-66	-70	-64	-60	-73	-59	-66	-71	-57	-59
22	-72	-60	-63	-69	-58	-59	-73	-67	-67	-72	-56	-66
23	-72	-64	-63	-72	-55	-63	-72	-64	-64	-72	-59	-64
24	-71	-59	-63	-71	-55	-59	-72	-63	-71	-71	-56	-64
25	-72	-61	-63	-71	-59	-59	-72	-63	-70	-70	-54	-64
26	-72	-66	-64	-71	-57	-61	-72	-65	-70	-71	-57	-59
27	-73	-63	-64	-70	-59	-58	-70	-63	-70	-72	-58	-59
28	-74	-64	-64	-69	-63	-59	-72	-66	-69	-70	-56	-59
29	-74	-59	-63	-66	-63	-59	-71	-60	-64	-69	-54	-72
30	-72	-63	-63	-72	-59	-59	-72	-60	-69	-70	-57	-60

Окончание таблицы Б.1

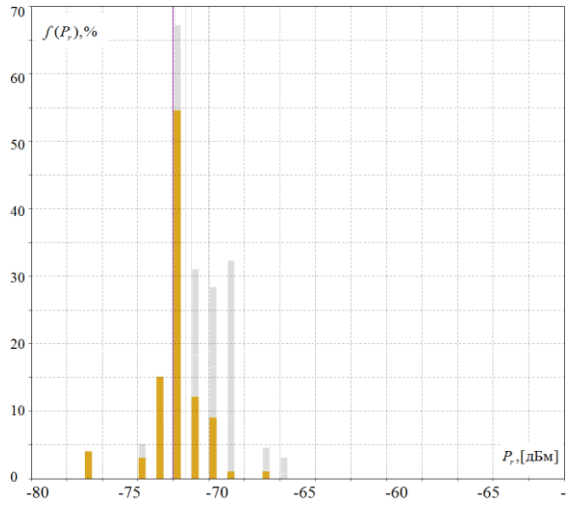
№ измерения.	Положение 1			Положение 2			Положение 3			Положение 4		
	БС1, дБм	БС2, дБм	БС3, дБм	БС1, дБм	БС2, дБм	БС3, дБм	БС1, дБм	БС2, дБм	БС3, дБм	БС1, дБм	БС2, дБм	БС3, дБм
31	-72	-59	-63	-69	-59	-63	-73	-59	-69	-71	-59	-64
32	-72	-63	-63	-69	-57	-59	-73	-61	-66	-70	-57	-69
33	-73	-64	-64	-70	-59	-64	-72	-59	-70	-70	-57	-69
34	-71	-63	-71	-70	-55	-64	-72	-58	-67	-72	-58	-69
35	-72	-63	-71	-70	-61	-59	-73	-64	-66	-70	-54	-69
36	-72	-59	-61	-69	-55	-70	-73	-63	-67	-70	-55	-70
37	-72	-61	-63	-69	-58	-59	-72	-63	-70	-72	-57	-63
38	-71	-59	-63	-69	-57	-59	-72	-60	-70	-71	-55	-69
39	-72	-60	-64	-69	-57	-59	-72	-60	-70	-70	-54	-69
40	-71	-59	-66	-69	-57	-69	-71	-59	-67	-72	-59	-69
41	-72	-57	-66	-73	-58	-64	-67	-58	-70	-70	-57	-64
42	-72	-59	-64	-73	-57	-64	-71	-64	-66	-71	-58	-69
43	-70	-60	-66	-72	-57	-64	-70	-63	-70	-71	-54	-70
44	-72	-63	-63	-69	-59	-67	-72	-63	-69	-71	-56	-69
45	-70	-60	-64	-71	-55	-63	-71	-69	-67	-71	-55	-71
46	-72	-63	-64	-70	-55	-64	-72	-63	-66	-70	-56	-70
47	-73	-59	-63	-67	-57	-63	-71	-64	-65	-73	-58	-70
48	-72	-61	-63	-70	-55	-63	-72	-64	-65	-70	-57	-69
49	-72	-67	-64	-70	-63	-63	-72	-66	-67	-70	-55	-67
50	-72	-59	-65	-72	-57	-64	-72	-69	-64	-71	-57	-63
51	-72	-59	-64	-69	-63	-59	-72	-66	-67	-72	-55	-64
52	-72	-59	-64	-69	-59	-59	-71	-61	-64	-70	-55	-64
53	-71	-59	-63	-71	-59	-60	-72	-64	-67	-69	-55	-63
54	-72	-59	-64	-69	-66	-63	-72	-64	-64	-71	-55	-70
55	-73	-58	-63	-67	-66	-59	-72	-65	-61	-69	-54	-64



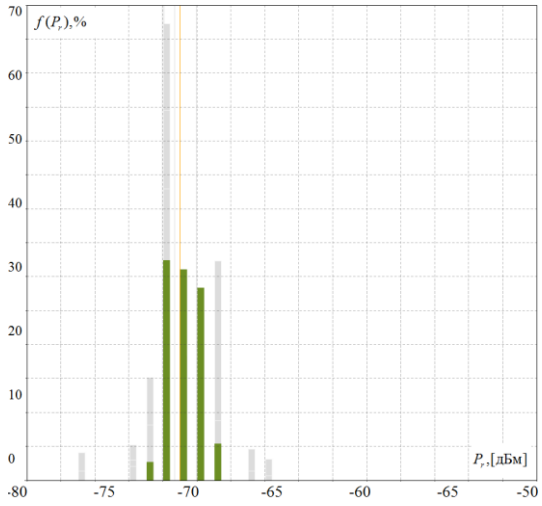
а) Точка доступа № 1, положение 1



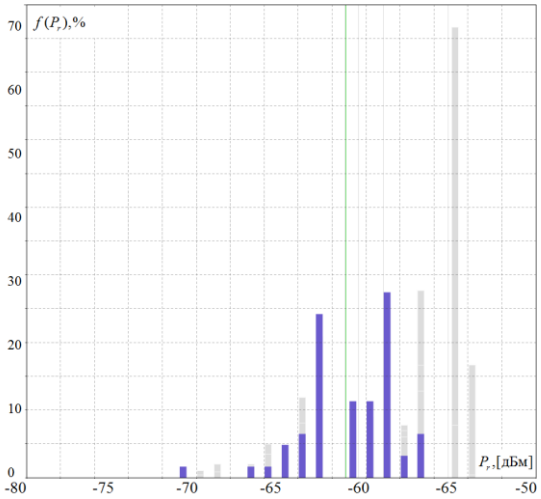
б) Точка доступа № 1, положение 2



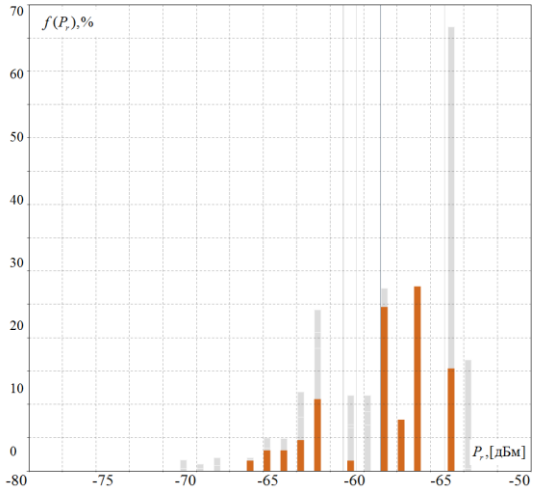
в) Точка доступа № 1, положение 3



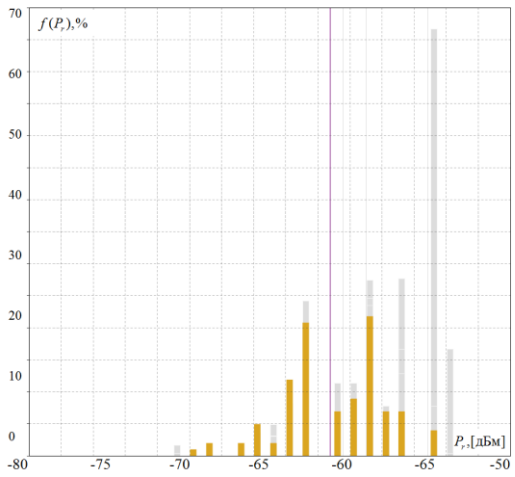
г) Точка доступа № 1, положение 4



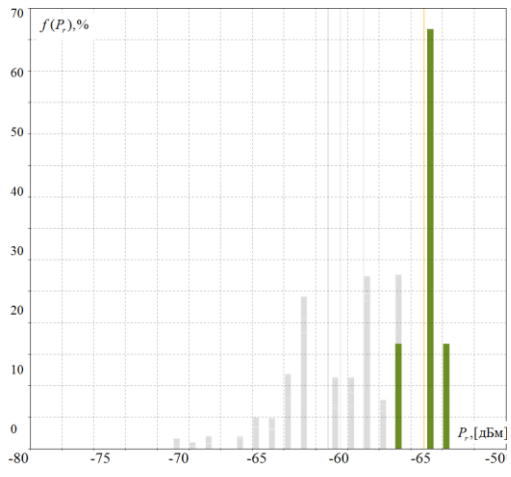
д) Точка доступа № 2, положение 1



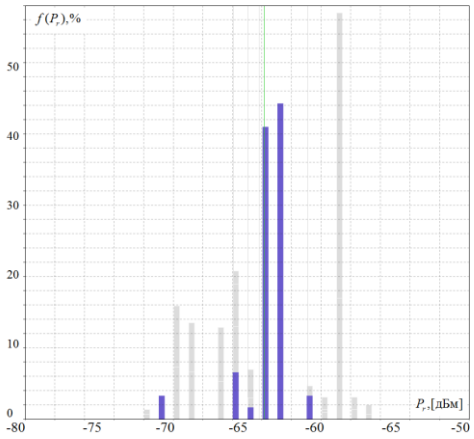
е) Точка доступа № 2, положение 2



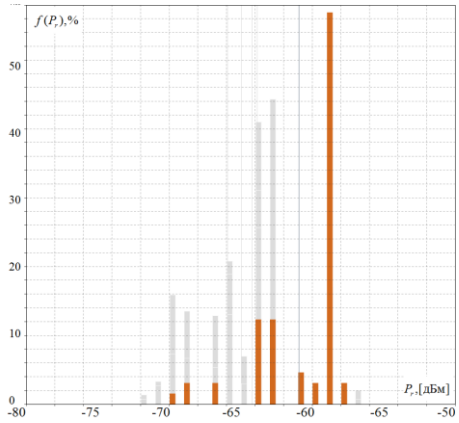
ж) Точка доступа № 2, положение 3



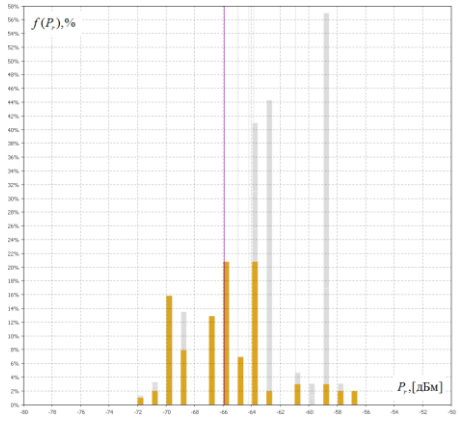
и) Точка доступа № 2, положение 4



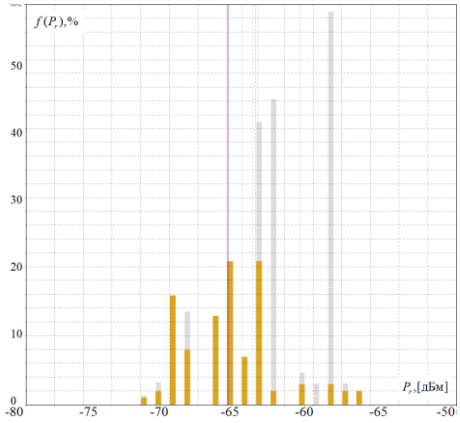
к) Точка доступа № 3, положение 1



л) Точка доступа № 3, положение 2



м) Точка доступа № 3, положение 3



н) Точка доступа № 3, положение 4

Рисунок Б.1 – Плотности распределения вероятностей уровней мощности сигнала точек доступа (ТД) 1-3 в различных положения:
а) ТД № 1, положение 1; б) ТД № 1, положение 2; в) ТД № 1, положение 3; г) ТД № 1, положение 4; д) ТД № 2, положение 1; е) ТД № 2, положение 2; ж) ТД № 2, положение 3; и) ТД № 2, положение 4; к) ТД № 3, положение 1; л) ТД № 3, положение 2; м) ТД № 3, положение 3; н) ТД № 3, положение 4.

СПРАВКА

Материалы получены с использованием [39, 79] и изложены в [42, 43]. Представленные сведения необходимы для обоснования параметров имитационной модели, используемой для моделирования определения местонахождения МАУ в специальных помещениях и оценивания оптимальных параметров частных моделей определения местоположения.

Д. О. Маркин

ПРИЛОЖЕНИЕ В

к стр. 101

Моделирующий алгоритм имитационной модели определения местоположения мобильного абонентского устройства

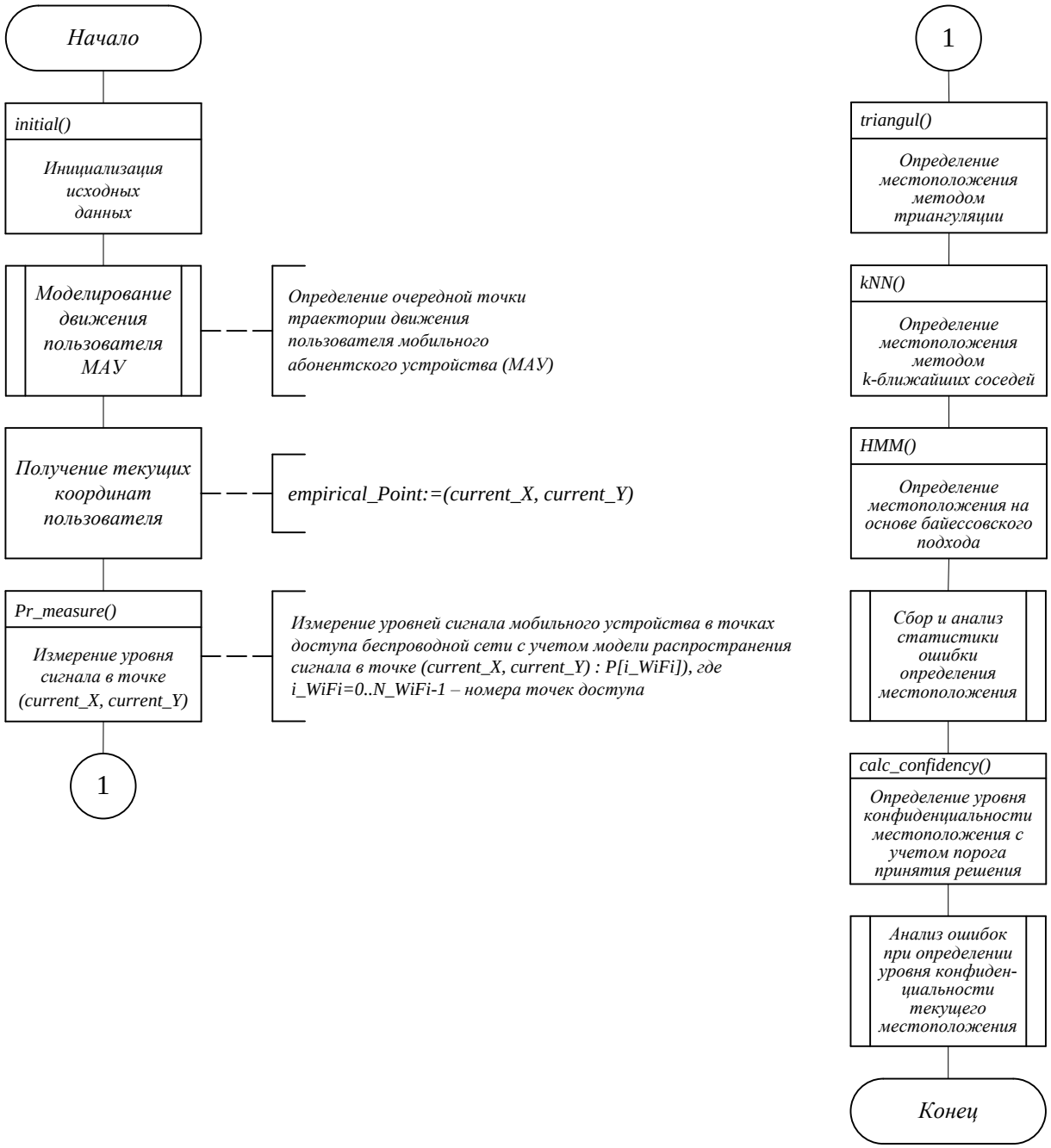


Рисунок В.1 – Блок-схема общего моделирующего алгоритма

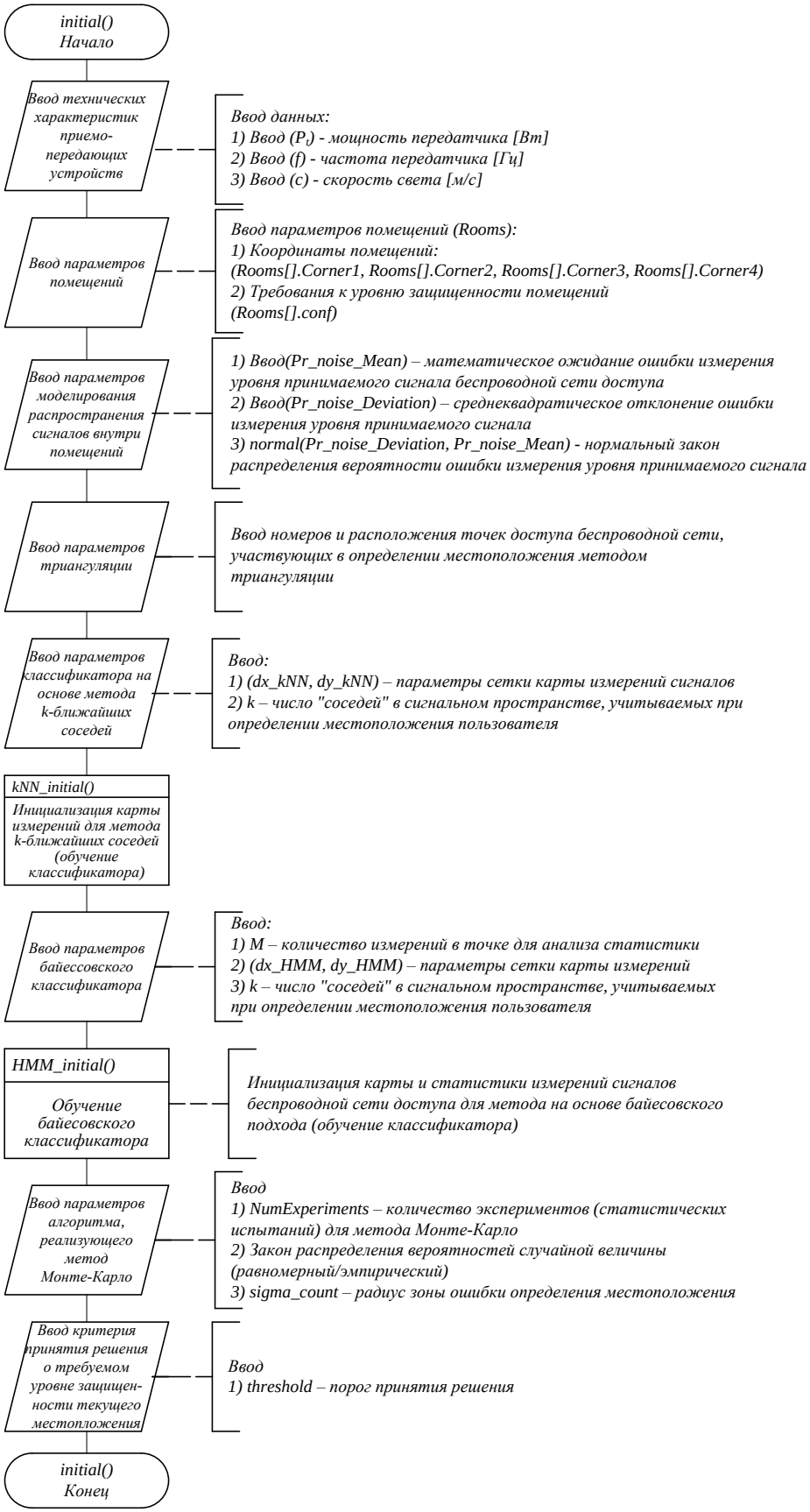


Рисунок В.2 – Блок-схема алгоритма инициализации входных данных

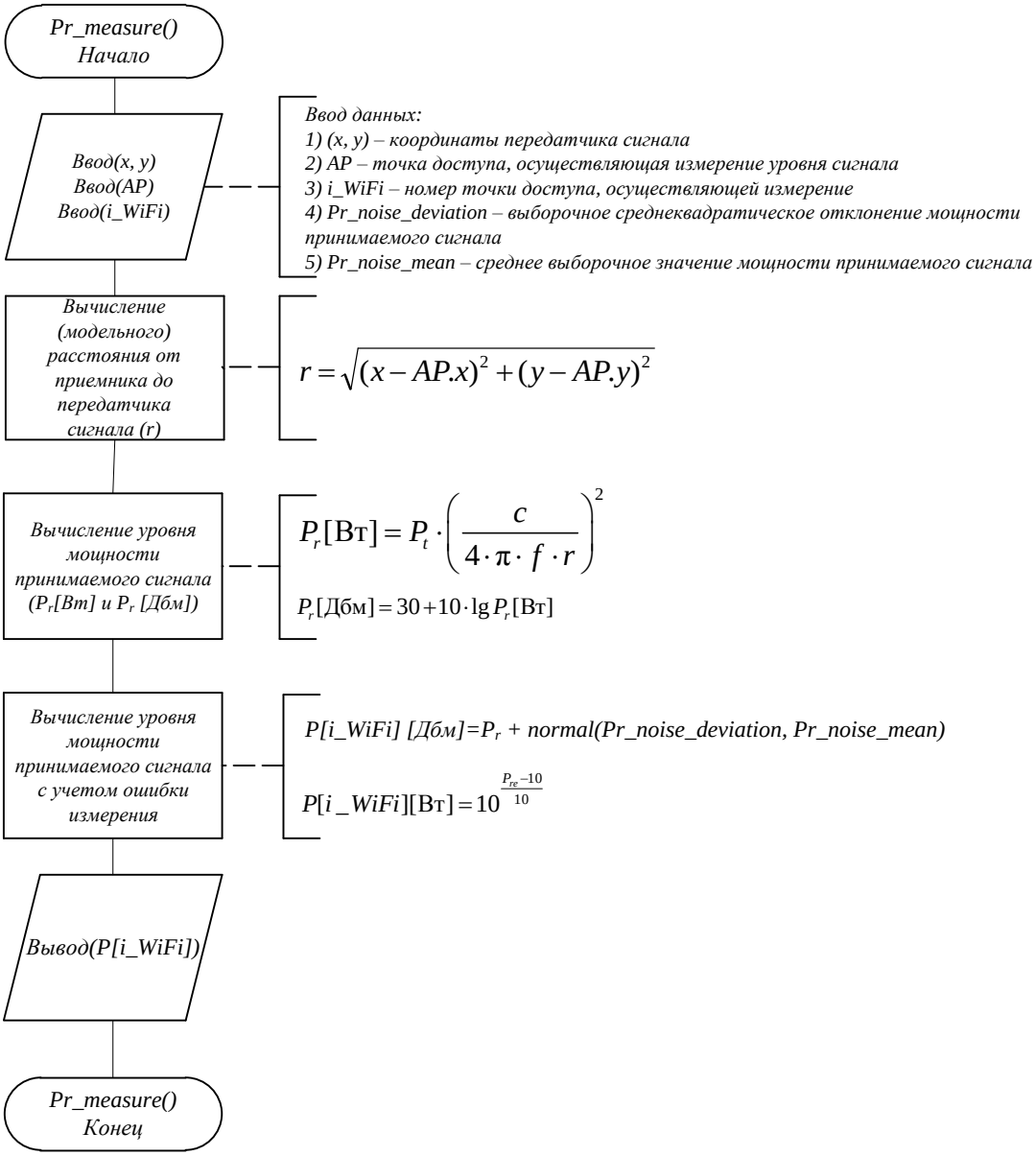


Рисунок В.3 – Блок-схема моделирующего алгоритма измерения уровня сигнала

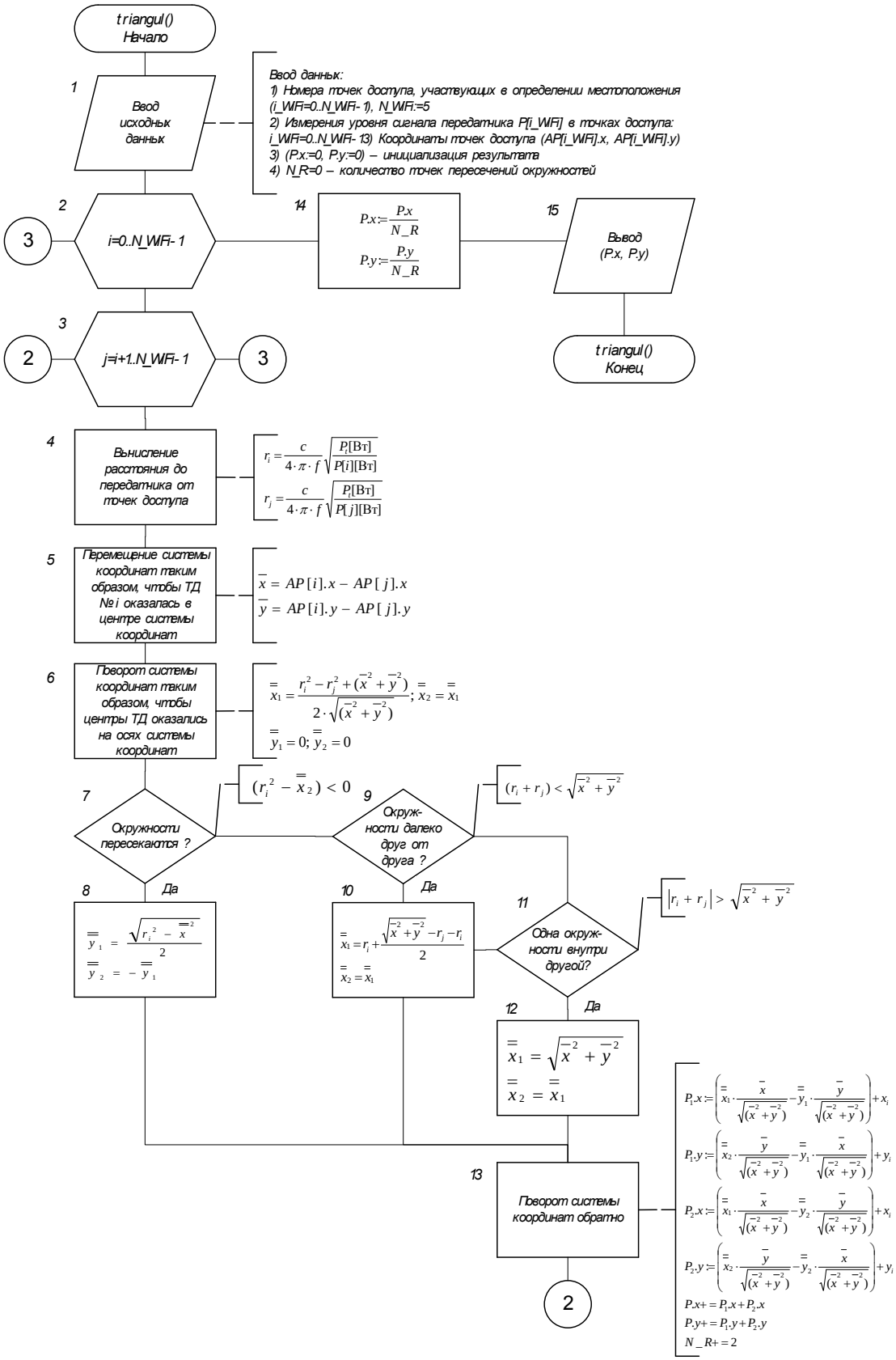


Рисунок В.4 – Блок-схема моделирующего алгоритма процедуры определения местоположения методом трилатерации

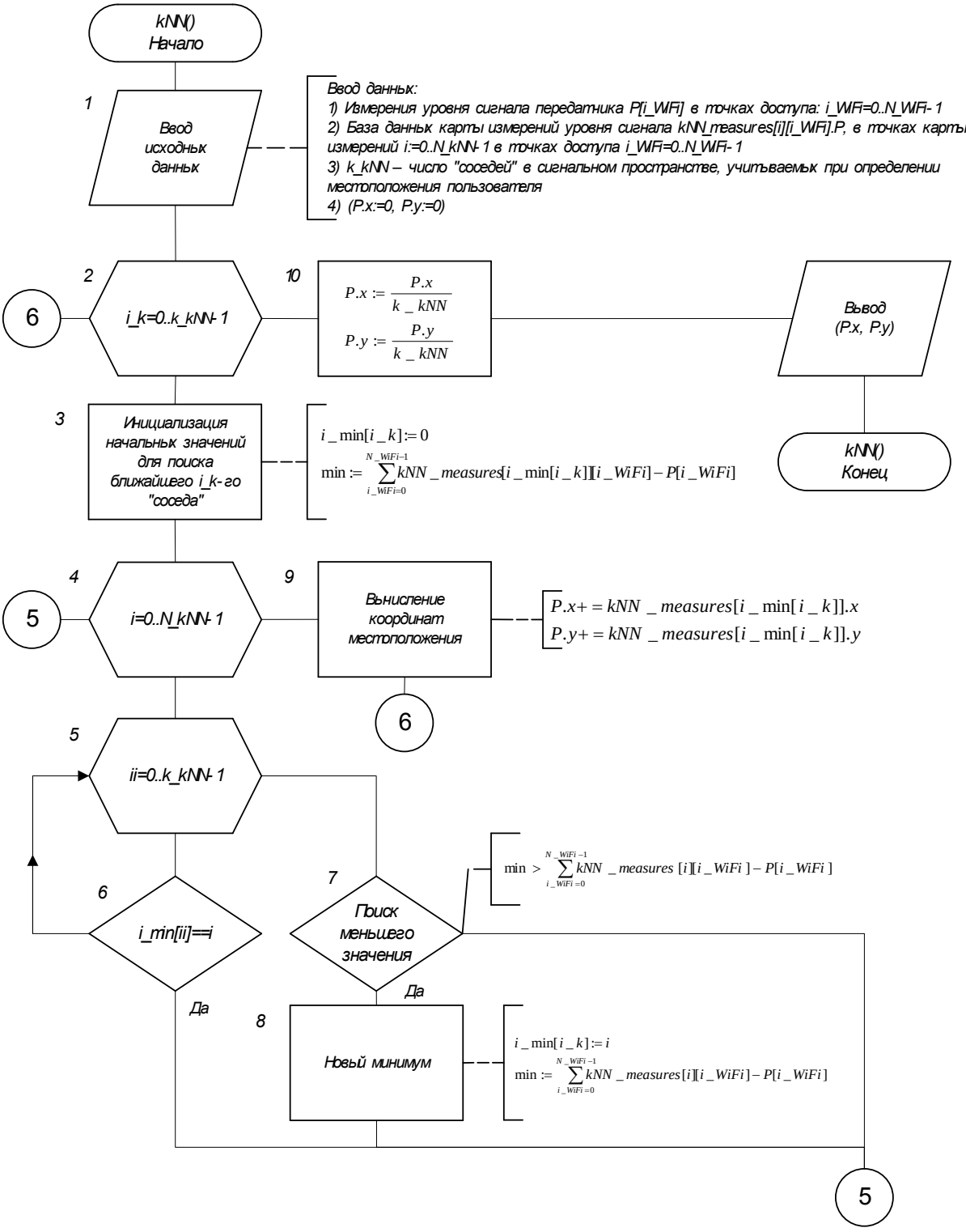


Рисунок В.5 – Блок-схема моделирующего алгоритма процедуры определения местоположения методом k-ближайших соседей

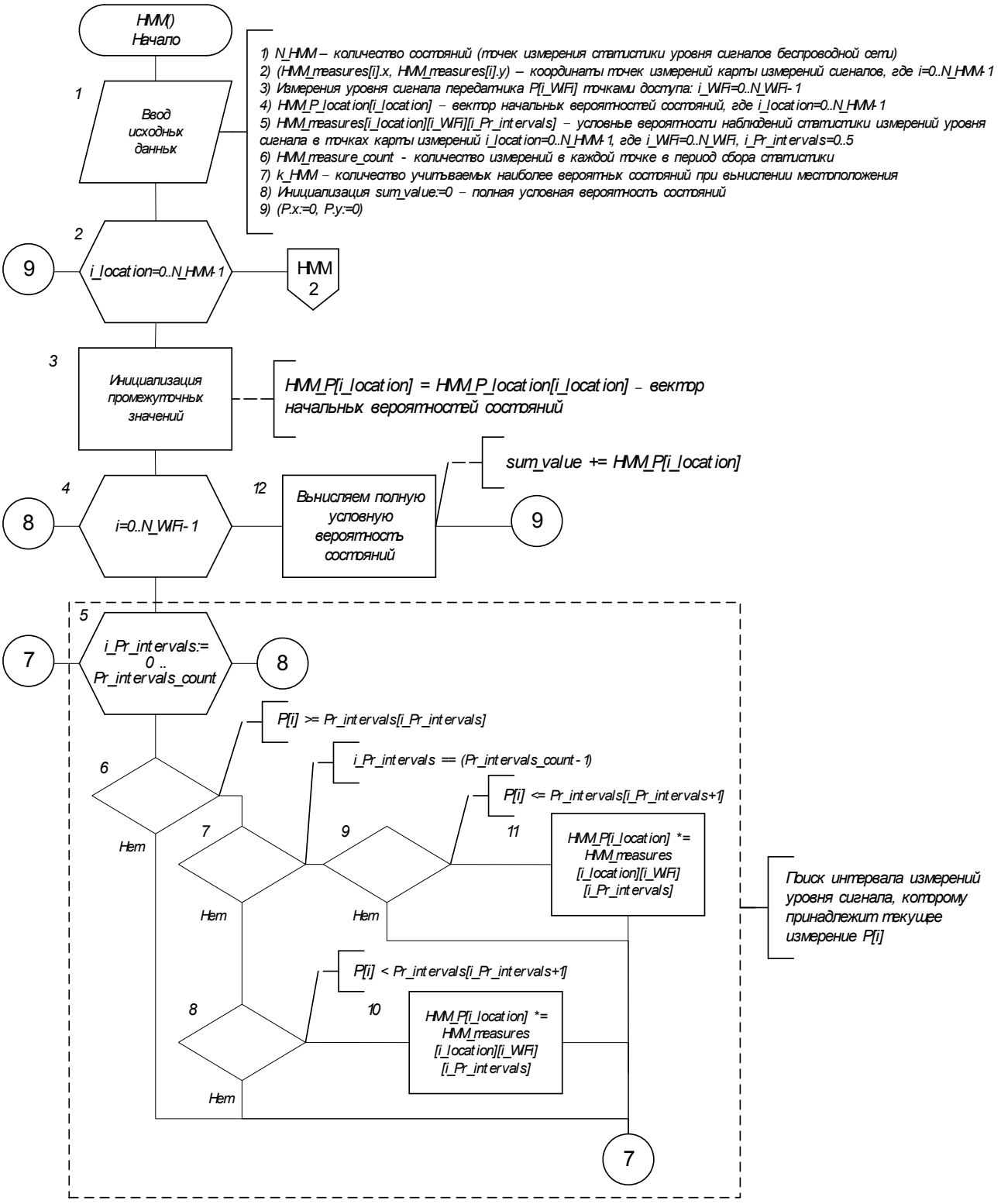


Рисунок В.6 – Блок-схема моделирующего алгоритма процедуры определения местоположения методом на основе скрытых марковских моделей (начало)

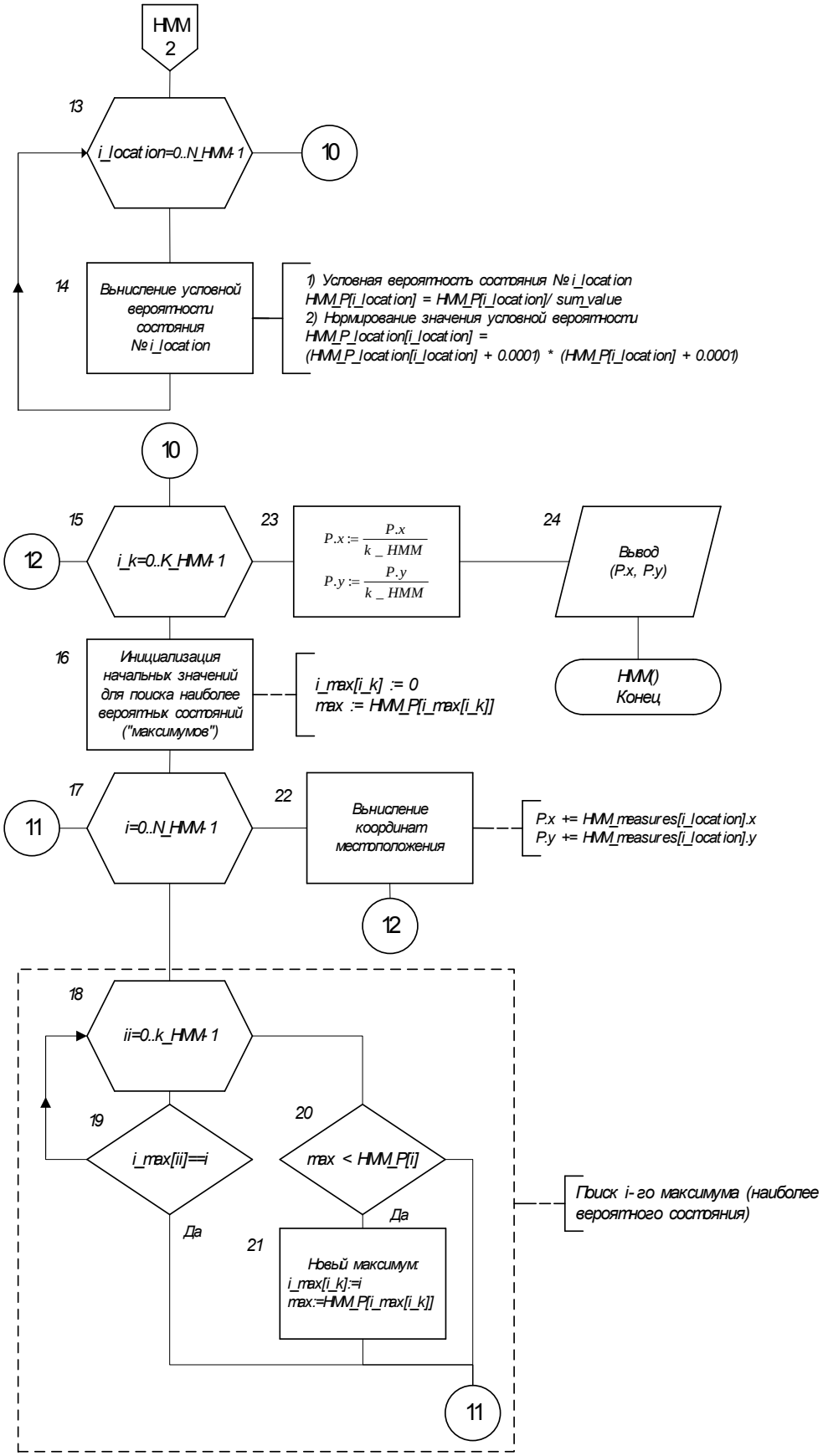


Рисунок В.7 – Блок-схема моделирующего алгоритма процедуры определения местоположения методом на основе скрытых марковских моделей (окончание)

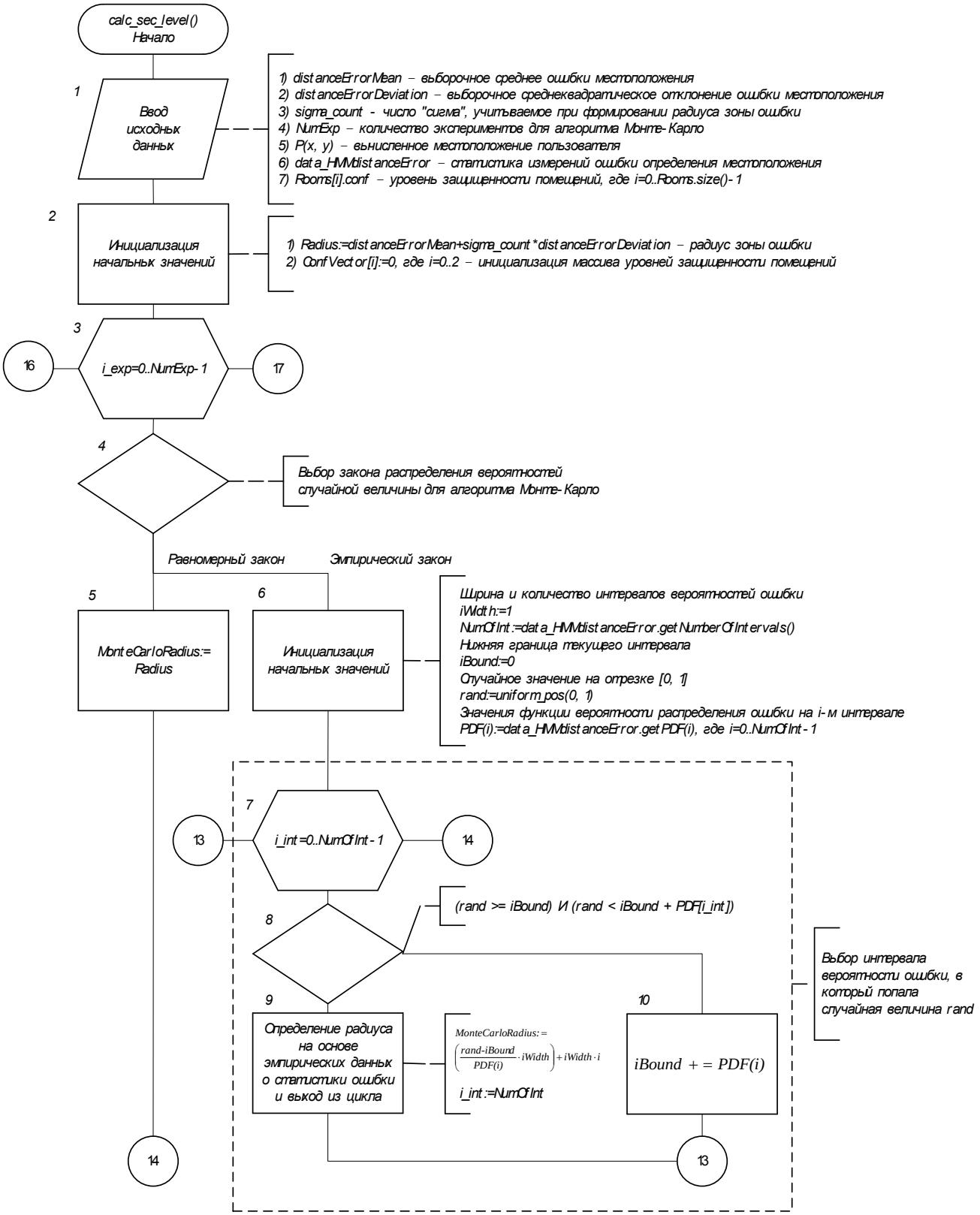


Рисунок В.8 – Блок-схема моделирующего алгоритма процедуры определения вероятности нахождения МАУ в специальном помещении и принятия решения об требования по уровню его защищенности (начало)

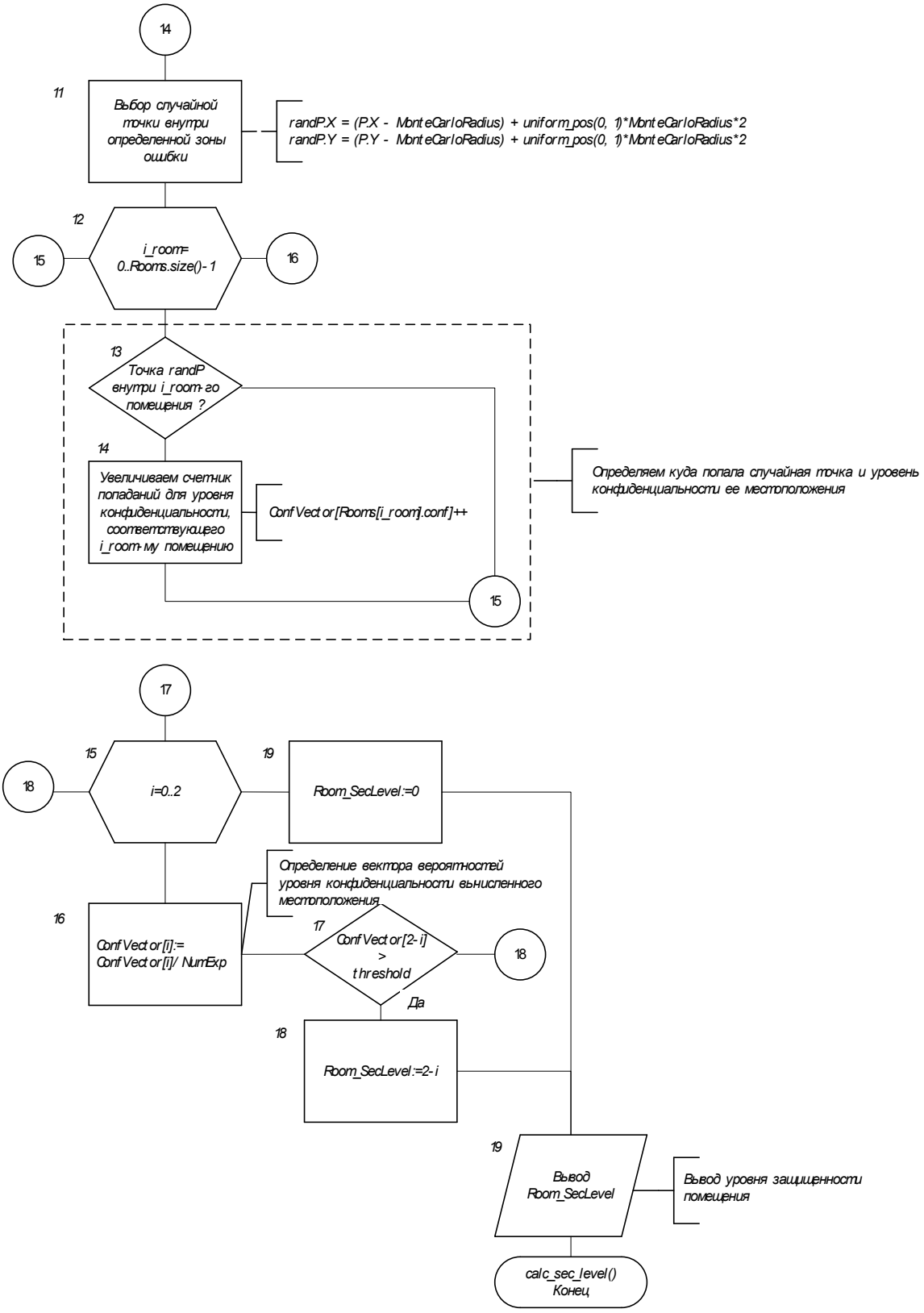


Рисунок В.9 – Блок-схема моделирующего алгоритма процедуры определения вероятности нахождения МАУ в специальном помещении и принятия решения об требования по уровню его защищенности (окончание)

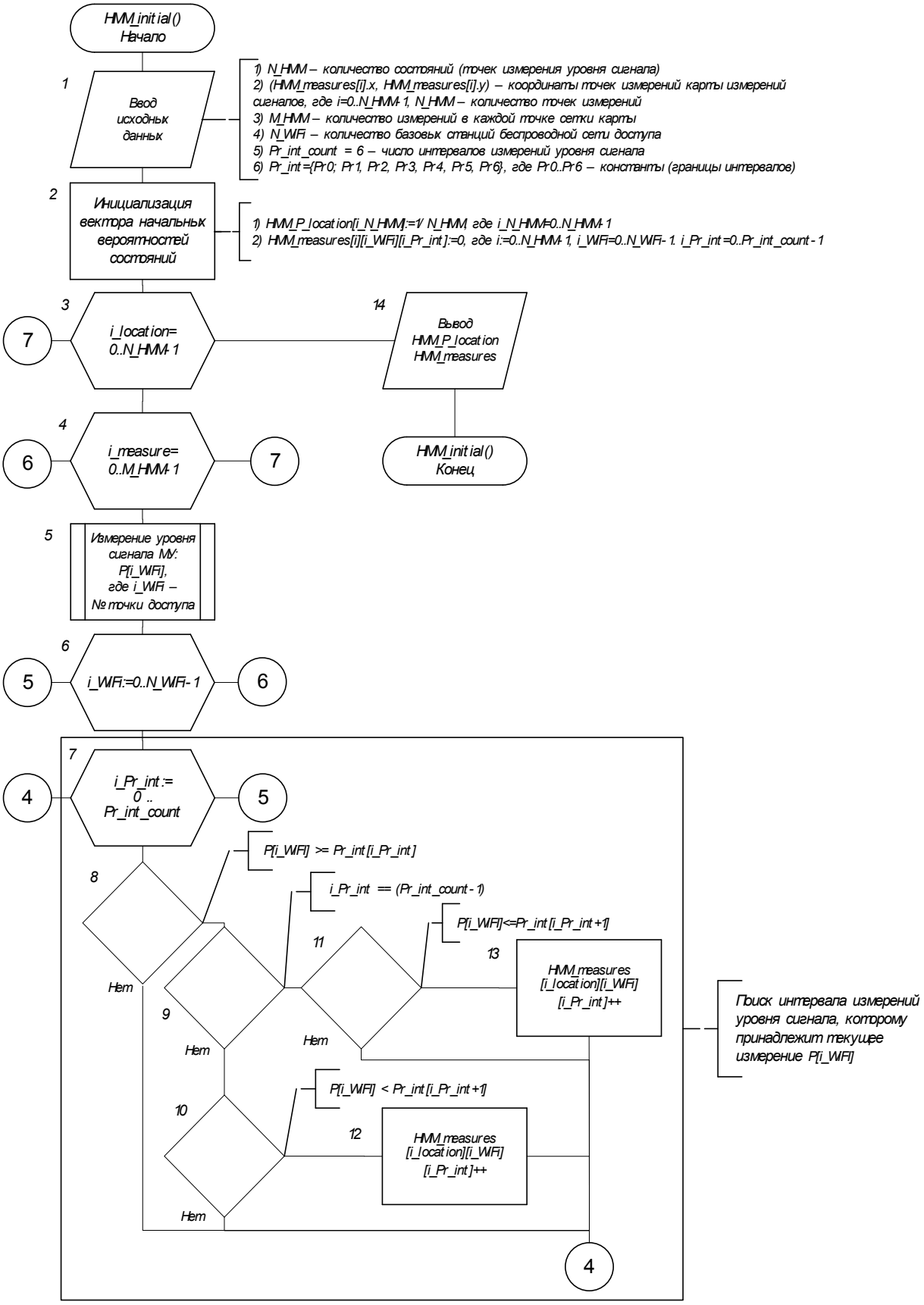


Рисунок В.10 – Блок-схема алгоритма обучения байесовского классификатора

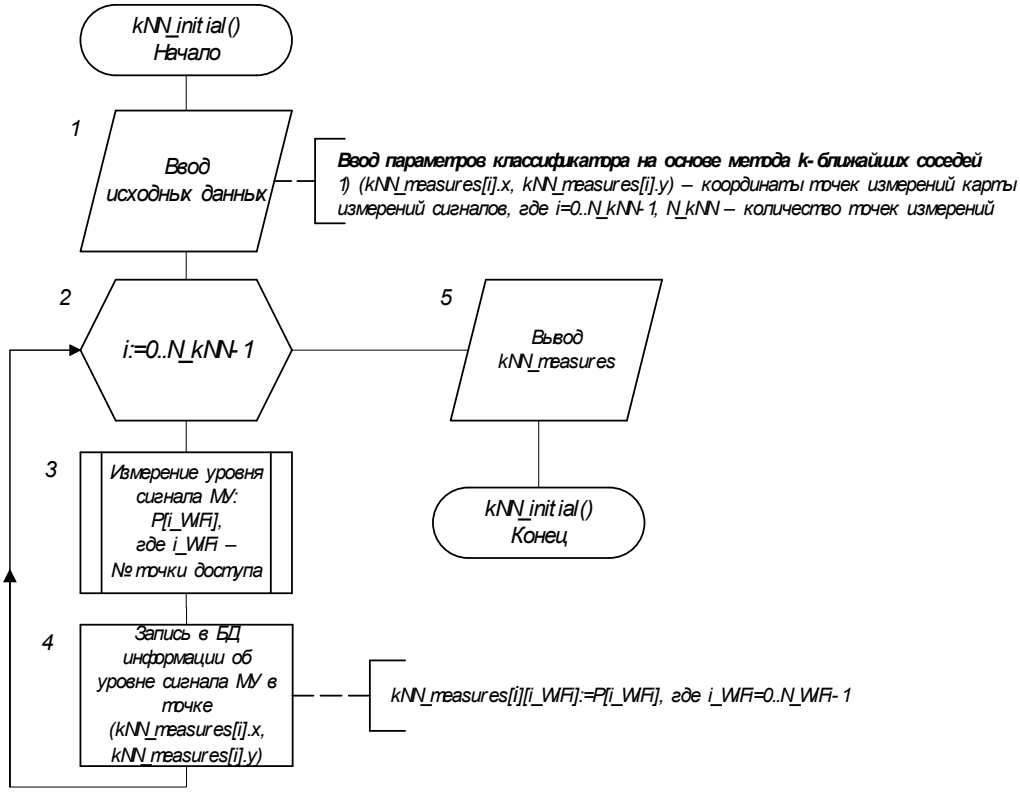


Рисунок В.11 – Блок-схема процедуры обучения классификатора, основанного на использовании метода k-ближайших соседей

СПРАВКА

Материалы изложены в [39, 40, 42, 43, 77, 79] и необходимы для формального описания частных процедур и общего алгоритма управления конфигурацией МАУ, учитывающего атрибуты доступа пользователей МАУ, а также моделирующего алгоритма, реализующего работу системы управления безопасностью МАУ в корпоративных сетях с разными требованиями по защищенности.

Д. О. Маркин