Федеральное государственное автономное образовательное учреждение
высшего образования
«Санкт-Петербургский государственный университет аэрокосмического
приборостроения»

На правах рукописи

Чжао Лэй

МЕТОД И АЛГОРИТМЫ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ОТКРЫТОЙ СЕТИ СВЯЗИ С НАЗЕМНЫМИ ПОДВИЖНЫМИ ОБЪЕКТАМИ

2.2.15. Системы, сети и устройства телекоммуникаций

Диссертация на соискание ученой степени
кандидата технических наук

Научный руководитель
к.т.н., доцент
Карманов Андрей Геннадьевич

Санкт-Петербург 2021

Содержание

Введение

В современном мире электронные средства играют все большую роль в жизни человека. Сложные информационные системы (ИС) занимают одно из ключевых мест не только в промышленности, но и в нашей повседневной жизни. Для устойчивого функционирования ИС при влиянии негативных воздействий разработчикам необходимо решать ряд задач, таких как: выявление узких мест каналов, узлов при перегрузке, обеспечение безопасного обмена между источниками и приемниками информации и т.д.

Ведущие производители оборудования активно ведут исследования и разработки в области мобильных систем связи с целью повышения пропускной способности и скорости передачи цифровых данных.

Не смотря на то, что в беспроводных сетях встраиваются специальные протоколы безопасности, которые включают в себя шифрование и аутентификацию пользователя, большое внимание уделяется защите передаваемой информации.

Роль беспроводных технологий в повседневной деятельности человека растет с каждым годом. Беспроводной доступ к сети интернет на сегодняшний момент времени поддерживают практически все мобильные устройства. Беспроводные сети организованы в аэропортах, отелях, кафе и многих публичных местах. Их рост обусловлен удобством развертывания и эксплуатации, приемлемой скоростью передачи данных и относительной дешевизной. Беспроводной трафик растет и постепенно приближается к объему данных, передаваемых по наземным линиям связи.

Актуальность темы работы обусловлена потребностью для целого ряда устройств систем связи с мобильными подвижными объектами в повышении их защищенности на этапе разработки. Этому способствуют следующие факторы:

− сравнительно невысокая стоимость и массогабаритные параметры средств связи, что способствует бурному развитию и повсеместному развертыванию мобильных систем;

− на этапе разработки потребность в определении показателей защищенности, которые определяют запас живучести компонентов систем связи, рассматриваемый в работе как фактор противостояния атакам злоумышленников;

− тенденция в использовании аппарата искусственных нейронных сетей, требующая развития методов эффективного машинного обучения в условиях ограничений временных и вычислительных ресурсов;

− широкие возможности устройств связи по совмещению телекоммуникационных, измерительных и управляющих функций усложняют алгоритмы защиты данных от несанкционированного доступа, что затрудняет прогнозирование устойчивости разработанных на базе них систем;

− многопараметрическая неопределенность, возникающая на ранних этапах проектирования сетей и систем связи, увеличивается при переходе к беспроводным их видам и приводит к росту уязвимостей всех составляющих компонентов, а внесение изменений в уже готовые версии продуктов приводит к значительным затратам.

Анализируя **степень разработанности темы** настоящей работы, можно отметить следующее.

Методам построения безопасных систем связи, оценке их устойчивости, посвящен ряд работ как в России: А.Г. Додонов, В.Ф. Крапивин, М.Г. Кузнецова, В.М. Вишневский, Ю.М. Парфенов, Д.Л. Белоцерковский, Ю.Е. Мельников, Ж.С. Сарыпбеков, Ю.Е. Малашенко, И.А. Рябинин, Б.С. Флейшман, Ю.Ю. Громов, Д.В. Ландэ, И.Ю. Стекольников и др., так и за рубежом C.J. Colbourn, Y. Li, K. Sekine, H. Imai, M.X. Cheng, D.-Z. Du, A.E. Smith, S. Tani и др. В своих работах авторы в основном используют вероятностный подход, который имеет ряд недостатков, один из которых заключается в сложности получения априорных значений вероятностей нанесения ущерба компонентам систем связи.

Для решения многих задач с использованием аппарата искусственных нейронных сетей авторами предлагаются процедуры, которые носят не строгий, но рекомендательный характер, а предлагаемые готовые решения являются избыточными. Это повышает стоимость реализации и время обучения нейронных

сетей. Поэтому необходима разработка модифицированных методов и алгоритмов для повышения безопасности сети связи с наземными подвижными объектами.

Разработанный в настоящее время математический аппарат для расчета и прогнозирования показателей защищенности мобильных систем связи требует уточнений, для чего необходимо их развертывание в местах дислокации. Низкая точность, получаемая при расчетах, обусловлена сложностью математических моделей и использованием оценок экспертов. Это не позволяет получить готовое решение для задачи определения показателей защищенности и устойчивости систем связи, и образует новую область для исследований.

Таким образом, поставленная в работе задача является актуальной.

Область исследования. Содержание диссертационной работы соответствует паспорту специальности 2.2.15. (05.12.13) Системы, сети и устройства телекоммуникаций: п.2. Исследование процессов генерации, представления, передачи, хранения и отображения аналоговой, цифровой, видео-, аудио- и мультимедиа информации; разработка рекомендаций по совершенствованию и созданию новых соответствующих алгоритмов и процедур; п.10. Исследование и разработка новых методов защиты информации и обеспечение информационной безопасности в сетях, системах и устройствах телекоммуникаций; п.12. Разработка методов эффективного использования сетей, систем и устройств телекоммуникаций в различных отраслях народного хозяйства; п.13. Разработка методов совмещения телекоммуникационных, измерительных и управляющих систем; п.14. Разработка методов исследования, моделирования и проектирования сетей, систем и устройств телекоммуникаций.

Объекты исследования: механизм защиты данных в беспроводных сетях, сложные информационные системы, беспроводные протоколы передачи данных между подвижными объектами, а также методики расчета параметров устойчивости систем и средств связи.

Предметом исследования являются методы, модели и алгоритмы защиты информации в системах связи с подвижными наземными объектами и рекомендации по их совершенствованию.

Цель и задачи исследования.

Цель работы – определение показателей защищенности беспроводных систем связи с подвижными наземными объектами для повышения их безопасности на этапе проектирования.

Для достижения поставленной цели были решены следующие задачи:

− анализ известных открытых протоколов организации беспроводной связи для наземных подвижных объектов;

− исследование современных принципов защиты систем радиосвязи;

− анализ методов исследования уровня защищенности систем радиосвязи;

− разработка метода определения показателей защищенности открытых систем связи с подвижными объектами;

− разработка алгоритмов для настройки искусственных нейронных сетей для решения задач определения показателей защищенности и устойчивости систем связи;

− проверка эффективности разработанных метода и алгоритмов с помощью имитационных экспериментов на ЭВМ.

Методология и методы исследований базируются на использовании аппарата теорий множеств, графов, искусственных нейронных сетей, вероятности и математической статистики.

Научная новизна состоит в:

− разработке метода определения показателей защищенности конкретных вариантов построения беспроводных сетей связи с наземными подвижными объектами с использованием статистических и смоделированных данных, отличающийся возможностью получения количественных показателей защищенности без использования экспертных оценок и расчетных методик;

− разработке алгоритма настройки искусственной нейронной сети для решения задачи определения показателей защищенности систем связи на основе принципа последовательного приближения, решающего задачу неопределенности по настройке искусственной нейронной сети под конкретную задачу;

− разработке алгоритма прогнозирования устойчивости беспроводной сети при изменении ее параметров, отличающийся от известных подходов возможностью прогнозирования условий отказа сети при изменении ее параметров.

Положения, выносимые на защиту:

− метод определения показателей защищенности к преднамеренным деструктивным воздействиям на беспроводную открытую систему связи с наземными подвижными объектами на базе стандартных протоколов;

− модифицированный алгоритм многоэтапного обучения искусственной нейронной сети, анализирующей защищённость беспроводной системы связи, отличающийся от известных тем, что подбор параметров (нейросети) и метода оптимизации производится последовательным приближением, аналогично методу покоординатного поиска;

− алгоритм определения вероятности отказа в обслуживании беспроводной сети линейного типа при росте числа наземных мобильных абонентов.

Теоретическая и практическая значимость результатов, полученных в диссертационной работе, заключается в следующем.

Теоретическая значимость заключается в определении условий повышения уровня защищенности беспроводной системы связи с мобильными наземными станциями и разработанных алгоритмов определения показателей защищенности систем связи на базе открытых протоколов.

Практическая значимость результатов исследований заключается в том, что разработанные алгоритмы и метод являются основой для проектирования новых защищенных систем связи с подвижными объектами, а также мониторинга состояния и понижения устойчивости линий связи.

Степень достоверности результатов. Степень достоверности основных полученных результатов обеспечивается корректностью поставленных научно-технических задач, представленной совокупностью допущений и ограничений, корректным применением математического аппарата, непротиворечивостью

полученных результатов, согласующихся с практическими и статистическими данными, апробацией основных положений работы на научных конференциях и семинарах, а также в публикациях автора и имеющихся актах внедрения.

Внедрение результатов. Результаты работы использованы в учебном процессе кафедры Геоинформационных систем Университета ИТМО, г. Санкт-Петербург (2017) и внедрены в Ситуационном центре ЗАО "Институт телекоммуникаций" г. Санкт-Петербург (2021). Практическое использование результатов работы подтверждено соответствующими документами.

Апробация результатов работы. Основные положения диссертационных исследований докладывались и обсуждались на научно-технических конференциях и семинарах. Среди них:

− XLIV и XLV учебно-методические конференции Университета ИТМО (Санкт-Петербург, февраль 2015, 2016 гг.);

− III и IV Всероссийские конгрессы молодых ученых (Санкт-Петербург, апрель 2015, 2016 гг.);

− Международная научно-практическая конференция (Самара, апрель 2015 г.).

Публикации. Теоретические и практические результаты, представленные в диссертации, отражены в 11-ти печатных работах, из них 5 работ в изданиях, входящих в перечень ведущих рецензируемых научных журналов и изданий, выпускаемых в Российской Федерации, рекомендованных ВАК.

Личный вклад автора. Все проведенные исследования, а также результаты работы: метод прогнозирования показателей устойчивости, алгоритмы настройки искусственных нейронных сетей, определения вероятности отказа в обслуживании системы связи линейного типа с ростом числа абонентов, – личные достижения автора под руководством научного руководителя.

Структура и объем диссертационный работы. Диссертационная работа содержит 145 страниц основного текста, состоит из введения, четырех глав, заключения, списка использованных источников из 103 наименований, содержит 27 рисунков и 17 таблиц.

ГЛАВА 1
АНАЛИЗ СУЩЕСТВУЮЩИХ МЕТОДОВ ПОСТРОЕНИЯ СИСТЕМ СВЯЗИ С НАЗЕМНЫМИ ПОДВИЖНЫМИ ОБЪЕКТАМИ

1.1. Обзор и анализ систем подвижной связи

1.1.1. Классификация систем связи

При организации связи между наземными подвижными объектами в качестве носителя информационного сигнала используются радиоволны, распространяющиеся в пространстве. Радиосвязь может быть односторонняя – обеспечивать передачу информации в прямом, и двусторонняя – в прямом и обратном направлениях. Также радиосвязь можно разделить на симплексную (поочередный прием и передача информации) для которой требуется одна рабочая частота и дуплексную (двусторонний обмен информацией), когда требуется две несущие частоты [1].

Грубо частотную сетку, использующуюся для радиосвязи, можно разделить на следующие поддиапазоны: длинные волны (f =150…450 кГц, λ = 2000…670 м), средние волны (f =500…1600 кГц, λ = 600…190 м), короткие волны (f =3…30 МГц, λ = 100…10 м), ультракороткие волны (f =30…30000 МГц, λ = 10…0,01 м), или ДВ, СВ, КВ и УКВ сокращенно. Подробно классификация диапазонов радиочастот приведена в таблице 1.1.

Таблица 1.1. Классификация диапазонов радиочастот

Наименование	Диапазон частот	Диапазон длин волн ($\Delta\lambda$)	Использование	Сокращение
Крайне низкие частоты	3…30 Гц	100 000…10 000 км	–	КНЧ

Сверхниз-кие частоты	30…300 Гц	10000… 1000 км	–	СНЧ
Инфраниз-кие частоты	300…3000 Гц	1000… 100 км	–	ИНЧ
Очень низкие частоты	3…30 кГц	100…10 км	Глобальные системы навигации, системы связи с низкой скоростью передачи информации, системы дальней навигации.	ОНЧ
Низкие частоты	30…300 кГц	10…1 км	Системы дальней навигации.	НЧ
Средние частоты	300…3000 кГц	1000…100 м	Радиовещание, системы навигации средней дальности.	СЧ
Высокие частоты	3…30 МГц	100…10 м	Связь на дальние расстояния с низкой скоростью передачи данных. Радиовещание.	ВЧ
Очень высокие частоты	30…300 МГц	10…1 м	Связь на небольшие расстояния и ближняя навигация	ОВЧ
Ультра-высокие частоты	300…3000 МГц	100…10 см	Вещание, радиорелейная и спутниковая связи, радиолокация, спутниковая навигация	УВЧ
Сверхвысо-кие частоты	3…30 ГГц	10…1 см	Радиорелейная и спутниковая связи, радиолокация.	СВЧ

Крайне-высокие частоты	30…300 ГГц	10…1 мм	–	КВЧ
Гипервысо-кие частоты	300…3000 ГГц	1…0,1 мм	–	ГВЧ

Радиосвязь также можно разделить на связь без ретрансляторов, спутниковую, радиорелейную и сотовую.

Спутниковую связь можно рассматривать как связь через удаленные ретрансляторы, находящиеся на большой высоте. Системы спутниковой связи основаны на использовании искусственных спутников земли, находящихся на высокой эллиптической, геостационарной или низковысотной орбите. Такая связь осуществляется между наземными подвижными и стационарными станциями. Подвижные станции для спутниковой связи устанавливаются на самолетах, морских судах, автомобилях, а стационарные используются как элементы радиовещательных служб и поставщиков интернет контента.

Наземная радиорелейная связь использует деци- и сантиметровые волны, а антенны станций располагаются в зоне прямой видимости и при высоте мачт 70..100 м дальность связи составляет 40…50 км.

Сотовая связь является основой для построения сотовых сетей. Особенностью таких сетей является то, что зоны покрытия базовых станций делятся на ячейки или соты, представляющие в идеальных условиях правильные шестиугольники. В стандартах GSM (Global System for Mobil Communication) и CDMA (Code Division Multiple Access) каждая мобильная станция имеет свои международные идентификационные коды (INSI и IMEI), зашитые в память. Смежные БС, работающие на разных частотах, образуют кластер, состоящий из m станций. БС размещаются таким образом, чтобы можно было использовать тот же набор частот несколько раз. Если каждой БС выделено n каналов с шириной полосы F_n у каждого, то общая ширина занимаемой полосы частот системой связи будет:

$F_c = nF_n$.

Параметр m увеличивается с уменьшением радиуса ячейки $R_{яч}$, поэтому, уменьшая $R_{яч}$ можно увеличить повторяемость частот.

Оборудование для построения систем связи можно разделить на любительское и профессиональное. Профессиональные средства связи предназначены для выполнения определенных задач в жестких условиях эксплуатации, поддерживают специализированные функции (например, поддержку организации связи внутри групп и подгрупп) и подлежат регистрации в органах надзора за связью.

Основными параметрами, определяющими разделение на различные классы профессиональных средств связи, являются:

- плотность абонентов в обслуживаемой зоне;
- площадь покрытия, которая определяет масштаб системы;
- уровень сервиса;
- автоматический или ручной выбор канала;
- возможности и глубина группообразования;
- наличие индивидуальных и аварийных вызовов;
- идентификация абонентов;
- выход в телефонную сеть, полный дуплекс на уровне абонентского терминала;
- передача коротких сообщений;
- передача данных и др.

Исходя из перечисленных параметров, а также, исходя из области применения, системы связи можно классифицировать следующим образом.

1. Конвенциональные системы связи используются при невысокой плотности абонентов (идентификаторов), а радиоканалы выбираются пользователем.

2. Локальные системы малого радиуса действия. Разрабатываются для использования на небольшой территории (радиус действия не превышает 7 км).

Нашли применения в службах охраны железнодорожного и речного транспорта и др. отраслях.

3. Диспетчерские системы с симплексной связью. Одна из абонентских станций используется как стационарная диспетчерская, а ее антенна размещается на значительной высоте. Радиус действия повышается до носимой станции – до 10 км, до возимой – до 50 км. Такие системы используются в МВД, так как мобильные станции позволяют осуществлять связь внутри группы на небольших расстояниях (до 2 км), а связь с диспетчерской станцией для управления работой подразделений – на значительных.

4. Ретрансляционные диспетчерские системы. Связь абонентов между собой может осуществляться как через центральную, так и через ретрансляционную станцию, в качестве которой может быть абонентская станция. Такая система связи обладает значительной гибкостью и используется службами МВД, МПС, РАО ЕЭС, нефтегазовым комплексом и т.д.

5. Сложные многозоновые диспетчерские системы являются результатом объединения нескольких зон в единую систему и используются для организации связи с низкой плотностью абонентов, но на больших расстояниях, например, вдоль трубопроводов. В таких системах для объединения подсистем служат специальные диспетчерские пульты или коммутаторы.

6. Транкинговые системы делают возможным объединение абонентов внутри групп или подгрупп, ограничивая число доступных каналов, и позволяют работать при высокой плотности абонентов с сохранением централизованного управления системой. Широко используются в профессиональной деятельности различных направлений.

7. Аналоговые транкинговые системы служат для речевой связи и отправки коротких сообщений. Открытым европейским стандартом является MPT 1327, на котором построено множество систем как с распределенным, так и с централизованным управлением. В России также распространено оборудование, работающее на частотах 150, 300 и 400 МГц. До сих пор спрос на такие системы обуславливает большой срок жизни данной технологии.

8. Цифровые интегрированные системы связи предназначены для обеспечения речевой связи, передачи данных и телефонии. Основным сегментом таких систем служат общекорпоративные сети для передачи голоса и данных при управлении производственными процессами. Реализацией могут служить системы на базе открытого стандарта TETRA. Интегрированные системы могут объединять подсистемы с низкоскоростной передачей данных.

9. Абонентские радиостанции используют технологии приведенных решений, а подавляющее большинство моделей предназначено для голосовой связи и передачи данных с небольшой скоростью (в основном для сообщений).

Основными преимуществами цифровых систем связи перед аналоговыми являются: отсутствие фоновых помех, большие скорости передачи данных, поддержка пакетных режимов, сокращение времени установки связи.

1.1.2. Классификация беспроводных сетей

Системы и сети подвижной связи можно классифицировать, используя рекомендации Международного союза электросвязи, на: сухопутные, морские, авиационные, спутниковые и общего пользования. Сухопутные включают: беспроводные, сотовые и транкинговые системы радиосвязи. Наземные сети подвижной связи являются основой построения систем подвижной связи общего пользования. Абонентами используются преимущественно каналы связи наземной сети, которые делятся на федеральные и региональные: на основе стандартов NMT-450 (аналоговый) и GSM-900 (цифровой). Спутниковая сеть задействуется при выходе абонента из зоны обслуживания наземной сети. Поэтому спутниковые сети подвижной связи в первую очередь предназначены для междугородной и международной связи абонентов, но они же могут использоваться и для внутризоновой, и для местной. Основными сдерживающими факторами развития спутниковых систем связи является сложность передающей аппаратуры и высокая стоимость связи. Поэтому в настоящее время спутниковая

связь используется для радиовещания, передачи данных сети интернет, радиолокации и систем связи специального назначения.

Беспроводные сети можно классифицировать по дальности действия сети [2–10]:

− персональные беспроводные сети (WPAN – Wireless Personal Area Networks), имеющие радиус действия до нескольких десятков метров. Используются для развертывания связи между устройствами, а также с сетями более высокого уровня;

− региональный уровень сетей (WMAN – Wireless Metropolitan Area Networks), характеризуются дальностью до нескольких километров;

− сети сотовой связи (WWAN – Wireless Wide Area Networks) с зоной покрытия в десятки километров.

Из 10

Протоколы для цифровых систем мобильной радиосвязи можно разделить на два больших класса: закрытые (корпоративные) и открытые [10].

Рассмотрим основные беспроводные стандарты связи, используемые в настоящее время для передачи данных [2–9].

BlueTooth. Стандарт BlueTooth (IEE 802.15.1) разрабатывался на малую мощность, а радиоканал обеспечивает скорость 721 кбит/с, поэтому объем передаваемых данных незначителен, а зона покрытия ($R_{яч}$) составляет 10…15 м. Модернизированный стандарт связи IEE 802.15.3 предусматривает скорость до 55 Мбит/с с зоной покрытия до 100 м с одновременной работой до 245 пользователей. Используемая полоса частот 2,4…2,4835 ГГц не требует лицензии на вещание.

Wireless USB – беспроводная замена проводного соединения по шине USB. Стандарт предназначен для высокоскоростного обмена данными персонального компьютера с периферийными устройствами: принтерами, сканерами, фото- и видеокамерами, внешними накопителями. Скорость до 180 Мбит/с обеспечивается на расстоянии до 10 м.

Wireless HD. Стандарт разрабатывался для передачи видео высокого разрешения (HD) и может использоваться для развертывания беспроводной сети, обладающей следующими характеристиками. Пропускная способность – до 28 Гбит/с на расстояние до 10 м. Широкополосный сигнал ($\Delta f = 7$ ГГц) на центральной частоте 60 ГГц не может обходить объекты, находящиеся на пути от источника к приемнику. Необходимо также, чтобы приемник и передатчик находились в зоне прямой видимости.

WiGig – стандарт IEEE 802.11 a,d также работает на не лицензируемых частотах около 60 ГГц и обеспечивает скорость до 7 Гбит/с на расстояние до 10 м. Недостатки те же.

WHDi (Wireless Home Digital Interface) – технология для высоко-скоростной передачи данных, оптимизированная для передачи HD-видео. Технология WHDi позволяет установить беспроводное соединение компьютера с монитором. Используемая частота в 5 ГГц позволяет обеспечивать скорость 3 Гбит/с.

DASH7 – стандарт, предназначенный для организации беспроводных сенсорных сетей. Сенсорные сети объединяют миниатюрные электронные устройства, состоящие из сенсора (датчика температуры, давления, движения, освещенности и т.п.), приемо-передатчика и миниатюрного источника питания. В технологии DASH7 используется не лицензируемая частота 433 МГц, обеспечивая скорость передачи данных до 200 кбит/с на расстояние до 2 км. Стандарт DASH7 – серьезный конкурент патентованным технологиям организации беспроводных сетей, таких как ZigBee или Z-Wave.

WirelessHART – протокол беспроводной связи, – разработка HART Communication Foundation для обмена данными с полевыми датчиками с использованием расширяемого набора команд "запрос-ответ", передаваемых в цифровом виде. Технология WirelessHART обеспечивает передачу данных на частоте 2,4 ГГц на расстояние до 200 м со скоростью до 250 кбит/с между устройствами, находящимися в пределах прямой видимости.

MiWi – спецификация IEEE 802.15.4 протокола для организации беспроводных персональных и сенсорных сетей, работающих с низкой скоростью

передачи данных. Сеть MiWi может объединять до 1024 узлов, управляемых до 8 контроллерами (каждый контроллер рассчитан на управление до 127 узлами). Передача данных может вестись на частоте 2,4 ГГц, а также на частотах 868 и 915 МГц со скоростью до 250 кбит/с.

RuBee – стандарт, разработанный для организации беспроводных сенсорных сетей, в которых передача данных ведется с помощью магнитных волн на частоте 131 КГц, обеспечивая скорость до 1200 Бод на расстояния до 30 м. Достоинством стандарта является низкое энергопотребление, что позволяет автономно работать таким сетям в течение нескольких лет от одного источника питания. Специфика работы сетей, построенных на стандарте RuBee, оправдывает их использование в тех случаях, когда требуются долгая работа без обслуживания и высокая надежность связи при низкой скорости передачи данных.

HiperLAN (High Performance Radio LAN) – стандарт беспроводной связи, для двух ревизий. HiperLAN–1 запущена в 1981 году. Обеспечивает скорость передачи данных до 10 Мбит/с на расстоянии 50 м и позволяет работать с мобильными объектами, двигающимися со скоростью до 1,4 м/с. Вторая ревизия HiperLAN–2 работает на частотах, близких к 5 ГГц, обеспечивая скорость до 54 Мбит/с уже на расстоянии 150 м и двигающихся со скоростями до 10 м/с.

Wi-Fi – семейство стандартов, основанных на спецификации IEEE 802.11, работающей на частотах 2,4 или 5 ГГц со скоростями передачи данных от 2 до 300 Мбит/с на расстояние до 200 м. Это наиболее распространенный на сегодня стандарт для организации беспроводных сетей и подключения к сети интернет в домах, офисах и на предприятиях. Wi-Fi-совместимое оборудование в настоящее время может поддерживать модификации стандартов IEEE 802.11: a, b, g, n и i (см. табл. 1.2). Базовый стандарт IEEE 802.11 предназначен для беспроводных сетей, работающих на очень низких скоростях (до 2 Мбит/с). Протокол IEEE 802.11a ратифицирован в 1999 году; передача данных возможна со скоростью до 54 Мбит/с. Он не совместим с протоколом IEEE 802.11b, который совместим с IEEE 802.11g. Ревизия g ратифицирована в 2003 году. На сегодня самым передовым стандартом является IEEE 802.11n, обеспечивая наивысшие скорости

передачи данных по сравнению с предшественниками. Новый стандарт IEEE 802.11ac будет обладать еще большими скоростями.

Таблица 1.2. Стандарты Wi-Fi

Протокол	802.11	802.11a	802.11b	802.11g	802.11n	802.11ac
Используемый частотный диапазон: 2,4/5,0 ГГц	+/–	–/+	+/–	+/–	+/+	–/+
Радиус ячейки, м	До 70	До 100	До 100	До 110	До 160	До 200
Скорость передачи, Мбит/с	До 2	До 54	До 11	До 54	До 300	До 1300
Метод модуляции	GFSK, BPSK, DBPSK, DQPSK	BPSK, QPSK, 16-QAM, 64-QAM	DPSK, DBPSK, DQPSK	BPSK, QPSK, 16-QAM, 64-QAM, DBPSK, DQPSK	BPSK, QPSK, 16-QAM, 64-QAM	256-QAM

Zigbee – еще одна технология организации беспроводных сенсорных сетей, работающей на частоте 2,4 ГГц, обеспечивающая скорость передачи данных до 250 кбит/с на расстоянии до 75 м при нахождении источника и приемника в зоне прямой видимости. Оборудование, работающее на этом стандарте, характеризуется низким потреблением электроэнергии. Стандартом поддерживаются разные типы сетей: от точка-точка и звезда до сложных вариантов, включающих ретрансляторы и поддерживающих автоматическую маршрутизацию, позволяя увеличить дальность связи и передавать данные между узлами, находящимися не в зоне прямой видимости. Стандарт используется для связи как внешних устройств с ЭВМ, так и при организации сложных сетей для автоматизации управления устройствами в помещениях и домах.

RONJA (Reasonable Optical Near Joint Access) – оптический стандарт, обеспечивающий скорость передачи данных до 10 Мбит/с на расстоянии до 1400 м между объектами, находящимися в зоне прямой видимости. Стандарт используется для организации систем связи типа точка-точка в сетях типа Ethernet с полнодуплексной связью. При сложных погодных условиях (к ним относятся (снег, дождь, туман, дым) увеличивается непрозрачность среды для оптического сигнала и дальность связи уменьшается.

WiMAX (Worldwide Interoperability for Microwave Access) – высокоскоростная технология, построенная по стандарту IEEE 802.16, для связи и передачи данных на большие расстояния. Также представляет собой семейство стандартов. Аппаратура сети WiMAX по стандарту IEEE 802.16d работает на частоте 1,5…11 ГГц обеспечивает передачу данных на расстояние до 80 км со скоростью до 75 Мбит/с. Не предоставляет возможности перемещения между БС без обрыва связи.

Второй стандарт этой серии WiMAX Mobile – IEEE 802.16e работает на частоте 2,3…13,6 ГГц, обеспечивая передачу данных на расстояния до 5 км со скоростью до 40 Мбит/с. Технология WiMAX Mobile была отнесена до недавнего времени к поколению связи 4G, но в настоящее время она вытеснена более современным стандартом LTE.

Classic WaveLAN – беспроводная технология для организации локальных сетей, работающая на частотах 900 МГц или 2,4 ГГц, обеспечивая скорость передачи данных до 2 Мбит/с. Является альтернативой решений с помощью Ethernet и Token Ring.

NMT (Nordic Mobile Telephone) – стандарт беспроводной аналоговой связи, разработанный в 1978 году, использующийся по настоящее время в РФ. Покрытие сети NMT сей час сравнимо с зоной охвата сотовых операторов. NMT обеспечивает связь с абонентами по принципу частотного разделения каналов на расстояния до 70 км от БС. Для передачи данных от абонента к БС используется диапазон частот 453…457,5 МГц, а в обратную сторону – 463…467,5 МГц. Шаг каналов F_n составляет 12,5 кГц. Так как частота работы составляет 450 МГц, то

затухание сигнала при сложном рельефе ландшафта (постройки, гористая местность и т.п.) является значительным. Вдали от городов стандарт позволяет получить устойчивую связь на больших расстояниях.

AMPS (Advanced Mobile Phone System) – стандарт, разработанный в 1983 году для беспроводной связи аналогового типа, начал работу в СШАЮ а затем распространился в европейских странах, в том числе и РФ (используется компанией Билайн). В AMPS также как и в NMT используется принцип частотного разделения абонентов. Число каналов (F_n = 30 кГц) составляет 832. Построение абонентской сети схожа с принципами построения по стандарту GSM, в которой в качестве базовых используются станции, размещенные в углах сот, связанных с центрами коммутации.

Mobitex – разработанная в середине 80-х годов получила распространение в 23 странах. Хотя она и менее популярна, чем сотовая связь в стандарте GSM, активно используется как специальная связь для групп быстрого реагирования, пожарных расчетов, военными, полицией и т.д. Стандарт является открытым и основан на коммутации пакетов для передачи данных и голоса. Может использоваться для связи типа точка-точка, то есть для связи между двумя абонентами, минуя БС. Используются частоты 80, 400, 800 или 900 МГц, а пропускная способность зависит от нескольких факторов: объема передаваемой информации, загруженности каналов и т.д. и в среднем составляет 2 кбит/с.

GSM (Global System for Mobile Communications) – стандарт беспроводной цифровой сотовой мобильной связи, относится к поколению 2G. Используется узкополосный сигнал с частотным и временным разделением каналов (NBTDMA) [11, 12]. Используется четыре диапазона частот: 450, 900, 1800 и 1900 МГц, использование которых зависит от используемой абонентской аппаратуры, а также от региона. Дальность связи теоретически может достигать 120 км с использованием усилителей, но качество связи при этом будет низкой.

Развитие стандарта привело к следующим техническим особенностям. Передатчик включается только при наличии речевого сигнала, а отключается в паузах и в конце разговора. Кодирование осуществляется с регулярным

импульсным возбуждением, долговременным предсказанием и линейным предикативным кодированием с предсказанием (RPE/LTR-LTP-кодек). Скорость преобразования речевого сигнала 13 Кбит/с. Шифрование сообщений по алгоритму RSA (с открытым ключом). Для защиты от ошибок при передаче сообщений используется блочное и сверточное кодирование. При малой скорости перемещения подвижных станций используется медленное переключение рабочих частот (SFH).

TDMA (Time Division Multiple Access) – популярный стандарт сотовой беспроводной связи, использующийся более чем в 70 странах и продолжающий развиваться, занимая второе место после стандарта GSM. TDMA основан на временном разделении абонентов, работая в одном диапазоне частот. Каждому абоненту выделяется определенный временной слот, за который производится передача информации. Поочередно аппаратура выделяет такие слоты пользователям поочередно, многократно повторяя этот процесс. С ростом числа абонентов пропускная способность канала снижается.

GPRS (General Packet Radio Service) – технология пакетной радиосвязи, которая является надстройкой над стандартом GSM. При такой технологии пакеты сначала собираются, а затем передаются; теоретически достижима скорость – 171,2 кбит/с, хотя средняя скорость – 50…60 кбит/с. При использовании GSM скорость достигает величины 14,4 кбит/с. Стандарт GPRS используется преимущественно для доступа в сеть интернет, а также для передачи данных между устройствами в сети GSM.

EDGE (Enhanced Data rates for GSM Evolution) – также надстройка над стандартом GSM, представляющая технологию беспроводной связи для пакетной передачи данных. EDGE является более помехоустойчивой и скоростной технологией передачи данных за счет улучшенных алгоритмов контроля и исправления ошибок. Средняя скорость передачи составляет 75…130 кбит/с при пиковой 474 кбит/с.

CDMA (Code Division Multiply Access) – группа стандартов для сотовой связи, занимающая промежуточное положение между поколениями 2G и 3G, и

называемая 2.5G. Стандарты CDMA используют кодовое разделение абонентов при котором узкополосный сигнал модулируется псевдослучайной последовательностью, в результате получается широкополосный шумоподобный сигнал. Приемная аппаратура демодулирует входящий сигнал и получается исходный. Для различных абонентов цифровые последовательности отличаются друг от друга, за счет чего может осуществляться многопользовательская связь.

WCDMA (Wideband Code Division Multiple Access) – вариант стандарта CDMA с широкой полосой частот и гибридно-фазовым разделением абонентов. Стандарт обеспечивает скорость передачи данных до 2 Мбит/с для стационарных абонентов и до 384 кбит/с для мобильных объектов, двигающихся с большой скоростью. Для приема и передачи данных используются две полосы частот шириной 5 МГц. По сравнению с CDMA стандарт WCDMA обладает большей надежностью и скоростью передачи данных.

CDMA 2000 – семейство стандартов CDMA2000 1X, CDMA2000 1X EV-DO, CDMA2000 1X EV-DO Rev. A, B и др., являющаяся развитием стандарта CDMA. Ранний стандарт CDMA2000 1X обеспечивал скорость передачи данных до 153 кбит/с и относился к 2G. Поколение 3G состоит из стандарта CDMA2000 1X EV-DO (скорость до 2,4 Мбит/с от БС к абоненту и 153 кбит/с в обратную сторону), стандарта CDMA2000 1X EV-DO Rev. A (скорость до 3,1 Мбит/с от БС и до 1,8 Мбит/с в обратном направлении), и Rev., B (скорости до 4,9 Мбит/с и до 2,4 Мбит/с соответственно). В последнем варианте есть возможность объединения нескольких частотных каналов, поэтому теоретически скорость возрастает до 73,5 Мбит/с от БС и до 27 Мбит/с в направлении к БС. Кроме того, в группе стандарты различаются способом кодирования, принципом разделения каналов и др.

HSPA (High-Speed Packet Access) – технология-надстройка широкополосной пакетной передачи данных с полосой частот 5 МГц над мобильными сетями поколения 3G: WCDMA/UMTS, отличающаяся большей скоростью передачи данных (теоретический предел от абонента 5,7 Мбит/с и 14,4 Мбит/с в обратном направлении). Но из-за загруженности сети и ограничений оборудования такие скорости являются не достижимыми и максимальная скорость приема данных

абонентскими станциями составляет всего 7,2 Мбит/с. Дальнейшие усовершенствования стандарта направлены на повышение скоростей до 42 и 12 Мбит/с.

LTE (Long-Term Evolution) – технология беспроводных сетей, построение которых отличается от поколений 2G и 3G. Для разделения абонентов используются технология коммутации пакетов и ортогональное частотное разделение каналов (OFDMA), дающие преимущества по сравнению с сетями предыдущих поколений. Скорости передачи данных до 300 от БС к абоненту и до 75 Мбит/с в обратную сторону.

TETRA – стандарт с технологией множественного доступа с временным разделением каналов – TDMA [10, 12]. Предусматривает работу только в режиме транкинговой связи в узком диапазоне частот с ограничением по мощности сигнала. Нашел применение в системах беспроводной связи в северо-западной Европе для густонаселенных городских территорий. Может использоваться для передачи голоса и данных в диапазонах 410…430, 870…875, 915…921 МГц. Тип связи – цифровой.

***APCO* 25** – международный стандарт, разработанный Association of Public Safety Communications Officials, использующий частотное разделение каналов (FDMA). Нашел применение для организаций, обеспечивающих общественную безопасность и службах МЧС [10]. Стандарт позволяет создавать соединения между мобильными абонентами, минуя БС. Стандарт APCO 25 позволяет работать в транкинговом и конвенциональном режимах. Цифровое абонентское оборудование обратно совместимо с аналоговыми пользовательскими устройствами связи. Стандарт предусматривает полную совместимость оборудования от портативных и мобильных абонентских устройств до БС различных производителей, а также позволяет поддерживать связь с десятками тысяч абонентов, принадлежащих различным организациям. Цифровая передача голоса и данных осуществляется со скоростью 9,6 кбит/с по каналу шириной 12,5 кГц с возможностью перехода на значение 6,25 кГц. Стандарт поддерживает

режим шифрования без ухудшения качества голосового сигнала. Используется три диапазона частот: 138…174, 406…512 и 746…869 МГц.

Практически во всех странах организации, особенно службы по обеспечению безопасности, испытывают дефицит радиочастотных каналов для развертывания систем мобильной связи. Каналов становится еще меньше из-за продажи прав использования некоторых диапазонов частот коммерческим операторам связи. Это влечет к сужению полосы канала с 25 до 12,5 кГц производителями.

1.1.3. Особенности разработки новых стандартов беспроводных сетей

В отличие от типового жизненного цикла при разработке новых стандартов систем связи мной выявлено несколько отличий.

1. Этап возникновения идеи обуславливается в потребности новой системы связи. В результате формулируются основные требования к параметрам системы связи в соответствии с ее назначением.

2. Далее выбирается готовый протокол связи или принимается решение о необходимости разработки нового протокола. Здесь отмечу, что открытые протоколы связи чаще поддерживаются производителями оборудования, чем закрытые из-за большей доступности документации, предоставляемой разработчиками протоколов.

3. Разработка новых протоколов или модернизация существующих для нового проекта системы связи сопряжено с затратами времени и средств, необходимостью выделения частотного диапазона, но позволяет добиться требуемых для данной системы связи параметров. В этом случае новый протокол будет несовместимым с сетевым оборудованием сторонних фирм, что ограничит рынок сбыта готовых систем связи. Проработка вопросов интеграции разрабатываемой системы связи в городскую сеть также занимает значительные ресурсы.

4. Поддержка открытых протоколов, разработанных ранее, позволяет продлить этап эксплуатации их жизненного цикла.

5. Продажа лицензии фирмы-разработчика протоколов осуществляется только на мобильную аппаратуру, а для БС документация закрыта.

При разработке новых стандартов связи определяются: методы передачи данных, помехоустойчивого кодирования, дальность связи, совместимость с другими сетями, потребляемая мощность станций.

Развитие систем радиосвязи происходит по поколениям; аналоговые стандарты снимаются с эксплуатации.

Поэтому систему связи с подвижным объектом будем рассматривать как сложную информационную систему (ИС), для которой характерны следующие свойства: большое число взаимосвязанных узлов и связей между ними, изменчивость ИС во времени (деградация, развитие и т.п.) и стохастический характер поведения.

1.2. Анализ угроз и уязвимостей для систем радиосвязи

1.2.1. Анализ угроз

Угроза безопасности – это совокупность условий и факторов, которые создают потенциальную опасность, связанную с утечкой информации, несанкционированными и/или непреднамеренными воздействиями на нее. Опасность – это состояние, в котором находится объект вследствие появления угрозы [2].

Угроза возникает из источника, направлена на объект и способна проявляться. У объекта злоумышленником находятся уязвимости, через которые возможны реализации атак, снижающие или нарушающие безопасность передаваемой по сети информации. Для информации актуальны угрозы нарушения: конфиденциальности, целостности, доступности, наблюдаемости и аутентичности.

Конфиденциальность информации – свойство, заключающееся в возможности получения информации только авторизованным пользователем [6]. Конфиденциальность информации необходимо обеспечивать для усложнения пассивных атак, реализуемых злоумышленником. Основным способом обеспечить конфиденциальность передаваемых данных по беспроводной сети является их шифрование. Криптостойкость алгоритмов шифрования, а также вид протокола передачи данных будут определять уровень защиты данных от атак типа: пассивное прослушивание и перехват, незаконное использование прав (маскарадинг) и похищение ключей. Доступным и простым способом добычи конфиденциальной информации являются методы социальной инженерии с помощью сотрудников компаний.

Реализация угроз нарушения целостности приводят к тому, что неавторизованный пользователь может модифицировать информацию. Модификация подразумевает изменение, повреждение или разрушение информации. Для множества типов информации присуща ценность только тогда, когда гарантируется правильность данных. Возможность искажения информации позволяет злоумышленнику получать полный контроль над потоком данных, циркулирующих в системе связи, пользоваться привилегиями другого пользователя, передавать данные от чужого имени. Для противодействия таким угрозам служит применение различных цифровых подписей и однонаправленных функций хеширования.

Доступность объекта, системы, услуги – свойство, заключающееся в возможности получении доступа и использования процесса, ресурса, услуги пользователем или процессом, обладающим необходимым уровнем полномочия, в установленных рамках, заданных политикой безопасности, в течение определенного промежутка времени, значение которого не превышает заданное. Иными словами ресурс должен быть доступен авторизованному пользователю в определенном состоянии, в том месте и в то время, когда он необходим. Но надо отметить, что не всегда целью злоумышленника является непосредственно определенный ресурс системы, – это может быть объект или информация более

высокого уровня, нарушая доступность которых, блокируется доступ к объектам всех зависимых уровней. Основным видом атак, нарушающих доступность информации является DoS-атаки (Denial of Service), приводящие к отказу в обслуживании системы [13, 14]. При распределенной атаке злоумышленника реализуются DDoS-атаки, когда в распоряжении злоумышленника оказывается множество объектов, с которых ведется атака на жертву.

Угрозы нарушения аутентичности, то есть обход проверки аутентификации (проверки принадлежности объекту или пользователю предъявленных идентификаторов) для выдачи себя за авторизованного пользователя или процесс. Актуальной для систем связи является атака этого вида "человек посередине" (Man in the middle). Злоумышленник незаметно устанавливает связь либо с двумя абонентами, или абонентом и БС, оставаясь для них незаметными. Получая полный контроль над передаваемыми данными, злоумышленник может осуществлять любые действия с ними: перехват, анализ, модификацию, глушение и т.п. Еще одним развитием атак нарушения аутентичности является навязывание ложных адресов (ARP-spoofing), MAC-адресов, подмена базовых станций и др.

Существует также вероятность нарушения наблюдаемости – свойства систем, которое заключается в возможности фиксации деятельности пользователей и процессов, их причастности к конкретным событиям и/или процессов, фактов нарушения политики безопасности или скрытия ответственности за события, имевших место быть. Примерами таких атак являются изменение журналов протоколирования событий, вывод из строя систем контроля, DoS-атаки на журналы и протоколы, внедрение вредоносного программного обеспечения.

Для каждого описанного стандарта связи имеются свои особенности при определении угроз несанкционированного доступа передаваемой информации по радиоканалу от источника к приемнику. Все стандарты невозможно защитить от пассивного прослушивания радио эфира. Для анализа угроз рассмотрим систему, изображенную на Рисунок 1.1. Угрозы могут исходить из внешней среды или

злоумышленника и быть нацеленными на абонентскую станцию, канал передачи, БС. Основными угрозами системе радиосвязи являются следующие.

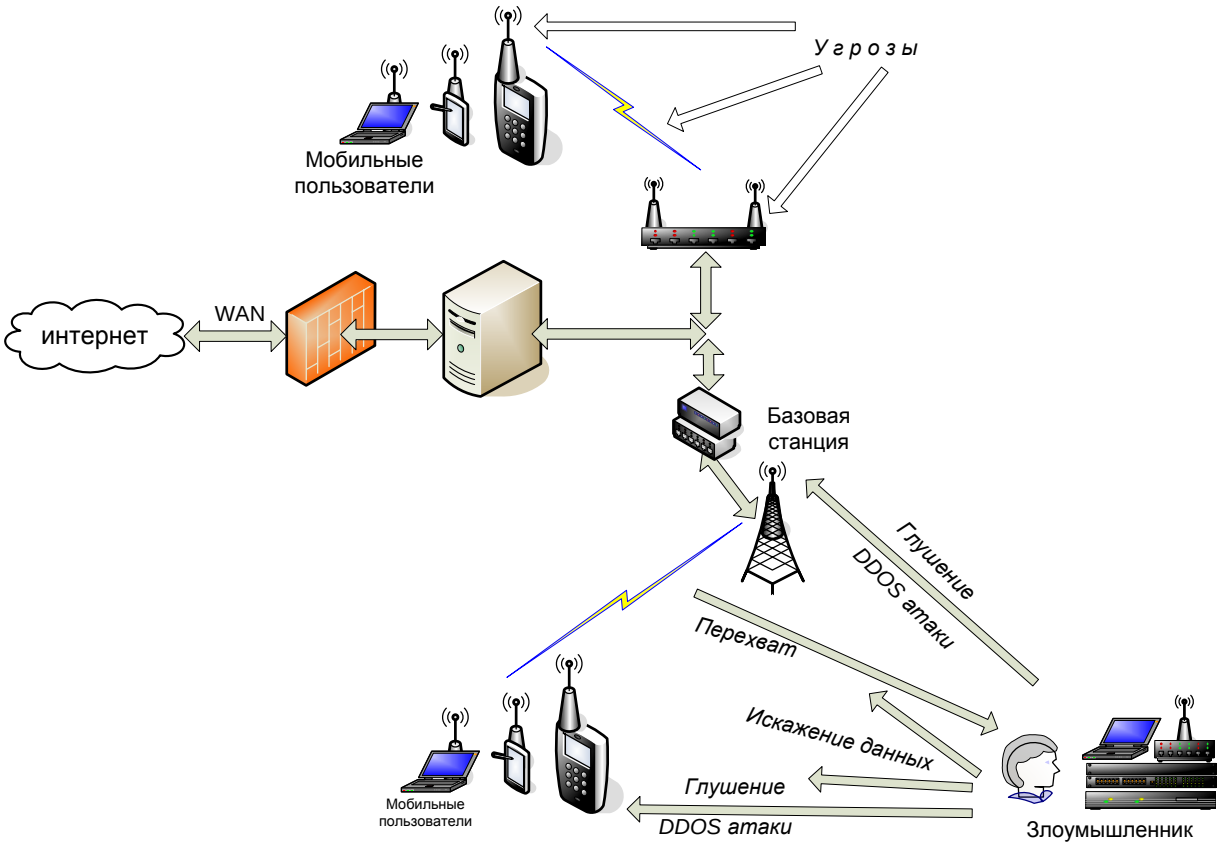


Рисунок 1.1 Анализируемая система радиосвязи

1. Внешняя помеха, источником которой может быть как внешняя среда (неумышленная), так и аппаратура злоумышленника (злонамеренная).

2. Перехват (прослушивание) информации с целью дальнейшей расшифровки. Удобство и легкость развертывания беспроводной сети оборачивается мобильностью не только пользователей, но и злоумышленника, местоположение которого определить достаточно сложно.

3. Искажение информации с целью препятствия приему пакета, искусственного сбоя.

4. DDoS-атака с целью перегрузки канала и/или аппаратуры радиостанций. Такие атаки очень эффективны и трудно поддаются анализу.

5. Подмена информации.

6. Клонирование SIM-карт, аппаратуры.

Злоумышленником могут реализовываться сразу несколько из шести перечисленных. Например, если уровень злонамеренно генерированной помехи превосходит допустимый уровень, при котором приемо-передающей аппаратуре невозможно выделить полезный сигнал, возникает глушение. Глушение мобильной станции абонента производится с целью ее подмены аппаратом злоумышленника, или чтобы не дать клиенту реализовать соединение с БС. Может осуществляться постановкой помех, или направленными DoS-атаками. Глушение БС опять же может осуществляться для лишения пользователя услуг связи, или для подмены БС пользователя базовой станцией злоумышленника.

Доступность аппаратуры для беспроводной связи делает возможным организацию ложной точки доступа с имитацией работы с фирменными сетевыми ресурсами. При этом конфиденциальная информация, исходящая от аппаратуры и самих пользователей, становится добычей злоумышленника.

Неправильная конфигурация оборудования, уязвимости в криптозащите и системе аутентификации облегчает взлом сетей.

Увеличение уровня привилегий (Elevation of privilege) способствует получение контроля над всей системой и наивысшего уровня доступа к ресурсам системы связи [15].

Подмена принимаемой пользователем информации также может иметь целью вторжение и модификацию данных, после чего следует DoS-атака.

Если перехват и расшифровка сигнала в реальном масштабе времени невозможны из-за недостаточного быстродействия аппаратуры, то они могут производиться Off-line. Все протоколы способны шифровать трафик, но делают это в той степени защиты, которая была заложена при разработке стандарта и в соответствии с местным законодательством (здесь и далее во всей работе будут учитываться требования законодательства РФ, или общие установки, заложенные в стандарт связи).

Для анализа угроз системам радиосвязи рассмотрим ее основные компоненты (см. Рисунок 1.2). Базовая станция (БС) может передавать информацию по каналам связи с мобильными объектами: носимыми

радиостанциями или радиотелефонами, мобильными радиостанциями, установленными, например, в автомобиле, радиомодемами, установленными в зданиях, стационарными радиостанциями или другими базовыми станциями. Через коммутаторы и контроллеры базовой станции осуществляется связь с телефонными аппаратами посредством автоматической телефонной станции (АТС). Центры коммутации обеспечивают взаимодействие между абонентами, устанавливая соединения, а также между другими системами радиосвязи.

Ресурсами системы связи являются:

- радиоканалы;
- оборудование;
- услуги сети;
- базы данных.

Для обеспечения информационной безопасности радиосети необходимо исключение несанкционированного использования системы и обеспечение секретности переговоров подвижных абонентов [16-20].

Угрозами являются:

1. Блокирование какой-либо службы или услуги мобильной сети:

- уничтожение сообщений;
- задержка сообщений;
- перегрузка сети ложными сообщениями;
- отключение узлов сети командами управления;
- постановка радиопомех.

2. Несанкционированное использование ресурсов сети: работа с запрещенными к использованию ресурсами сети путем маскировки под другого пользователя, которому доступ к услуге сети разрешен и/или неправомерное использование разрешенных ресурсов сети;

Реализация угроз может осуществляться с использованием похищенного оборудования, знаний внутренней работы и устройства сети.

Неправомерное использование разрешенных ресурсов сети может привести к доступу: к секретной информации, к оборудованию, а также к возможному изменению статуса или приоритета мобильной станции злоумышленника.

Наиболее действенными способами защиты является контроль системы связи, резервирование, шифрование, аутентификация и идентификация пользователей и операторов, надежные схемы управления доступом пользователей к ресурсам сети.

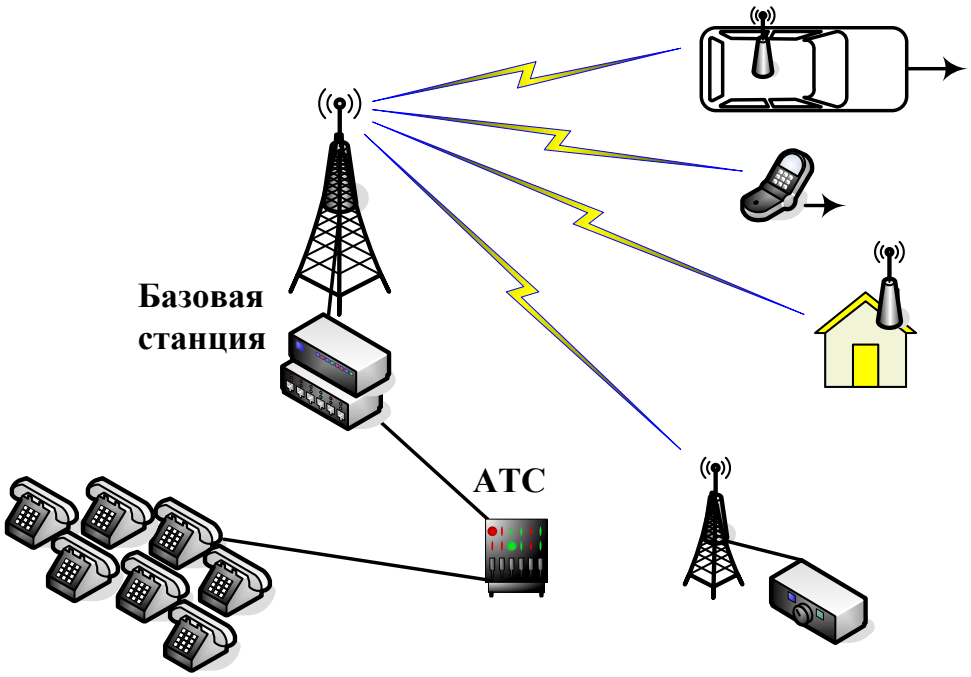


Рисунок 1.2. – Структура системы связи

1.2.2. Анализ уязвимостей

Нарушение информационной безопасности возникает вследствие реализации угроз из-за наличия у систем связи уязвимостей. Последние обусловлены:

- топологией сети;
- используемыми протоколами связи;
- особенностями функционирования;
- недостатками в программном обеспечении;

- конструкторскими и схемотехническими решениями;
- условиями эксплуатации и территориальным расположением.

При построении беспроводных сетей различных стандартов возможны следующие источники возникновения уязвимостей:

- среда передачи данных;
- технические параметры стандартов беспроводных сетей;
- системы аутентификации;
- криптографические методы и алгоритмы;
- программное и аппаратное обеспечения;
- человеческий фактор.

В арсенале злоумышленников имеются различные программные и технические средства для реализации перечисленных угроз (см. рис. 1.1). Например, сканирование доступных беспроводных сетей позволяет злоумышленнику получить следующие сведения:

- SSID – идентификатор сети;
- производителя оборудования;
- механизм шифрования;
- MAC-адрес оборудования;
- параметры канала, по которому идет передача данных;
- координаты пользователя (при работающем GPS-модуле).

1.3. Анализ подходов при организации защиты систем радиосвязи

Проанализируем основные подходы и алгоритмы, используемые разработчиками для защиты самых распространенных систем радиосвязи.

Blue Tooth

В зависимости от установок пользователя в спецификации Blue Tooth предусмотрено три режима защиты [21].

1. Минимальный (режим по умолчанию) – никаких специальных мер безопасности не используется, происходит кодирование данных общим ключом, которые могут приниматься любыми устройствами без ограничений.

2. Защита на уровне устройств – меры, включающие процедуры аутентификации и идентификации. Происходит разграничение функций устройства в зависимости от уровня доступа. Уровни доступа зашиты в специализированной интегральной микросхеме (ИМС); в зависимости от ее прошивки устройство связи обменивается данными с другими устройствами.

3. Защита на уровне сеанса связи – данные кодируются 128-битными ключами, генерируемыми случайным образом синхронно в паре устройств, участвующих в сеансе связи. В этом режиме используется шифрование данных.

Два последних режима могут использоваться совместно.

В процессе аутентификации оба устройства рассчитывают значение на основе отправленного адреса-идентификатора и полученного случайного числа. При несовпадении результатов расчета связь прерывается.

Авторизация необходима для того, чтобы для опознанного Blue Tooth-устройства был предоставлен доступ к определенной информации или услугам. Предусмотрено три уровня устройств: доверенное (trusted), не вызывающее доверия (non-trusted) и неизвестное (unknown), – ограничивают доступ в соответствии с политикой, называемой защитными слоями (layer security service).

Шифрование в стандарте Blue Tooth также используется в трех видах: без кодирования, кодирование в процессе установления связи между устройствами и кодирование при установлении связи и передачи информации.

Слабыми местами защиты Blue Tooth-устройств являются:

− предоставление пользователю широких полномочий для настройки и контроля над устройством;

− недостаточные средства аутентификации пользователя, что позволяет использовать нападения типа spoofing (радиодезинформации) при неправильном распознавании устройств;

− первичный процесс распознавания устройств (pairing) при котором по незакодированным каналам происходит обмен ключами, которые можно перехватить при прослушивании. Далее хакер, получив ключ инициализации, может рассчитать ключ связи;

− допускаемое стандартом использование коротких паролей, которые быстро подбираются с помощью списка стандартных последовательностей, наиболее часто используемых пользователями;

− возможность использования пользователями спаренных ключей связи вместо динамических, и модульных вместо комбинаторных. Это сводит на нет всю систему защиту ключей.

GSM

Для защиты мобильных станций и каналов связи используется шифрование и кодирование. Кроме того, предусмотрены следующие методы:

− защита от НСД к мобильной станции – пароль на вход;

− идентификация абонента с помощью уникального международного номера (INSI и IMEI);

− аутентификация абонента при каждом выходе на связь (алгоритм *A*3);

− шифрование информации, передаваемой по радиоканалу (алгоритм *A*5) с расшифровкой ключа (по алгоритму *A*8);

− секретность местонахождения абонента;

Алгоритм аутентификации *A*3 работает по аналогии со спецификацией Blue Tooth (см. Рисунок 1.3). Мобильная станция посылает запрос на БС при выходе на связь. Аппаратура БС генерирует случайное 128-битное число, которое отсылается абоненту. В мобильной станции по полученному числу и индивидуальному ключу аутентификации K_i (128 бит) по алгоритму *A*3 определяется отклик длиной 32 бита, который отправляется на БС. БС в свою очередь проделывает те же операции, а принятый отклик сравнивается с результатом расчета, и если они совпадают, то связь устанавливается.

Алгоритм *A*3 не стандартизован, а зависит от оператора сети. Оператор может использовать и стандартные алгоритмы (COMP128, COMP128-2, COMP128-3, MILENAGE). Выполнение алгоритма ограничено 500 мс.

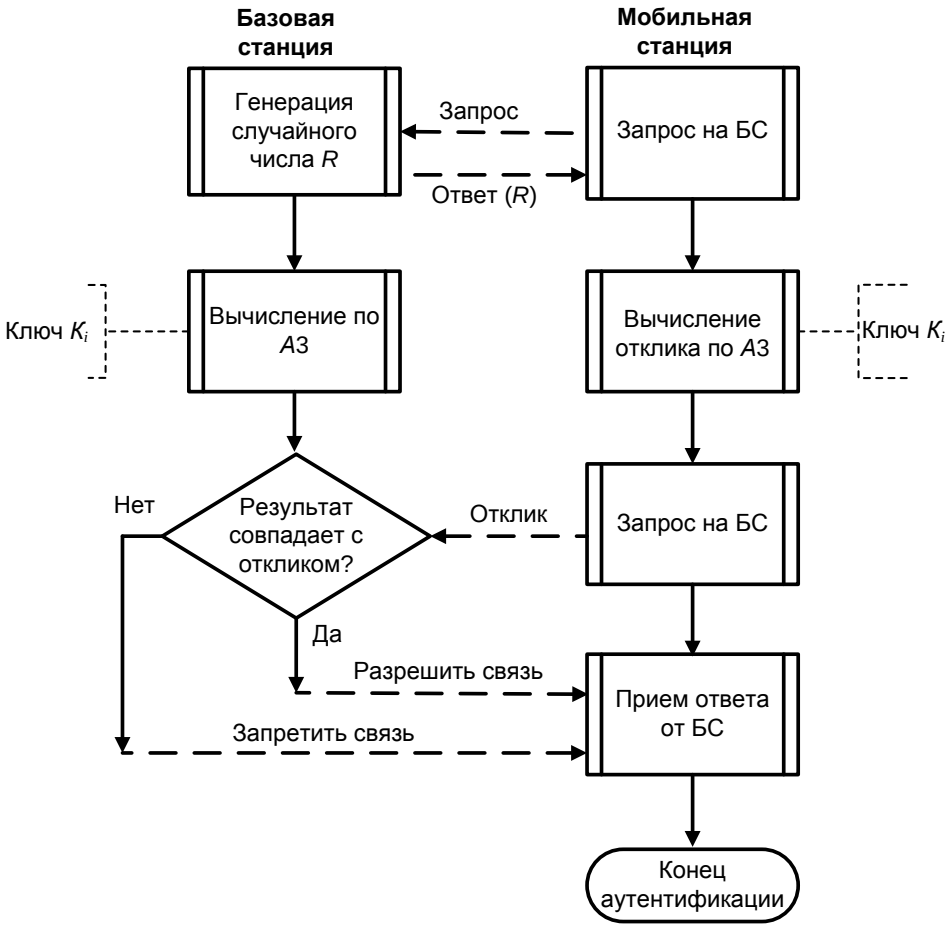


Рисунок 1.3. Процесс аутентификации в спецификации GSM

*A*5 – поточный алгоритм шифрования, используемый для защиты информации, поступающей от мобильной станции на БС. В алгоритме шифрования используется операция XOR (побитовое сложение по модулю два) псевдослучайной последовательности и шифруемой информации. Датчик псевдослучайных чисел реализован на трех сдвиговых регистрах (19, 22 и 23 бит). В алгоритме управления данными в регистрах производятся смещения, благодаря чему циркуляция информации приобретает неравномерный характер.

Число разновидностей алгоритма *A*5 конечно: в мире существует три модификации. В США и Европе распространен алгоритм *A*5/1 (см. Рисунок 1.4).

Также может использоваться алгоритм *A*5/2 в котором использован добавочный регистр (17 бит) для управления сдвигом остальных регистров. Последним вариантом является *A*5/3, работающий по алгоритму Касуми (см. Рисунок 1.5).

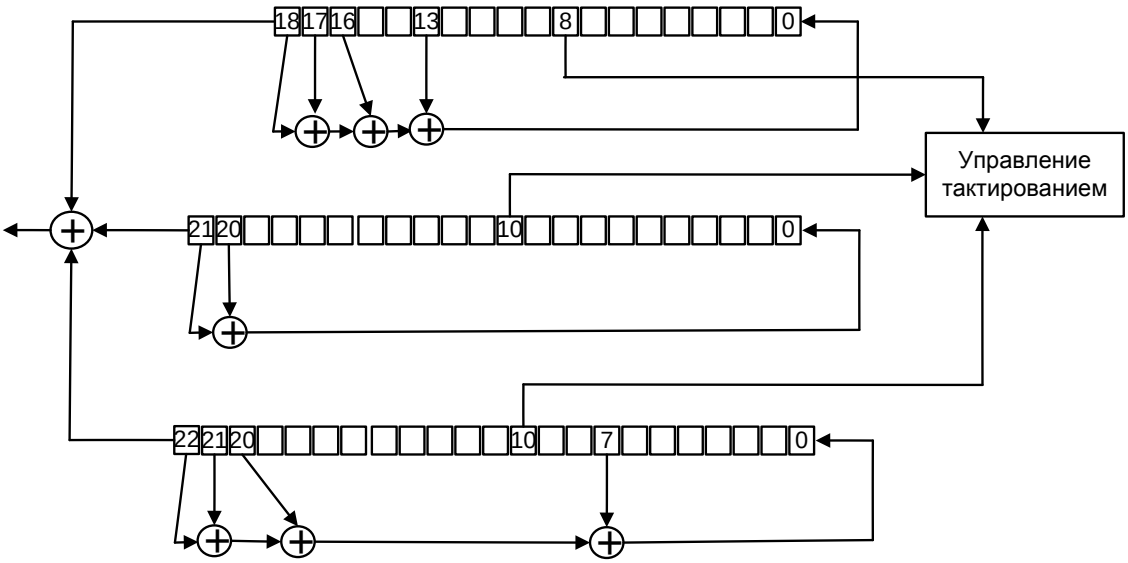


Рисунок 1.4. Принцип работы алгоритма *A*5/1

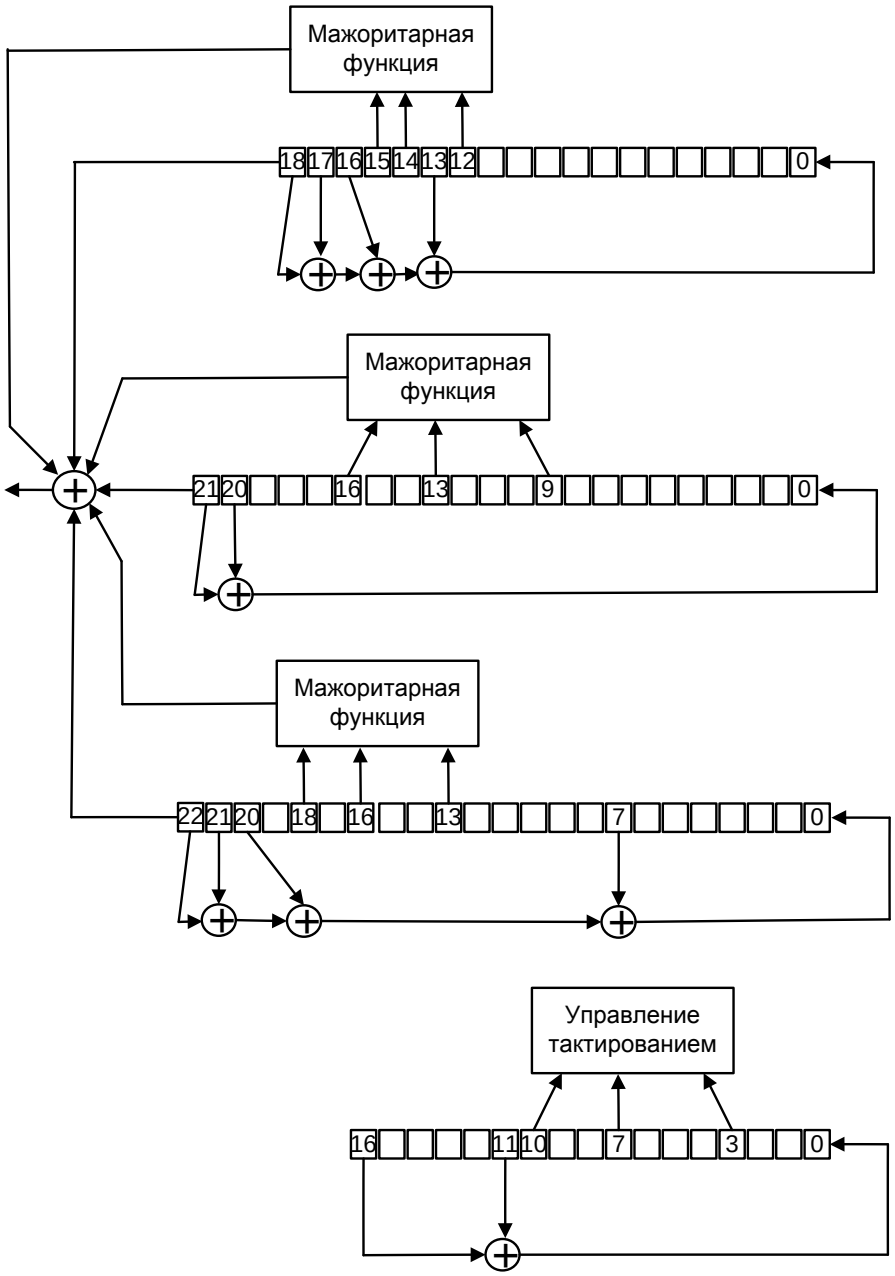


Рисунок 1.5. Принцип работы алгоритма *A*5/3

С помощью алгоритма *A*8 формируется ключ шифрования в SIM-карте. Длина такого ключа составляет 64 бит. Если длина сформированного ключа меньше 64 бит, то он дополняется нулями. Входными данными для алгоритма *A*8 являются сгенерированное случайное число и индивидуальный ключ аутентификации K_i, которые так же, как и во всех перечисленных выше алгоритмах, вычисляются как в мобильной станции, так и в БС.

Все алгоритмы за исключением алгоритма *A*5 зашиты в SIM-карту абонента.

Wi-Fi

Для защиты самой распространенной на данный момент сети Wi-Fi используются следующие технологии.

1. Технология WEP (Wired Equivalent Privacy) была разработана для шифрования потока передаваемых данных внутри ЛВС с использованием алгоритма RC4 со статическим ключом. В алгоритме используется 64-, 128-, 256- и 512-битное шифрование. Причем часть ключа является статической, а другая часть – динамической. Последняя часть называется вектором инициализации IV (Initialization Vector) и составляет 24 бит. Так как взлом 24- битного вектора инициализации, повторяющегося через определенный промежуток времени, возможен методом перебора (примерно $16 \cdot 10^6$ комбинаций), а остальная часть ключа взламывается за несколько секунд, то получить права зарегистрированного пользователя для входа в сеть – дело времени. Поэтому алгоритм RC4 на сегодня является нестойким. Для повышения уровня безопасности технологии WEP используется дополнительно стандарт IEEE 802.1x или технология VPN.

2. WPA (Wi-Fi Protected Access) – технология защиты с более стойким алгоритмом шифрования. В WPA используется протокол интеграции временного ключа (TKIP – Temporal Key Integrity Protocol), в котором каждому устройству присваивается генерируемый 128-битный ключ (число вариантов достигает $5 \cdot 10^{11}$) и технология проверки целостности сообщений (MIC – Message Integrity Check), созданная для защиты пакетов от перехвата и их перенаправления. В алгоритме MIC сверяются отправленные данные от отправителя и от получателя и в случае расхождения, данные не используются. Алгоритм генерации ключей функционирует по иерархическому принципу с динамической их заменой через каждые 10 000 переданных пакетов.

Разработано два вида технологии WPA. WPA-PSK (Pre-shared key) – технология больше всего подходит для домашней или офисной беспроводной сети, использующая для генерации ключей и входа в сеть ключевую последовательность. При подборе последовательности злоумышленником все

преимущества технологии теряются. Другая WPA-802.1x – производит вход в сеть через сервер аутентификации.

3. WPA2 – построенный на предыдущей технологии стандарт, использует спецификацию IEEE 802.11i. Шифрование производится по алгоритму AES, аутентификацию – по IEEE 802.1x, а также защитных технологий RSN и CCMP. В технологии WPA2 используется два типа ключей: PTK (Pairwise Transient Key) – для защиты однонаправленного трафика, уникальный для каждого клиента и GTK (Group Temporal Key) – для шифрования широковещательного трафика. PTK позволяет обнаруживать подмену адресов и перехват данных, что не может сделать GTK. При отправке широковещательного пакета авторизованным пользователем, другие пользователи в ответ отправляют отправителю свой личный ключ (PTK). Отправленные ключи могут быть перехвачены злоумышленником при прослушивании сети и перехвате информации.

По статистике, технологию защиты WPA или WPA2 использует большинство пользователей при поддержке современного оборудования для Wi-Fi сетей.

4. WPS (QSS) – получившее широкое распространение технология, для подключения к сети с помощью "одного нажатия". Закравшаяся ошибка в стандарт WPS, позволяющая получать доступ к сети с помощью 8-ми символьного цифрового кода (PIN), позволяет осуществить его взлом с помощью подбора всего 4-х цифр из восьми. Для этого необходимо перебрать 10 000 вариантов, чтобы получить доступ к сети и узнать пароль вне зависимости от его сложности. Отправляя 10…50 запросов в секунду (чтобы не попасть на проверку безопасности), защита, построенная по технологии WPS, взламывается за 3…15 часов.

5. IEEE 802.1x – относительно новый стандарт семейства, в котором за основу взят IEEE 802.11 с исправлением недостатков последнего. В IEEE 802.1x используются: протокол расширенной аутентификации (EAP –Extensible Authentication Protocol) совместно с сервером аутентификации (RADIUS – Remote Authentica-tion Dial-In User Server) пользователей с использованием логина и

пароля, а также протокол целостности и шифрования данных между сервером и клиентом (TLS – Transport Layer Security), производящим их взаимную аутентификацию. TLS служит технологией для защиты от перехвата и подмены сообщений.

После аутентификации пользователя в технологии IEEE 802.1x ему отправляется зашифрованный (128-битный по умолчанию) ключ на срок действующего сеанса связи. При установке нового сеанса генерируется новая ключевая последовательность, отсылаемая пользователю. Недостатком стандарта является необходимость развертывания сервера идентификации, что увеличивает сложность и стоимость.

6. Технология виртуальных частных сетей (VPN – Virtual Private Network), предложенная компанией Intel, основана на создании безопасных тоннелей от пользователя до узла доступа или сервера. В VPN-туннеле информация шифруется; для этого используются протокол IPSec (в 70%), PPTP или L2TP с алгоритмами шифрования DES, Triple DES, AES и MD5. Взломостойкость VPN очень высока, но из-за сложности конфигурирования технология VPN используется преимущественно в крупных корпоративных сетях.

1.4. Требования к системам связи. Проблемы, возникающие с ростом их сложности

К системам связи предъявляются следующие требования.

1. Высокая готовность – способность в любой момент времени и в любом месте системой связи выполнять свои функции. Готовность в свою очередь обеспечивается такими показателями, как: живучесть, помехоустойчивость, помехозащищенность и электромагнитная совместимость с другими радиоэлектронными средствами, а также надежность.

2. Устойчивость функционирования – комплексный показатель. Регламентируется рядом нормативных документов: ГОСТ Р 53111-2008, "Устойчивость функционирования сети связи общего пользования. Требования и

методы проверки", Приказ Министерства связи и массовых коммуникаций РФ от 25 августа 2009 г. № 104 "Об утверждении Требований по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования" и др. как способность сохранять свою целостность при отказе части компонентов системы связи. В свою очередь целостность определяется как способность обработки информации при взаимодействии компонентов систем связи. Целостность обеспечивается функциональной совместимостью протоколов связи и интерфейсов устройств.

Устойчивость функционирования системы связи обеспечивается: необходимым уровнем показателей надежности, заложенных при проектировании средств связи, соблюдением условий эксплуатации, своевременностью проведения технического обслуживания аппаратных и программных средств, проверки функционирования, диагностики и анализа неисправностей сети. Показателем устойчивости функционирования является коэффициент готовности, определяемый как вероятность того факта, что система связи окажется в работоспособном состоянии в произвольный момент времени за исключением времени простоя.

3. Пропускная способность – своевременная передача и прием заданных потоков сообщений в единицу времени, которая определяется количеством каналов связи, числом переговоров, обеспечиваемых в единицу времени, количеством сообщений, переданных в единицу времени, суммарной скоростью передачи данных, скоростью передачи данных.

4. Мобильность – способность развертывания и свертывания в установленные сроки, изменение структуры системы связи и ее дислокации.

5. Защищенность – способность системы радиосвязи противостоять действиям, направленным на взлом алгоритмов защиты системы связи. Поэтому при функционировании систем связи необходимо: сохранять целостность и доступность информации, предусмотреть систему защиты информации от внешних атак, а также политику безопасности. За показатель защищенности в

моей работе принято время взлома компонентов системы связи с подтверждением в средствах массовой информации.

6. Доступность – способность обеспечения доступа для авторизованных пользователей к ресурсам системы связи с сохранением приоритетов и способов установления связи. Доступность обеспечивается рациональным выбором структуры сети и ее состава, распределением мобильных и базовых станций с учетом ландшафта местности, планирование ресурсов систем связи с учетом потребления, своевременное развертывание и обеспечение готовности систем связи.

7. Управляемость – способность изменения состояния системы связи в зависимости от управляющих сигналов и внешней обстановки. Управляемость обеспечивается: своевременностью подачи управляющих воздействий при изменении условий функционирования, эффективностью средств автоматизации в средствах и комплексах связи, надежностью средств связи, оперативностью принятия решений, эффективным проектированием систем управления и средств связи.

Рост сложности систем представим как эволюцию, которая, в зависимости от предпринятых средств обеспечения устойчивости, может стать причиной постепенной деградации ИС [21-25]. Средства обеспечения устойчивости предназначены для:

- контроля работоспособности;
- резервирования элементов системы;
- защиты подсистем;
- реконфигурации и управления.

Действие средств обеспечения устойчивости приводит к снижению или исключению первичных последствий в результате действия внешних воздействующих факторов на ИС. При этом ИС может осуществить переход в одно из устойчивых промежуточных состояний в зависимости от эффективности и оперативности средств обеспечения устойчивого функционирования. ИС после

воздействия на нее внешних факторов может перейти в одно из следующих состояний(см. Рисунок 1.6):

- работоспособное;
- аварийное;
- неработоспособное.

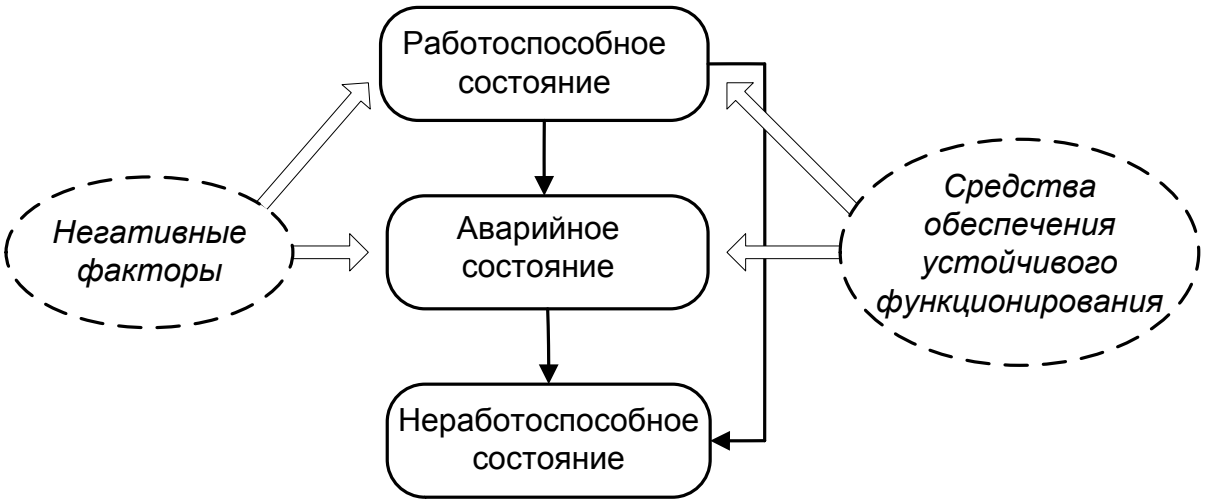


Рисунок 1.6 – Возможные переходы ИС при действии внешних негативных факторов

Не смотря на то, что ИС может остаться в работоспособном состоянии, после действия внешних факторов могут проявляться вторичные последствия от их действия, представляемые как плохо управляемые или неуправляемые процессы различной физической природы: тепловые, электрические и т.д. Таким образом, средства обеспечения устойчивого функционирования оказывают влияние на развитие и результат первичных, вторичных и т.д. последствий от действия неблагоприятных воздействий на сложную ИС.

Поэтому необходимо, во-первых, сохранение работоспособности ИС, а, во-вторых, успешное выполнение поставленной перед ней задачи. Средства обеспечения устойчивости должны иметь большее быстродействие, чем влияющие внешние факторы.

Область действия (точка или область), природа (тепловая, электрическая, механическая и др.) и интенсивность (импульс или продолжительное воздействие) – основные факторы при действии на ИС негативных факторов.

Поэтому негативные воздействия можно рассматривать как многофакторное дестабилизирующее действие на ИС [26-30].

Источники внешних воздействий – это влияние природы, других сложных систем, субъектов, а внутренних воздействий – отказы элементов и действия оперативного персонала.

Таким образом, поддержание устойчивого функционирования – это соревновательный процесс, при котором эффективность и быстродействие средств для обеспечения устойчивости "проверятся" воздействующими негативными факторами, наносящими сложной ИС определенный ущерб.

В связи с тем, что понятие устойчивости известно давно и используется при разработке технических средств, создана развитая теория, позволяющая исследовать это свойство, обеспечение устойчивого функционирования сложных систем связи с наземными подвижными объектами, особенно при их разрастании вызывает трудности, поэтому в настоящей работе этому аспекту уделяется внимание.

Устойчивость системы связи можно интерпретировать как способность выполнять основные функции во время атак, повреждений и аварийных ситуаций [31-34], или как способность ИС адаптироваться к новым условиям при влиянии дестабилизирующих воздействий, которые приводят к частичному ухудшению работоспособности, и выполнять свою основную функцию.

Значимость работ в этой области обусловлена основными свойствами сложных технических систем.

− Рост сложности и стоимости ИС приводит к значительному ущербу при реализации угроз даже в отношении отдельных подсистем.

− В сложных ИС восстановление работоспособности является трудоемкой операцией.

− Многочисленные связи между подсистемами, реализующиеся по каналам и потокам, могут стать причиной нарушения работоспособности ИС вплоть до ее гибели.

Развитие сетей радиосвязи сопряжено с внедрением новых технологий и услуг (MMS, SMS, WAP, GPRS, WEB и др.), а также интеграцией в сети распространения данных – интернет. Такая эволюция приводит к следующим негативным последствиям.

Во-первых, использование технологий беспроводного доступа, таких как Blue Tooth, WiFi, LTE и пр., ведет к образованию новых угроз из-за изменения среды передачи данных (см. п. 1.2.2).

Во-вторых, новые программно-технические решения для реализации новых функций и введения дополнительных услуг, дают почву для появления новых атак на сети подвижной связи.

В-третьих, использование приложений с активным обменом данными приводит к росту трафика и перегрузке каналов связи.

В-четвертых, рост числа абонентов и их неравномерное распределение по местности приводит к усложнению расчетов для размещения БС и определения их числа.

В-пятых, доступность мобильных абонентских станций и оборудования для сетей приводит к росту подготовленных атак, а также клонирвоания абонентских терминалов и БС.

С другой стороны, устойчивость функционирования сложных ИС, состоящих из большого числа элементов, характеризует способность этих элементов противостоять воздействию внешних факторов. Поэтому, устойчивость функционирования ИС определяется ее структурой (топологией) и надежностью ее элементов. Причем отказ элементов сети должен компенсироваться, а основная цель функционирования системы сохраняться как можно дольше по времени в условиях действия вредных факторов [21].

Модель оценки устойчивого функционирования сложной ИС должна адекватно отражать зависимость ее показателей от параметров системы связи: топологии сети **G**, цели **C** и условий ее функционирования **U**, надежности **P**, а также решаемых задач **Z**. Общий показатель устойчивости системы **Q** имеет

интегральный и комплексный характер зависимости от устойчивости входящих подсистем:

$$\mathbf{Q} = F(Q_1, Q_2, ..., Q_k),\ Q_i = f(G_i, C_i, U_i, Z_i, P_i). \quad (1.1)$$

Запас структурной устойчивости системы будет определяться ее избыточностью и обеспечиваться резервированием элементов. Надежность системы – сложный функционал, включающий как надежность входящих в ИС элементов, так и структуру подсистем:

$$\mathbf{P}_{\text{сист}} = f(P_i, G_i),\ i = \overline{1, n}. \quad (1.2)$$

С увеличением сложности ИС растет сложность моделей (1.1) и (1.2), и уменьшается уровень негативных воздействий, достаточный для перехода ИС в худшее состояние. Параметры математических моделей, характеризующих устойчивость функционирования системы связи можно получить с помощью статистического анализа оценок.

1.5. Постановка задачи

Открытую сеть связи с наземными подвижными объектами характеризуется целевыми показателями: защищенности, устойчивости, под которой понимается совокупность трех свойств: надежности, живучести, помехоустойчивости.

Учитывая случайный характер возможностей нарушителя и характеристик системы связи при их взаимодействии, *защищенность* канала связи представима суммой вероятностей скрытности $P_{\text{скр}}$ и помехозащищенности $\text{Р}_{\text{ПЗ}}$:

$$P_{\text{ЗКан}} = P_{\text{скр}} + P_{\text{ПЗ}} - P_{\text{скр}} P_{\text{ПЗ}}$$

где вероятность того, что канал будет раскрыт при помощи средств разведки:

$$P_{\text{разв}} = 1 - P_{\text{скр}}$$

вероятность подавления канала связи помехой:

$$P_{\text{подавл}} = 1 - P_{\text{ПЗ}}.$$

От успешного проведения разведки противопоставляется трехуровневая защита: внешний уровень – энергетический, затем структурный и

информационный. Поэтому скрытность работы канала:

$$P_{\text{скр}} = 1 - P_{\text{разв}} = 1 - P_{\text{обнаруж}} P_{\text{стр}} P_{\text{инф}},$$

где вероятность раскрытия канала $P_{\text{разв}}$ определяется тремя составляющими: вероятностью обнаружения факта работы канала связи $P_{\text{обнаруж}}$, структуры сигнала $P_{\text{стр}}$ и содержания информационного сообщения $P_{\text{инф}}$.

Обнаружение сигнала (энергетическое) характеризуется радиусом обнаружения:

$$R_{обнаруж} = \frac{\lambda}{4\pi}\sqrt{\frac{W_{пер} K_{пер} K_{про}}{\eta_{про}\alpha_0 \gamma_2}}$$

где λ, $W_{\text{пер}}$, $K_{\text{пер}}$ – параметры сигнала системы связи: длина волны, мощность излучения, коэффициент направленного действия антенны, соответственно;

$K_{\text{про}}$, $\eta_{\text{про}}$, γ_2 – параметры системы перехвата сигнала: коэффициента направленности антенны для перехвата сигнала, чувствительность приемника, отношение сигнал/шум на входе приемника, соответственно;

α_0 – величина потерь на тракте между сетью связи и приемником-обнаружителем.

Скрытность сигнала (структурная) определяется:

$$S = \log_2 A,$$

где A – количество возможных комбинаций какого-либо параметра сигнала: несущая частота, амплитуда, вид модуляции, структура кода и др.

Если в системе связи используется составной сложный сигнал, то:

$$S = \sum_{k=1}^{l} S_k = \sum_{k=1}^{l} log_2 A_k ,$$

где A_k – параметры k–х составных элементов сложного сигнала.

Переходя к системе связи:

$$P_{\text{сист.св.}} \geq P_{\text{сист.св.зад.}}$$

то есть вероятность функционирования системы связи не должна быть меньше заданной.

Функционирование системы связи перестанет осуществляться, когда

отношение сигнал шум приемника $\gamma_{пр}$ станет меньше критического значения $\gamma_{крит}$:

$$q_{пр} = \gamma_2 \leq \gamma_{крит}$$

вероятность подавления канала помехами $P_{подавл}$ зависит от плотности вероятности распределения на входе приемного тракта приемника, которая зависит от характеристик помех и сигнала.

Тогда при равномерном усилении частот сигнала, помехозащищенность радиоканала:

$$(W_{пер} K_{пер}) \frac{K_{пр}}{K_{помех}} \frac{\alpha_0}{\alpha_{пер}} \frac{1}{K_з} \gamma_{крит} \geq (W_{пер\ пом}, K_{пер\ пом})$$

где $K_{пр}$ и $K_{помех}$ – характеристики приемной антенны системы связи: коэффициенты направленности антенны приемника к сигналу и генератору помех, соответственно;

$\alpha_{пер}$ – величина потерь в канале линии связи приемник-передатчик;

$K_з$ – коэффициент запаса по мощности;

$\gamma_{крит}$ – критическое значение сигнал/шум;

$W_{пер\ пом}$,$K_{пер\ пом}$ – характеристики передатчика помех: мощность и коэффициент направленности антенны, соответственно.

Из полученных соотношений можно сделать вывод: увеличение скрытности и помехозащищенности системы связи достигается увеличением базы сигнала, направленности антенн передатчика и приемника.

В работе модель структурной *устойчивости* сети, исходя из параметров: число узлов связи число узлов связи N, связность узлов m, средняя длина маршрута $L_{ср}$, число ребер (звеньев сети) R и др. (полный перечень приведен в главе 3 диссертации), которые сводятся в обобщенный показатель:

$$B = F\ (N, m, L_{ср}, R, \ldots),$$

и ввести коэффициент защиты элементов сети $A \in [0,1]$ то:

$$q(A) = \frac{\left(2 + B - \sqrt{B(B+4}\right)}{2A}$$

а структурная устойчивость определяется:

$$\gamma(K_П, v) = \frac{1 - q(A)}{1 - q(A) + B\left(1 + \frac{K_П(1 - q(A))}{B + v(1 - q(A))}\right)}$$

где $K_П$ – коэффициент отсутствия готовности системы связи, или коэффициент простоя, v – относительная интенсивность восстановления отказов.

Тогда запас структурной устойчивости, который необходимо поддерживать в пределах 0,2…0,3:

$$\Delta\gamma = \gamma(1 - P_{пор}),$$

где $P_{пор}$ – вероятность поражения системы связи, которая в наихудшем случае: $P_{пор} \to 0{,}5$.

С другой стороны:

Устойчивость представляем как вероятность своевременной доставки информации до приемника:

$$P_{СД} = P_{ПР}\, K_Г\, P_{СВ}|t_{дост} < t_{дост\ max}$$

где $P_{ПР}$ – вероятность правильной, безошибочной доставки информации;

$K_Г$ – коэффициент готовности системы связи;

$P_{СВ}$ – вероятность связности сети связи;

$t_{дост\ max}$ – ограничение сверху время доставки информации потребителю.

Первый множитель определяется системой обнаружения и исправления ошибок. В связи с тем, что в системах связи всегда используются: система коррекции ошибок, методы помехоустойчивого кодирования и т.д., то:

$P_{ПР} \to 1$

$P_{СВ}$ зависит от модели надежности системы связи, т.е. от ее графа.

При последовательном соединении рабочих элементов сети связи:

$$P_{СВ} = \prod_{i=1}^{m} P_{раб.эл._i},$$

а каждый рабочий элемент определяется показателями:

$$P_{раб.эл._i} = q_{ИТВ_i} q_{РЭП_i} q_{ФП_i} q_{ОТК\,i}$$

где $q_{ИТВ_i}$ –вероятность отказа элементов сети связи из-за воздействий информационно-технических; $q_{РЭП_i}$ – средств радио-электронного подавления узлов сети; $q_{ФП_i}$ – физического поражения узлов; $q_{ОТК_i}$ – внутренних и естественных процессов.

Аналогично, должно достигаться:

$$P_{СД} < P_{СД_{max}}.$$

В соответствии с ГОСТ 5311–2008 Устойчивость функционирования сети связи общего пользования: из-за вероятностного характера воздействия внешних дестабилизирующих факторов и их интенсивности на систему связи, а также неполноты учета показателей ее стойкости, показатели надежности и живучести носят вероятностный характер и могут только прогнозироваться.

К показателям надежности для данной диссертации относим следующие.

1. Вероятность связности сети – вероятность, что имеется хотя бы один канал для передачи информации по каналу связи, то есть:

$$P_{связности} = P\left(k_{раб.к.} \geq 1\right)$$

где $k_{раб.к}$ – количество работающих каналов для передачи информации.

При этом качество обслуживания Q должно быть: $Q \leq Q_{зад}$, то есть не хуже заданного или требуемого.

2. Коэффициент готовности канала связи:

$$K_{Г} = \frac{T_0}{T_0 + T_B}$$

где T_0 – среднее время наработки на отказ канала;

$T_в$ – среднее время восстановления работоспособности (ремонта).

Коэффициент готовности представим:

$$K_Г = F(T_{ДО}, T_{ОЖ}, T_{РЕК}, T_{ОТК}),$$

где $T_{ДО}$ – время, необходимое для диагностики отказа сети;

$T_{ОЖ}$ – ожидаемое время восстановления связи;

$T_{РЕК}$ – время реконфигурирования маршрутов в сети;

$T_{ОТК}$ – среднее время работы между отказами.

При допущении о пуассоновском потоке процессов отказа и восстановления, параметры $T_{ОЖ}$ и $T_{ОТК}$ экспоненциально распределяются во времени, и, тогда:

$$T_{ОЖ} = 1/\mu_{ОЖ} \text{ и } T_{ОТК}=1/\lambda_{ОТК}$$

где $\lambda_{ОТК}$ – интенсивность отказов соединения в сети;

$\mu_{ОЖ}$ – интенсивность восстановления связи.

Целевая функция, описанная для возможности оптимизации вариантов построения систем связи, с использованием теории полезности, как скалярная функция полезности примет вид:

$$Q(k_1,k_2,...,k_m)=\sum_{j=0}^{m} c_j f_j(k_j),$$

где c_j – шкалирующие коэффициенты; f_j (k_j) – скалярные функции полезности, характеризующие варианты сети по j-му показателю качества k_j;

$k_1, k_2, ..., k_m$ – совокупность показателей качества сети связи, причем:

$$\forall k_j \geq k_{j_{min}}, j=1,2, ..., m.$$

Проблема в том, что показатели k_j, противоречивы и связаны между собой, поэтому уровни $k_{j_{min}}$ зависят от значений остальных показателей качества:

$$k_{i_{min}} = f(k_j, ..., k_m), j=1,2,...,m, i \neq j.$$

Эта зависимость из-за неопределенности априорной информации относительно предпочтительности различных вариантов сети, содержит элементы нечетких множеств, поэтому множество показателей K представим как множество подчиненных оценок, ранжированных по значениям функции принадлежности:

$$K=\left\{\left(k_1,k_2, ..., k_m\right),\xi_{\bar{k}}\left(k_1,k_2, ..., k_m\right)\right\},$$

где функция принадлежности:

$$\xi_{\bar{k}}\left(k_1,k_2, ..., k_m\right)=\frac{1}{m}\left[\sum_{j=1}^{m}\left(\xi_{k_j}\left(k_j\right)\right)^{\beta}\right]^{1/\beta}$$

при β =0 форма функции становится линейной аддитивной, при β →∞ – нелинейной.

К отдельному показателю живучести отнесем коэффициент оперативной готовности:

$$K_{ОГ} = P_{сохр.раб.}(t)K_{Г}$$

где $P_{сохр.раб.}$ – вероятность сохранения работоспособности при действии внешних воздействующих факторов.

Для традиционных узлов с коммутацией каналов основной нормируемой составляющей надежности является готовность, требование к которому задается в виде: "не более 2 часов простоя за 20 лет службы", что соответствует значению коэффициента готовности "пять девяток", т.е. $K_Г > 0{,}99999$.

1.6. Выводы по первой главе

На основе вышеизложенного материала можно сделать следующие выводы.

1. Неоспоримыми преимуществами беспроводных протоколов связи являются простота развертывания, дешевизна оборудования и отсутствие проводки, а к недостаткам можно отнести: довольно высокий уровень потребления энергии, влияние помех и интерференция при работе в нелицензируемых диапазонах частот, возникающие сложности при защите передаваемых данных.

2. На развитие систем мобильной связи оказывает влияние поддержка производителями, поставляющих компоненты систем связи как для базового, так и для абонентского оборудования. Поэтому для открытых стандартов среди производителей наличествует более острая конкуренция, что приводит к более широкому распространению таких систем по сравнению с системами связи с закрытыми протоколами.

3. Для организации связи с наземными подвижными объектами наиболее подходящей является радиосвязь на основе открытых протоколов.

4. Рост сложности систем приводит к тому, что обеспечение устойчивого функционирования и восстановление работоспособности является трудоемкой задачей.

5. Система радиосвязи характеризуется множеством уязвимостей, которые требуют многостороннего анализа и проработки.

6. Для организации защищенной системы связи с учетом ее эволюции необходимо разработать процедуры выбора оптимального протокола, оценки устойчивости проектируемой системы радиосвязи.

7. Для повышения устойчивости сети используются меры:

− оптимизация топологии сети для упрощения ее адаптации к условиям, возникающим в результате воздействия различных дестабилизирующих факторов;

− рациональная маршрутизация между узлами сети – применение специальных мер защиты сети и ее элементов от влияния источников помех различного характера;

− развитие системы резервирования;

− внедрение автоматизированных систем управления, организующих работу по перестройке и восстановлению сети, поддержанию ее работоспособности в различных условиях и др.

ГЛАВА 2
АНАЛИТИЧЕСКИЙ ОБЗОР И ВЫБОР МЕТОДОВ ИССЛЕДОВАНИЯ УРОВНЯ УСТОЙЧИВОСТИ СИСТЕМ РАДИОСВЯЗИ

Методами для решения поставленных в работе задач могут являться:

- иерархические деревья решений;
- метод экспертных оценок;
- генетические алгоритмы;
- алгоритмы корреляционного анализа;
- искусственные нейронные сети и др.

Вкратце рассмотрим в данной главе наиболее подходящие методы, а также их достоинства и недостатки применительно к специфике решаемых задач.

2.1. Методы анализа оценок

Методы анализа оценок базируются на методах статистики [35-38], а также позволяют учитывать профессиональный, научный и практический опыт разработчиков. С помощью анализа оценок принимается решение о выборе конкретного варианта-победителя: технического устройства, технологии изготовления, претендента, проекта. Цель такого подхода при выборе решения – рассмотрение нескольких наборов оценок, из-за чего вероятность: правильного выбора из множества вариантов, прогнозирование развития процессов, поиск решения сложной задачи таким методом повышается. Необходимо отметить, что при использовании метода оценок:

- точность решения будет повышаться с помощью метода искусственных нейронных сетей;
- количество наборов оценок обычно составляет 5…12 штук;
- оценки имеют качественный тип;
- если оценка количественная, то для нее рекомендуется использовать не более пяти градаций;

− оценки могут быть грубыми, без уточнения деталей и подходов.

Методы формирования оценок можно разделить на две группы [39]. Методы множественных оценок заключается в непосредственном формировании массива значений разработчиками системы связи. Недостатками такой процедуры является сложность алгоритма получения информации, формирования мнения разработчиков, возможность "давления" отдельных оценок на принятие определенных решений. К таким методам относятся: мозговая атака, сценариев, деловых игр, совещаний и суда [40-43].

Методы получения мнений отдельных разработчиков заключаются в сборе оценок независимо друг от друга, а затем в их статистической обработке. К ним относятся методы опроса, метод Дельфи, интервью. Достоинствами методов являются: оперативность, использование опыта отдельного разработчика, высокая "помехоустойчивость" мнений, низких затрат на оценивание. Недостатком является высокая степень субъективизма. После индивидуального формирования оценок, в результате проведения 3…4 итераций, множество вариантов сужается.

После формирования оценок производится их обработка, для чего используется аппарат методов математической статистики. Окончательное решение принимается с помощью методов: предпочтения (ранжировки), задания весовых коэффициентов, парных сравнений и последовательных сравнений для которых разработано множество модификаций. Вкратце механизм обработки результатов опроса следующий [44-47].

1. Формирование обобщенной оценки: при числе наборов оценок k, состоящих из оценок x_i, (i=1 ,…, k) используется среднее арифметическое:

$$x_{\text{ср}} = \frac{\sum_{\text{i=1}}^{\text{k}} x_i}{k}, \qquad (2.1)$$

представляющее собой точечную оценку математического ожидания для множества наборов, или медианное значение M_k, находящееся посередине относительно числа больших и меньших оценок.

2. Определение относительных весов факторов объектов, которые показывают насколько тот или иной фактор важен с точки зрения критерия. Для *n* сравниваемых критериев вес *j*-го фактора w_j определяется как:

$$w_j = \frac{\sum_{i=1}^{k} w_{ji}}{k} \qquad (2.2)$$

где w_{ji} – вес *j*-го фактора, определенный по оценкам из *i*-го набора, который находится как:

$$w_{ji} = \frac{x_{ji}}{\sum_{j=1}^{n} x_{ji}}, \quad i = 1,...,k, \quad j = 1,...,n. \qquad (2.3)$$

3. Определение степени согласованности оценок, сформированных разработчиками, необходимо из-за того, что в оценках всегда имеет место расхождение [44]. Уверенность результирующего решения растет с уменьшением расхождения (с увеличением согласованности). Анализ разброса также определялся методами статистического анализа. По результатам опроса определяется вариационный размах:

$$R = x_{\max} - x_{\min}, \qquad (2.4)$$

то есть разница между максимальной и минимальной оценками. Среднее квадратическое отклонение (СКО):

$$\sigma = \sqrt{\frac{\sum_{i=1}^{k} \left(x_i - x_{\text{ср}}\right)^2}{k-1}}, \qquad (2.5)$$

коэффициент вариации:

$$\upsilon = \frac{\sigma}{x_{\text{ср}}} \cdot 100\% . \qquad (2.6)$$

Видно, что при $x_i \to x_{\text{ср}}$ в соотношении (2.5) коэффициент вариации υ стремится к 100%, но сделать точный вывод по полученному значению υ на

практике затруднительно, т.к. образуются диапазоны значений коэффициента вариации с нечеткими границами зон определенности.

Проверка согласованности сформированных оценок может определяться также *методом ранжирования*. В этом случае для *i*-го набора оценок строится упорядоченная последовательность:

$$x_{1i}, x_{2i}, \ldots, x_{ni}. \qquad (2.7)$$

Согласованность между ранжированными рядами двух наборов оценок определяется с помощью критерия ранговой корреляции Спирмэна (ρ), рассчитываемого по формуле:

$$\rho = 1 - \frac{6\sum_{j=1}^{n} d_j^2}{n(n^2-1)}, \qquad (2.8)$$

где d_j – междуранговая разница, определяемая как:

$$d_j = x_{ji} - x_{js}, i \neq s \ , \qquad (2.9)$$

где x_{ji} – ранг, присвоенный *j*-му фактору по оценкам из *i*-го набора,

x_{js} – ранг, присвоенный *j*-му фактору *s*-го набора оценок.

Критерий Спирмэна, определяемый по формуле (2.8) изменяется в диапазоне от –1 до 1. Коэффициент ρ стремится к 1 при увеличении согласованности принятых решений *i*-го и *s*-го набора. При рассогласованности в наборах сформированных оценок значение критерия ρ стремиться к –1, достигая ее при наибольшем расхождении.

Достоинством метода ранжирования является возможность его использования при оценке взаимоотношений меду фактором и результативным признаком или реакцией, когда признаки не могут быть определены точно, но могут быть построены из них упорядоченные ряды. Тогда коэффициент ρ может использоваться аналогично коэффициенту парной корреляции, причем положительное значение будет свидетельствовать о прямой зависимости между факторами, а отрицательное – об обратно пропорциональной. При этом, чем

ближе коэффициент, взятый по модулю, к единице, тем теснее связь между факторами.

Если число наборов оценок в методе с использованием ранжирования больше двух, то рассчитывается коэффициент конкордации (*W*) – общий коэффициент ранговой корреляции для группы из *k* наборов оценок. Дисперсионный коэффициент конкордации выражается как отношение оценки дисперсии *D* к максимальному значению этой оценки $D_{\max}$:

$$W = \frac{D}{D_{\max}} \tag{2.10}$$

и, учитывая взаимосвязь дисперсии и СКО (2.5), а также, что

$$D_{\max} = \frac{k^2(n^3 - n)}{12(n-1)}\ , \tag{2.11}$$

получим:

$$W = \frac{12S}{k^2(n^3 - n)}, \text{ где} \tag{2.12}$$

$$S = \sum_{j=1}^{n} \left(\sum_{i=1}^{k} x_{ji} - x_{cp} \right)^2 . \tag{2.13}$$

Соотношение (2.12) вместе с (2.13) позволяет определить *W* в случае отсутствия связанных рангов (повторных оценок в одном наборе данных для разных факторов или объектов). В противном случае значение знаменателя в (2.10) становится меньше, а соотношение (2.12) примет вид:

$$W = \frac{12S}{k^2(n^3 - n) - k\sum_{i=1}^{k} H_i}, \text{ где} \tag{2.14}$$

$$H_i = \sum_{p=1}^{Z_i} (h_p^3 - h_p), \tag{2.15}$$

где H_i – показатель связанных рангов для *i*-й ранжировки;

Z_i – число групп равных рангов в *i*-й ранжировки;

h_p – число равных рангов в p-й группе связанных рангов при ранжировке в i-м наборе данных.

При отсутствии повторяющихся рангов в наборах оценок $H_i = 0$, так как $Z_i = 0$ и $h_p = 0$ и при этом (2.14) совпадает с (2.12).

Коэффициент конкордации W изменяется в диапазоне [0,1]. Его максимум означает, что все наборы оценок согласованы по рангам, а минимум – что оценки рассогласованы. Надо отметить, второй результат может означать, что в наборах данных происходит образование страт с противоположными вариантами решения поставленной задачи.

При числе факторов $n > 7$ в качестве распределения для коэффициента W может быть принято χ^2 – распределение с $r = n - 1$ степенями свободы. При наличии связанных рангов χ^2 – распределение имеет вид:

$$\chi^2 = \frac{12S}{kn(n+1) - \frac{1}{n-1}\sum_{i=1}^{k} H_i} = \frac{12S(n-1)}{k(n^3 - n) - \sum_{i=1}^{k} H_i} \quad . \qquad (2.16)$$

Рассчитанное по соотношению (2.16) значение сравнивается с табличным, найденное для заданных уровня значимости и числа степеней свободы. Если табличное значение не будет превышать рассчитанное, то гипотеза о согласованности наборов оценок окажется верной.

Достоинствами метода ранжирования являются простота процедуры формирования оценок и наименьшее число необходимых для принятия решения наборов данных. Недостатками является допущение метода о равномерных распределениях оценок и важностей признаков, что на практике не происходит.

Альтернативой ранжирования является *метод задания весовых коэффициентов*, которые могут быть определены несколькими способами. Например, всем факторам назначаются веса таким образом, чтобы их сумма была равна какому-то фиксированному числу. Чаще всего это единица, или кратные десяти числа: 10 или 100. Другим способом расстановки весовых коэффициентов может быть присвоение наиболее важному фактору максимальной оценки, а

остальным – доли от этого числа. Далее рассуждения ведутся так же, как описано выше с использованием соотношений (2.8) – (2.13) [46].

Метод *последовательных сравнений* состоит в следующем. В каждом наборе данных производится упорядочивание факторов в порядке уменьшения их веса (значимости) (2.7) при $w_1 > w_2 > \ldots > w_n$, причем первому фактору присваивается максимальный вес, равный единице, а остальным – доли от единицы. Относительно первого фактора оцениваются варианты. При этом имеет место один из вариантов сравнения:

$$\begin{aligned} &w_1 > w_2 + w_3 + \ldots + w_n, \text{ или} \\ &w_1 = w_2 + w_3 + \ldots + w_n, \text{ или} \\ &w_1 < w_2 + w_3 + \ldots + w_n, \end{aligned} \qquad (2.17)$$

по которому производится оценка (a_{1n}) выбранного варианта. Далее составляется следующий набор вариантов, исключая последний весовой коэффициент, из которого выбирается один,:

$$\begin{aligned} &w_1 > w_2 + w_3 + \ldots + w_{n-1}, \text{ или} \\ &w_1 = w_2 + w_3 + \ldots + w_{n-1}, \text{ или} \\ &w_1 < w_2 + w_3 + \ldots + w_{n-1}, \end{aligned} \qquad (2.18)$$

который снова оценивается (a_{1n-1}). Так повторяется до процедуры сравнения вида:

$$\begin{aligned} &w_1 > w_2 + w_3, \text{ или} \\ &w_1 = w_2 + w_3, \text{ или} \\ &w_1 < w_2 + w_3. \end{aligned} \qquad (2.19)$$

Затем процесс выбора возобновляется, но с заменой коэффициента w_1 на w_2. по выражениям, аналогичным (2.17)–(2.19).

Преимуществом метода является самоанализ, который возможен на стадии формирования оценок. Недостатком является сложность (требуется специальная подготовка) и большая трудоемкость (в 4 раза по сравнению с методом ранжирования).

В методе *парных сравнений* все веса факторов сравниваются между собой попарно. Затем вычисляются оценки каждого фактора. Для удобства сравнения составляется таблица (см. табл. 2.1), в которой по горизонтали и вертикали

отложены факторы сравнения (*A*, *B*, *C*,…, *N*). По диагонали таблицы проставляются единицы (результат сравнения фактора с самим собой). Заполнение таблицы осуществляется построчно, но чтобы облегчить задачу разработчику при формировании оценок, половина таблицы (под или над диагональю) не заполняется в силу ее симметричности. Тогда оценки отдельного набора будут представлять собой матрицу:

$$\begin{matrix} a_{11}\ a_{12}\ a_{13}\ \ldots\ a_{1n} \\ a_{22}\ a_{23}\ \ldots\ a_{2n}\ . \\ a_{33}\ \ldots\ a_{3n} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ a_{nn} \end{matrix} \qquad (2.20)$$

Таблица 2.1 Форма для попарного сравнения факторов

	A	*B*	*C*	...	*N*
A	1	*A:B*	*A:C*	...	A:N
B	*B:A*	1	B:C	...	B:N
C	*C:A*	*C:B*	1	...	C:N
...	...	...	...	1	...
N	*N:A*	*N:B*	*N:C*	...	1

Суммируя оценки a_{11} по каждому *i*-му набору оценок, получим суммарные оценки *b*:

$$b_{11} = \sum_{i=1}^{k} a_{11}^{(i)}\ ,\ \ldots \qquad (2.21)$$

Из суммарных оценок составляется матрица, аналогичная по структуре матрице (2.20):

$$\begin{matrix} b_{11}\ b_{12}\ b_{13}\ \ldots\ b_{1n} \\ b_{22}\ b_{23}\ \ldots\ b_{2n}\ . \\ b_{33}\ \ldots\ b_{3n} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ b_{nn} \end{matrix} \qquad (2.22)$$

Определяя значение дисперсии суммарной матрицы (2.22) и максимальной из дисперсий по матрицам (2.20), определяется согласованность оценок. Чем ближе значения дисперсий, тем выше согласованность.

Метод парных сравнений по трудоемкости сложнее метода ранжирования, но проще метода последовательных сравнений. Необходимое количество наборов оценок в 2 раза больше, чем в методе ранжирования, но в 2 раза меньше, чем в методе последовательных сравнений.

Из вышеизложенного можно сделать вывод, что метод анализа оценок хорош при отсутствии возможности применить более точные методы.

2.2. Искусственные нейронные сети

2.2.1. Компоненты нейронных сетей

ИНС используются для решения определенных задач: классификации, распознавания и прогнозирования. Такой математический аппарат также выгодно применять для процедуры построения нелинейной регрессионной функции: $Y=F(X)$, когда получение в аналитическом виде F является нетривиальной задачей [47-51]. Конечно, известным фактом является возможность построения многочлена большого порядка для любого конечного набора данных $\{X,Y\}$, например, с помощью аппроксимирующего полинома вида:

$$y(x) = b_0 + \sum_{i=1}^{n} b_i x_i + \sum_{i \neq j} b_{ij} x_i x_j + \sum_{i=1}^{k} b_i x_i^2 + \ldots,$$

или многочленов Чебышева:

$$y_n(x) = \frac{1}{2}\left[\left(x + \sqrt{1-x^2}\right)^n + \left(x - \sqrt{1-x^2}\right)^n\right],\ -1 \le x \le 1\ , n = 0,1\ldots,$$

и итоговая модель будет достаточно точно повторять изменения от i-го к i+1 - му значениям, но между этими состояниями устойчивость модели не гарантировано.

Искусственная нейронная сеть (ИНС) – устройство обработки информации, состоящее из множества элементов Q – нейронов и множества связей S – синапсов: $INS=\{Q, S\}$. Нейроны имеют строение, аналогичное их биологическому аналогу [52, 53] . Каждый i-й нейрон по сути своей является вычислительным элементом (см. Рисунок 2.1), преобразующим поступающие в него сигналы x_j в выходной сигнал (OUT) в зависимости от синаптического веса w_j:

$$OUT_i = \sum_{j=1}^{m} w_j x_j, \ \ i = 1,...,n,$$

где m – количество входов нейрона, а с помощью преобразующей (сжимающей) функции φ_i формируется выходной сигнал y_i:

$$y_i = \varphi_i(OUT_i).$$

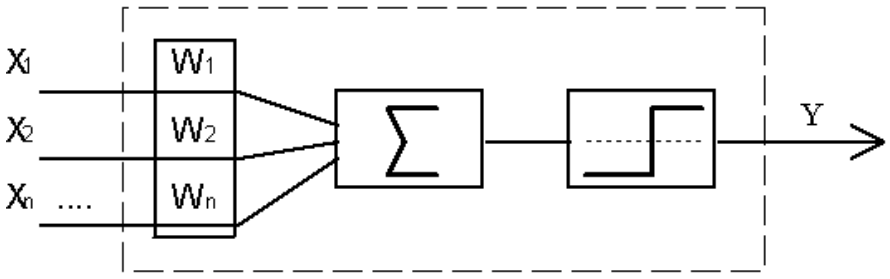


Рисунок 2.1 Схема нейрона по теории Маккалока и Пирса

В общем случае в качестве сжимающей используется функция произвольного вида, а на практике применяются: пороговая, сигмоидальная и гиперболический тангенс. Сигмоидальная функция обладает избирательной чувствительностью к сигналам разного уровня, достигающей максимума вблизи порога срабатывания Θ, где малые изменения входного сигнала OUT приводят к значительным изменениям выходного сигнала Y:

$$Y = f(OUT) = \frac{1}{1+\exp(\Theta - OUT)}. \qquad (2.23)$$

Наоборот, на границах чувствительности (выше/ниже порога срабатывания Θ), сигмоид (2.23) становится нечувствительным к изменению сигнала OUT.

Докажем это положение.

Сигнал на выходе j-го нейрона:

$$y_j(N) = \varphi_j(v_j(N)), \tag{2.24}$$

где N – итерация обучения, $v_j(N)$ – значение, получаемое на входе функции активации:

$$v_j(N) = \sum_{i=0}^{m} w_{ji}(N) y_i(N),$$

где w_{ji} – синаптический вес j-го нейрона i-го слоя.

Дифференцируя (2.24) по $\varepsilon_j(N)$, $y_j(N)$, $v_j(N)$, $w_{ji}(N)$ и, подставляя результаты в соотношение для сигнала ошибки:

$$E(N) = \frac{1}{2}\sum_{j \in C} \varepsilon_j^2(N),$$

получим:

$$\frac{\partial E}{\partial w_{ji}} = -\varepsilon_j(N)\varphi_j'(v_j(N))y_j(N).$$

Величину коррекции весов выразим:

$$\Delta w_{ji}(N) = -k\frac{\partial E(N)}{\partial w_{ji}(N)},$$

где k – параметр скорости обучения.

Градиент можно представить в виде:

$$\frac{\partial E}{\partial w_{ji}} = \frac{\partial E}{\partial \varepsilon_j}\frac{\partial \varepsilon_j}{\partial y_j}\frac{\partial y_j}{\partial v_j}\frac{\partial v_j}{\partial w_{ji}},$$

а локальный градиент для случая, если j-й нейрон находится в выходном слое:

$$\delta_j(N) = \frac{\partial E}{\partial v_j(N)} = -\frac{\partial E(N)}{\partial \varepsilon_j(N)}\frac{\partial \varepsilon_j(N)}{\partial y_j(N)}\frac{\partial y_j(N)}{\partial v_j(N)}\frac{\partial v_j(N)}{\partial w_{ji}(N)} =$$

$$= \varepsilon_j(N)\varphi_j'(v_j(N)),$$

а для для нейрона в скрытом слое:

$$\delta_j(N) = -\frac{\partial E(N)}{\partial y_j(N)}\frac{\partial y_j(N)}{\partial v_j(N)} = -\frac{\partial E(N)}{\partial y_j(N)}\varphi_j'(v_j(N))$$

или:

$$\delta_j(N) = \varphi'_j(v_j(N)) \sum \delta_k(N) w_{ki}(N).$$

Функция $\varphi'_j(v_j(N))$ зависит от функции активации, а сумма определяет значения ошибок нейронов, правее нейрона *j*, и значения синаптических весов связей.

Для сигмоидальной активационной функции:

$$\varphi_j(v_j(N)) = \frac{1}{1 + exp(-av_j(N))},$$

отсюда:

$$\varphi'_j(v_j(N)) = \frac{a\, exp(-av_j(N))}{\left(1 + exp(-av_j(N))\right)^2},$$

или через $y_j(N)$ по (2.24), избавляясь от экспоненты, получим:

$$\varphi'_j(v_j(N)) = ay_j(N)(1 - y_j(N)). \qquad (2.25)$$

Тогда для скрытого нейрона:

$$\delta_j(N) = \varphi'_j(v_j(N)) \sum \delta_k(N) w_{ki}(N) =$$

$$= ay_j(N)(1 - y_j(N)) \sum \delta_k(N) w_{ki}(N) \cdot$$

Так как в (2.25):

$$\Delta w_{ji}(N) \sim \varphi'_j(v_j(N)),$$

и

$$max\, \Delta w_{ji}(N) \to y_i(N) = 0{,}5,$$

то, следовательно, это свойство сигмоидальной функции в алгоритме обратного распространения ошибки вносит наибольший вклад в его устойчивость при обучении ИНС.

Множество *E* можно разделить на группы, содержащие нейроны со схожим назначением, или вертикальные слои. Различают входной, выходной и внутренние или скрытые слои. Определение числа слоев и количества нейронов в каждом слое, а также связей между ними, то есть структуры ИНС – достаточно сложная математическая задача. Наиболее часто ее решают, применяя многослойный персептрон Розенблатта (F.Rosenblatt), или полносвязную сеть (см. Рисунок 2.2). В такой структуре каждый входной нейрон соединен с нейроном внутренних слоев, которые в свою очередь соединены с элементами выходного слоя аналогичным образом. С ростом числа внутренних слоев ИНС прямо пропорционально растет сложность работы с ней, но, в то же время, увеличивается "гибкость", а с ней и точность результатов вычислений. Число внутренних слоев редко выбирается больше двух. В некоторых источниках даются следующие рекомендации [54, 55].

1. Число нейронов скрытого слоя определяется эмпирическим путем, но в большинстве случаев используется правило:

$$N_{\text{СКР}} \le N_{\text{ВХ}} + N_{\text{ВЫХ}},$$

где: $N_{\text{СКР}}$, $N_{\text{ВХ}}$, $N_{\text{ВЫХ}}$ – число нейронов соответственно в скрытом, входном и выходном слое.

2. Увеличение числа нейронов во входном и выходном слоях ведет к необходимости увеличения числа нейронов в скрытых слоях.

3. Для ИНС, моделирующей многоэтапные процессы, необходим дополнительный скрытый слой, но с другой стороны добавление скрытых слоев может привести к перезапоминанию и к неверному решению на выходе сети.

4. С другой стороны, чем больше нейронов, тем большее количество связей образуется в ИНС, тем больше вероятность того, что сеть обучится при более сложных задачах.

Поэтому количество слоев и число нейронов в скрытых слоях выбирается исследователем, исходя из его личного опыта или экспериментально.

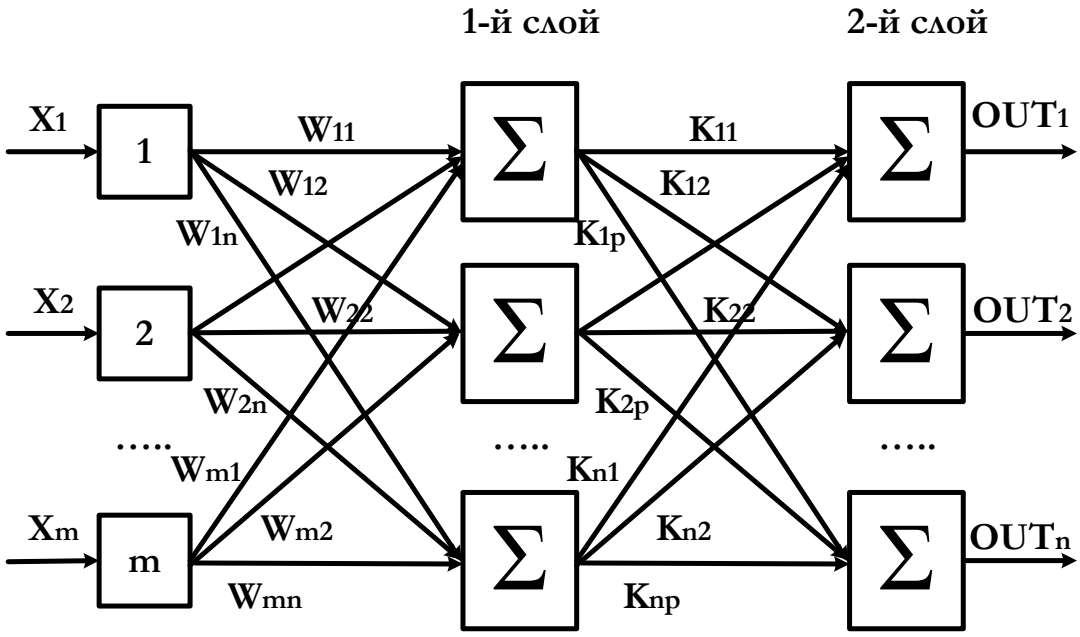


Рисунок 2.2. Структура персептрона (w_{mn} и k_{np} – веса)

Второй задачей, также требующей внимания, является обучение ИНС с заданной структурой, то есть подбор весов. Процедуры обучения ИНС делятся на два типа: с учителем и без него [56-58]. Обучение с учителем возможно, когда имеется обучающий набор данных, или обучающая выборка, вход-выход в достаточном объеме. Такой метод обучения получил наибольшее распространение из-за лучшего приближения результатов работы ИНС, а также простоты метода. Для использования метода обучения с учителем используется метод обратного распространения ошибки (error back propagation) (см. Рисунок 2.3). Он позволяет настроить веса нейронов в том числе и находящихся в скрытых слоях ИНС. Основная сложность этапа состоит в том, что все веса оказываются зависимыми друг от друга, и чем сильнее синаптическая связь нейрона в скрытом слое с последующим нейроном, например в выходном слое, тем больше ошибка первого влияет на ошибку второго. Поэтому необходимо отыскать взвешенное решение, а не локальное. При обучении информационные потоки направлены от входа к выходу, а оценки ошибок, делаемых сетью – в обратном направлении.

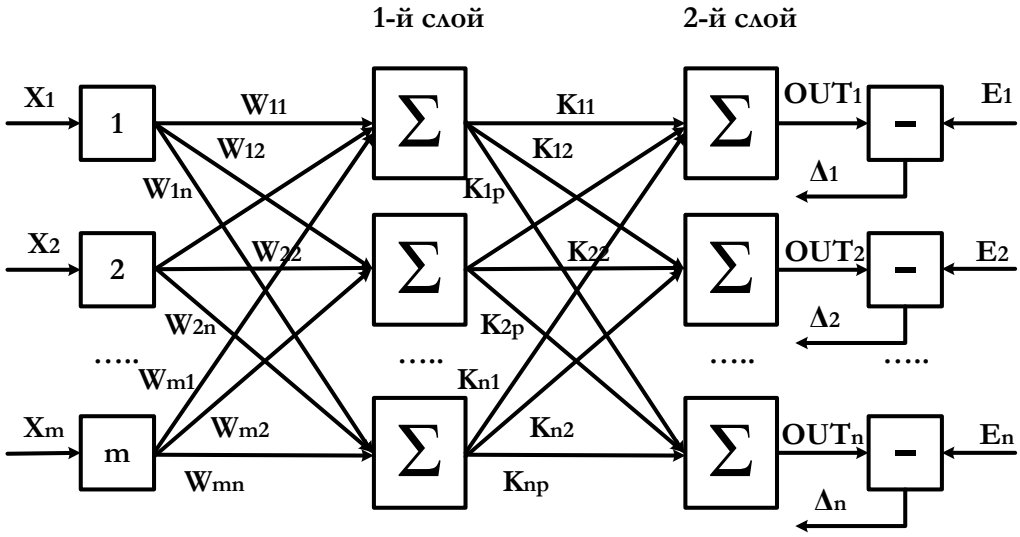


Рисунок 2.3 Принцип обучения сети методом обратного распространения ошибки.

Необходимое и достаточное условие конца обучения ИНС – получение минимальной ошибки (рассогласования):

$$\varepsilon_{\text{опт}} = \min\left[\frac{1}{2N_S}\sum_{i=1}^{N_S}\left(OUT_i - E_i\right)^2\right]. \qquad (2.24)$$

где: N_s – количество обучающих пар;

OUT_i – полученное с помощью сети значение выходного нейрона при i-м наборе обучения;

E_i – требуемое значение выходного нейрона при i-м наборе обучения.

Полная ошибка сети из (2.24):

$$\varepsilon = \varepsilon\left(\mathbf{W}, \mathbf{K}, \mathbf{L}_t \ldots\right) = \frac{1}{2N_S}\sum_{i=1}^{N_S}\Delta_i^2, \qquad (2.25)$$

где **W**, **K**, $\mathbf{L}_t$… – множества весов входного, выходного и скрытых слоев (t – количество скрытых слоев) соответственно, а функция (2.25) является неотрицательной функцией, определенной на множестве весов, и имеющей глобальный экстремум/экстремумы в точке ε = 0 (в этом случае сеть не допускает ошибок) [59-63]. Таким образом, задача обучения сети – это задача отыскания экстремумов-минимумов функции ошибки (2.25) в многомерном пространстве состояний с размерностью: $N_{\text{ВХ}}$ x $N_{\text{СКР}_1}$ x $N_{\text{СКР}_2}$ x … x $N_{\text{ВЫХ}}$. Для ее решения могут использоваться методы многофакторной оптимизации:

- метод наискорейшего (градиентного) спуска;
- метод параллельных касательных;
- сопряженных градиентов;
- BFGS;
- DFP и др.

2.2.2. Анализ методов оптимизации функции ошибки при обучении ИНС

Метод *наискорейшего спуска* относится к градиентным методам и используется, не смотря на свои недостатки, в большинстве случаев при настройке весов ИНС [61]. Если функция ошибки дифференцируема на множестве весов, то нахождение локального экстремума (минимума) происходит следующим образом (см. Рисунок 2.4).

1. Определяется начальная точка $\mathbf{X}^{(0)}$, координаты которой определяются либо пользователем, либо генерируется случайным образом.

2. Последующие точки последовательности вычисляются на i-й итерации для m-й компоненты по соотношению:

$$x_m^{(i+1)} = x_m^{(i)} - k_m^{(i)} \frac{d\varepsilon}{dx_m}, \qquad (2.26)$$

с проверкой выполнения условия:

$$\varepsilon(\mathbf{X}^{(i+1)}) < \varepsilon(\mathbf{X}^{(i)}), \ \ i = 1,2,\ldots , \qquad (2.27)$$

где $k_m^{(i)}$ – величина шага, задаваемая пользователем, которая неизменна, пока функция ошибки убывает (то есть при выполнении (2.27)).

Градиент функции ε показывает направление наибольшего изменения функции.

3. При нарушении условия (2.27) в точке, где перестает уменьшаться целевая функция ошибки, снова вычисляется градиент, и направление спуска изменяется.

4. Далее процесс повторяется до двухкратного выполнения системы неравенств:

$$\begin{cases} \left| x_m^{(i+1)} - x_m^{(i)} \right| < e \\ \left| \varepsilon(\mathbf{X}^{(i+1)}) - \varepsilon(\mathbf{X}^{(i)}) \right| < e \end{cases}, \qquad (2.28)$$

где e – точность, задаваемая пользователем.

Каждое новое направление движения к точке экстремума ортогонально предыдущему.

Недостатками метода наискорейшего спуска являются: возможность отыскания локального экстремума, хотя на практике исследователей всегда интересует глобальный, или близкое к нему значение функции, а также то, что способ ортогонального изменения направления движения не является наилучшей стратегией.

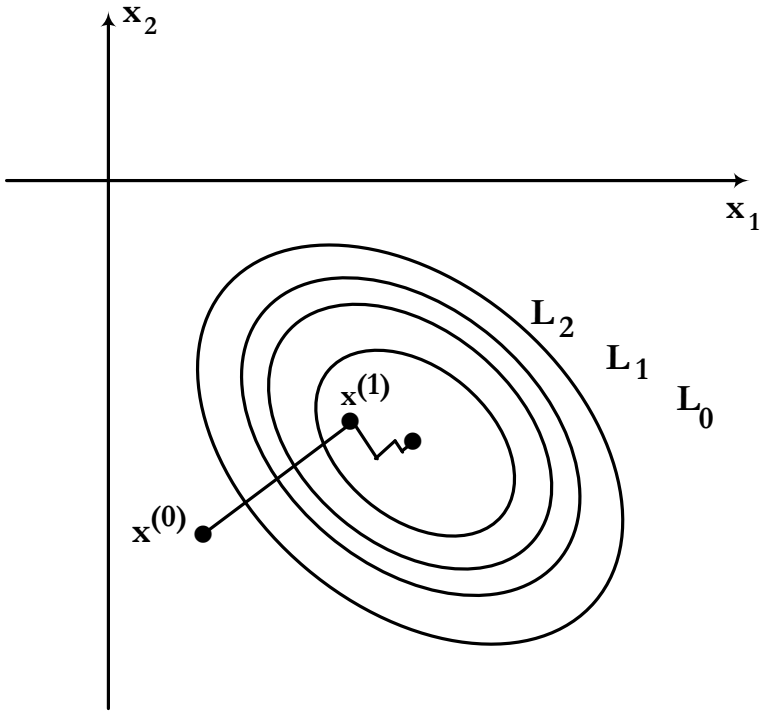


Рисунок 2.4. Геометрическая интерпретация нахождения минимума методом наискорейшего спуска

Метод параллельных касательных. Геометрическое пояснение работы метода изображено на рисунке 2.5. Если $x^{(0)}$ – точка на линии равного уровня –

эллипсе L_0, то через пересечение эллипса с касательной k_0 проходит вектор градиента g_1. Вектор градиента нормален к линии L_0 и касательной k_0. Точка $x^{(1)}$ является минимумом функции на прямой $x^{(0)}x^{(1)}$. В точке $x^{(1)}$ прямая касается линии L_1. Вектор градиента g_2 перпендикулярен прямой $x^{(0)}x^{(1)}$. Следовательно, прямая k_0 параллельна прямой k_1. В направлении вектора градиента g_2, находится точка $x^{(2)}$ как минимум функции, через которую проходит линия L_2. В итоге точка $x^{(0)}$ переместилась в точку $x^{(2)}$. Соединив точки $x^{(0)}$ и $x^{(2)}$, получим прямую, проходящую через начальную точку $x^{(0)}$ и центр эллипсов. В методе параллельных касательных также необходимо использование одного из методов одномерного поиска. Алгоритм метода должен закончиться через N итераций. Сходимость этого метода значительно лучше, чем у метода наискорейшего спуска.

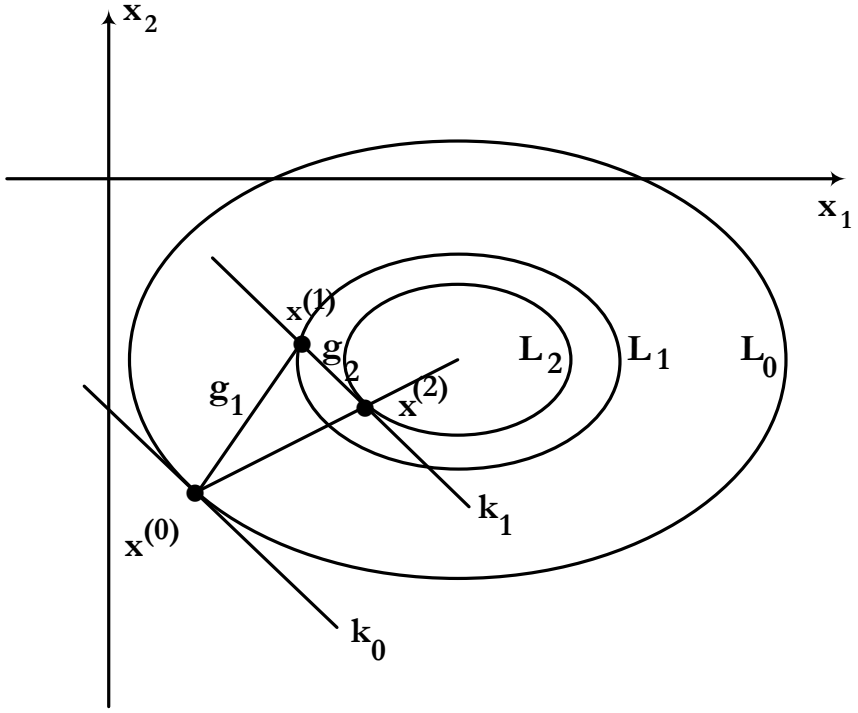


Рисунок 2.5. Геометрическая интерпретация нахождения минимума методом параллельных касательных

Метод сопряженных градиентов – метод отыскания безусловного экстремума, который сочетает исследование поведения первой производной и сопряженных направлений. Работу метода поясняет рисунок 2.6. Свойство сопряженности является обобщением понятия ортогональности и заключается в

выполнении условия равенства нулю скалярного произведения матриц x и Ay:

$$x^T Ay=0. \qquad (2.29)$$

Если в (2.29) матрица A – единичная, то оно выполняется.

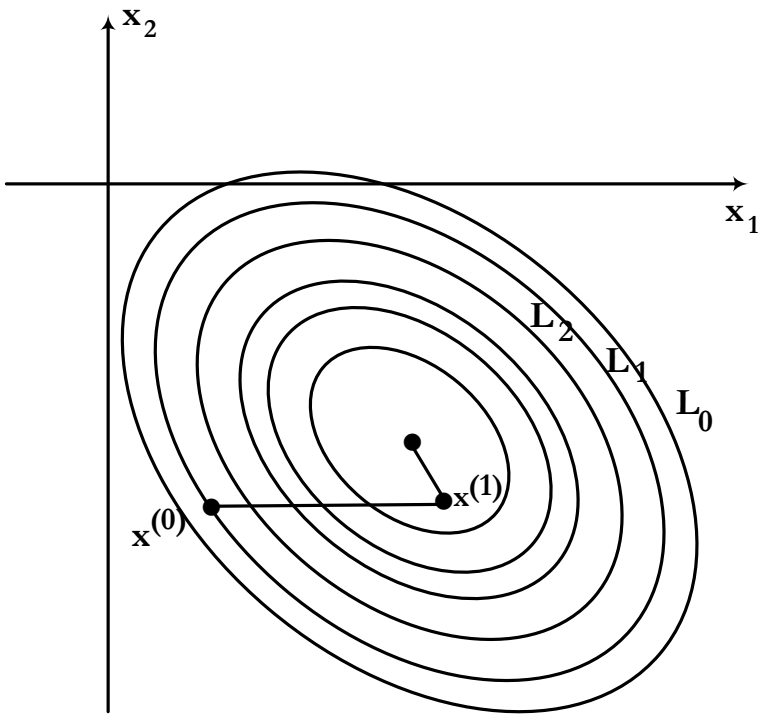


Рисунок 2.6. Геометрическая интерпретация нахождения минимума методом сопряженных градиентов

Вычисление сопряженных направлений *методом Грамма-Шмидта* для обучения ИНС затруднено из-за того, что элементы матрицы *A* неизвестны. Поэтому для ИНС можно использовать итеративные алгоритмы, например, на основе соотношения Флетчера-Ривса:

$$d^{(i+1)} = r^{(i+1)} + \beta^{(i+1)} d^{(i)} ,$$

(2.30)

$$\beta^{(i+1)} = \frac{r^{(i+1)T}}{r^{(i+1)T}} \frac{r^{(i+1)}}{r^{(i)}} ,$$

то есть сопряженное направление – результат сложения значения градиента, взятого с противоположным знаком, и предыдущего направления, умноженного

на коэффициент β. Для квадратичной функции метод сопряженных градиентов в лучшем случае находит искомый минимум за число шагов, равного размерности задачи (*N*). Для целевых функций произвольной формы число шагов заранее определить не возможно. При этом необходимо возобновлять процедуру через каждые *N* + 1 шагов, как предлагают Флетчер и Ривс.

В соотношении (2.30) определение сопряженных направлений может осуществляться *методом Полака-Райбера*:

$$\beta^{(i+1)} = \frac{r^{(i+1)T}\left(r^{(i+1)} - r^{(i)}\right)}{r^{(i)T} r^{(i)}} \quad . \qquad (2.31)$$

Работа методов определения сопряженных направлений зависит от выбора начальной точки. Если она близко расположена к минимуму, то метод Флетчера-Ривса сходится, в отличие от метода Полака-Райбера, который может зацикливаться, но зато имеет лучшую сходимость. Выбор вида:

$\beta = \max\{\beta, 0\}$,

что эквивалентно перезапуску процесса поиска с предыдущей точки изменения направления (по условию $\beta \le 0$), направит поиск в направлении наискорейшего спуска.

В алгоритме сопряженных градиентов осуществляется одномерная минимизация функций. Для этого можно воспользоваться методом чисел Фибоначчи, золотого сечения, или дихотомии. Метод золотого сечения – предпочтительнее, так как обладает такой же сходимостью, как и метод чисел Фибоначчи, но проще его по вычислениям. Метод дихотомии прост, но обладает сходимостью в 1,6 раза меньше, чем предыдущие два.

Конечно, еще большую сходимость обеспечивают методы второго порядка, например, *метод Ньютона* и *Ньютона-Рафсона*, осуществляющие поиск по формуле:

$$x_m^{(i+1)} = x_m^{(i)} + k_m^{(i)},$$

где шаг $k_m^{(i)}$ вычисляется как

$$k_m^{(i)} = -G(x_m^{(i)})^{-1} \frac{d\varepsilon}{dx_m}, \qquad (2.32)$$

где $G(\ldots)$ – определитель матрицы Гёссе:

$$G(X) = \begin{bmatrix} \frac{\partial^2 \varepsilon}{\partial x_1 \partial x_1} & \frac{\partial^2 \varepsilon}{\partial x_1 \partial x_2} & \ldots\ldots & \frac{\partial^2 \varepsilon}{\partial x_1 \partial x_n} \\ \frac{\partial^2 \varepsilon}{\partial x_2 \partial x_1} & \frac{\partial^2 \varepsilon}{\partial x_2 \partial x_2} & \ldots\ldots & \frac{\partial^2 \varepsilon}{\partial x_2 \partial x_n} \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ \frac{\partial^2 \varepsilon}{\partial x_n \partial x_1} & \frac{\partial^2 \varepsilon}{\partial x_n \partial x_2} & \ldots\ldots & \frac{\partial^2 \varepsilon}{\partial x_n \partial x_n} \end{bmatrix}. \qquad (2.33)$$

К ним же, с небольшой модификацией относится *демпфированный метод Ньютона*. Причем методы второго порядка могут носить как вспомогательный характер (например, в методе сопряженных градиентов), так и использоваться как самостоятельные. В случае использования метода Ньютона или его модификаций, метод сопряженных градиентов становится не первого, а второго порядка. В этом случае сложность алгоритма возрастает в основном из-за трудоемкой процедуры вычисления матрицы Гёссе.

Основным достоинством Ньютоновых методов является очень быстрая сходимость (быстрее, чем у методов, основанных на первых производных), достигающая квадратической.

Чтобы исключить недостаток метода Ньютона и его модификаций, разработан целый класс алгоритмов многопараметрической глобальной оптимизации, называемых квазиньютоновыми [61, 62]. Квазиньютоновы алгоритмы не требуют вычисления вторых производных, а в качестве матрицы Гёссе используют ее приближенную оценку с использованием рекуррентного соотношения:

$$G^{(i+1)} = G^{(i)} + \Delta G^{(i)}. \qquad (2.34)$$

Аналогично (2.34) строится приближение (аппроксимация) и обратной матрицы Гёссе.

Одним из эффективных алгоритмов этой группы является *BFGS*, названный так в честь разработчиков: Бройдена, Флетчера, Гольдфарба и Шанно. По методу BFGS аппроксимация матрицы Гёссе производится по соотношению:

$$G^{(i+1)} = G^{(i)} + \frac{\left(S^{(i)} - G^{(i)}Q^{(i)}\right)S^{(i)^T} + S^{(i)}\left(S^{(i)} - G^{(i)}Q^{(i)}\right)^T}{Q^{(i)^T}S^{(i)}} -$$

$$- \frac{\left(S^{(i)} - G^{(i)}Q^{(i)}\right)Q^{(i)}S^{(i)}S^{(i)^T}}{\left(Q^{(i)^T}S^{(i)}\right)^2}, \qquad (2.35)$$

где

$$S^{(i)} = x^{(i)} - x^{(i-1)}, \;\; Q^{(i)} = \frac{d\varepsilon}{dx^{(i)}} - \frac{d\varepsilon}{dx^{(i-1)}}. \qquad (2.36)$$

Направление оптимизации совпадает с направлением, обратным вектору градиента.

В алгоритме Давидона-Флетчера-Пауэлла (*DFP*) аппроксимация матрицы *G* осуществляется следующим образом:

$$G^{(i+1)} = G^{(i)} + \frac{Q^{(i)}Q^{(i)^T}}{Q^{(i)^T}S^{(i)}} - \frac{G^{(i)^T}S^{(i)^T}S^{(i)}G^{(i)}}{S^{(i)^T}G^{(i)}S^{(i)}}, \qquad (2.37)$$

Недостатком алгоритма является большой объем вычислений и большой объем памяти по сравнению с методами градиентного спуска и сопряженных градиентов. Необходимо сохранять на каждой итерации оценки матрицы Гёссе, размерность которой зависит от настраиваемых параметров ИНС. Поэтому этот метод больше подходит для обучения небольших по размеру сетей.

Если в результате обучения ИНС не достигается требуемой точности на ее выходе, то возможно несколько решений:

− свертка топологии сети с уменьшением числа связей между нейронами (упрощение структуры) без переобучения сети;

− изменение топологии сети с последующей перенастройкой всех весов, т.е. необходимо переобучение ИНС;

− дообучение ИНС до тех пор, пока точность не достигнет требуемого порога;

− изменение параметров ИНС таких, как: вид сжимающей функции и алгоритм оптимизации ошибки;

− комбинация перечисленных способов.

2.3. Алгоритмы построения деревьев решений

Методы, основанные на построении деревьев решений (Decision Trees), используются для задач трех типов: описания данных – в компактном виде точное описание объектов; классификации – отнесение объекта к заранее определенному классу и регрессии – установлении зависимости входных переменных от выходных [64, 65]. К третьему типу задач относится также прогнозирование целевой переменной.

При построении деревьев решений возникают три вида задач: синтез критерия, который будет являться определяющим при ветвлении, определение условия остановки роста дерева в глубину и механизм отсечения ветвей. Точность решения задач с помощью деревьев определяется "ветвистостью" деревьев, поэтому исследователями в этой области даются рекомендации не ограничивать "рост деревьев".

Если для построения деревьев используются условные вероятности наступления событий, то целевая функция принимает дискретные значения 0 или 1. Таким образом, все множество возможных решений **E** конечно и его можно разбить на два подмножества:

$$\mathbf{E}=\mathbf{E}_{+} \cup \mathbf{E}_{-}, \qquad (2.38)$$

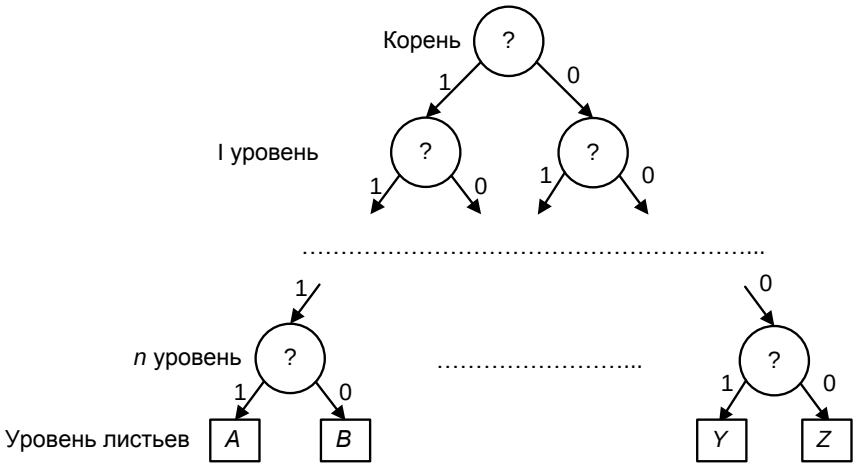
где $\mathbf{E}_{+}$ – подмножество, для которого целевая функция принимает положительные значения (1), $\mathbf{E}_{-}$ – подмножество, где значения целевой функции отрицательны (равны 0). Цель построения деревьев решений – определить классифицирующее правило, с помощью которого можно выделить из множества **E** подмножества $\mathbf{E}_{+}$ и $\mathbf{E}_{-}$. Метод работает по принципу перебора независимых переменных. В

результате перебора определяется та переменная, которая позволяет определить классифицирующее правило с наибольшей точностью.

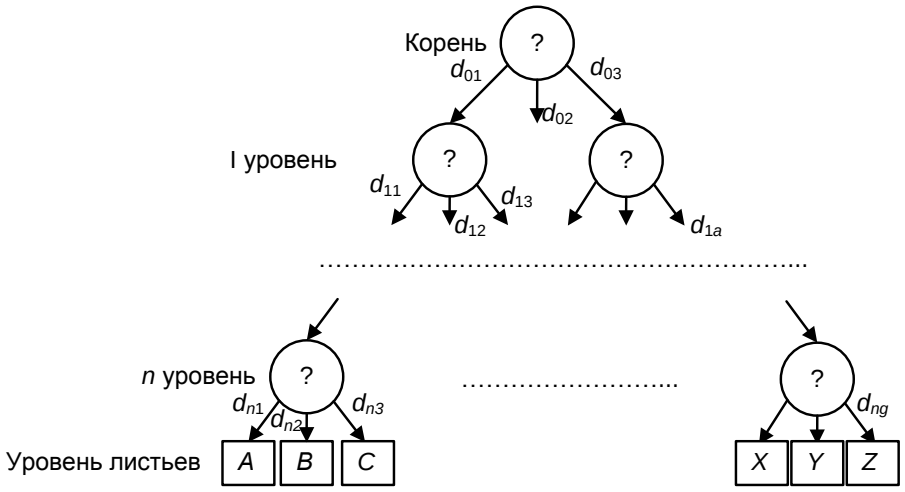
В связи с тем, что задача перебора базируется на двух дискретных состояниях, возникает иерархическая структура принятия решений или бинарное дерево перебора (см. Рисунок 2.7 (а)). В случае нескольких возможных значений атрибутов (состояний), а в общем случае еще и разных, дерево перебора и работа с ним становится сложнее (см. Рисунок 2.7 (б)). В теории принятия решений d_{ij} носят название диагнозов, которые определяют принадлежность того, или иного состояния, например, в методе Байеса.

Достоинством такой структуры является уверенное получение решения задачи даже при недостаточно полной информации о параметрах исследуемого объекта [66]. То есть при движении от начального узла (корня дерева), выбирая один из путей через узловые вершины, мы всегда закончим путь на одной из конечных вершин $A, B,\ldots, Z$ (листьев дерева). Каждое ветвление дерева представляет собой задачу выбора (проверки выполнения определенного критерия на i-м уровне), или выполнения процедуры оптимизации на текущем уровне (для сложных систем) [67]:

$$\mathbf{Q}_i(\mathbf{X}) = extrQ(x_1, x_2, ..., x_n). \qquad (2.39)$$



(а)



(б)

Рисунок 2.7 Примеры деревьев решений

Большое число вариантов алгоритмов начинает строить дерево решений, начиная от корня. Процедура расщепления рекурсивно применяется к исходному множеству **E**, а затем ко всем получаемым подмножествам и так далее с постепенным уточнением классификационного множества, с обоснованием критериев дробления и определением атрибутов. При отсутствии возможности определения классификационного правила дробление прекращается, а достигнутые узлы принимаются за листья.

Отличие в алгоритмах состоит в различных способах отнесение к тому или иному узлу в случае возникновения ситуации неопределенности. При этом могут создаваться дополнительные ответвления деревьев с дополнительными расщеплениями. При использовании неточных данных вместо определенного отнесения решения к каким-либо конечным вариантам, определяется непрерывная мера принадлежности, которая показывает вероятность принадлежности варианта решения к разным листьям (степень уверенности).

Наиболее используемыми являются следующие модификации алгоритмов:

CART (Classification and regression Tree) – алгоритм разработан Л. Брейманом с коллективом для построения бинарных деревьев. Алгоритм решает задачи классификации и регрессии;

C 4.5 – алгоритм построения деревьев с неограниченным количеством потомков узла, разработанный Р. Куинленом. Предназначен только для решения задач классификации;

QUEST (Quick, Unbiased, Efficient Statistical Trees) – разработан В. Ло и И. Ши на основе улучшенного варианта метода рекурсивного квадратичного дискриминантного анализа.

Алгоритм отсечения ветвей работает от листов к вершине дерева, отсекая или заменяя поддеревьями те ветви, которые не приведут к возрастанию ошибки.

Построение дерева решений осуществляется по обучающей выборке, а проверка адекватности построенной модели – по тестовому набору данных.

Недостатками алгоритмов построения деревьев решений являются:

− зависимости в полученных реальных данных достаточно сложны, что приводит к необходимости построения ветвистых структур деревьев, анализ которых затруднителен;

− при построении деревьев сложно найти компромисс между точностью и значимостью ветвей, поэтому получаемые структуры характеризуются "переобобщением";

− нахождение оптимального разбиения деревьев затруднительно, так как алгоритм не может вернуться назад для уточнения атрибута, с помощью которого можно было осуществить лучшее разбиение.

Достоинствами являются:

− наглядность, позволяющая проводить анализ вклада отдельных переменных в процедуре ветвления;

− работа с переменными различных типов;

− отсутствие необходимости в определении законов распределения данных.

2.4. Основные результаты и выводы по второй главе

1. Во второй главе были проанализированы методы для исследования уровня защищенности систем радиосвязи, среди которых можно выделить метод анализа оценок, аппарат искусственных нейронных сетей, а также алгоритмы построения деревьев решений. Использование описанных выше методов в работе предполагает сбор априорной информации, но зато позволит упростить процесс принятия решений на следующих этапах.

2. Использование вероятностных методов усложняет работу систем на их основе, так как необходимо получить выражения, определяющих влияние параметров системы связи друг на друга.

3. Метод формирования и анализа оценок применим в предметных областях с хорошо структурированными знаниями в отличие от аппарата искусственных нейронных сетей.

4. Для использования аппарата искусственных нейронных сетей необходимо определить структуру сети, вид сжимающей функции и алгоритм оптимизации, что потребует дополнительных исследований.

5. Скорость обучения нейронной сети зависит от точности, вида алгоритма оптимизации ошибки, а также от выполнения условия непротиворечивости обучающего множества.

6. Метод оценок удобно использовать в качестве вспомогательного, совместно с аппаратом искусственных нейронных сетей.

Глава 3
РАЗРАБОТКА МЕТОДА И АЛГОРИТМОВ ПРОГНОЗИРОВАНИЯ ПОКАЗАТЕЛЕЙ УСТОЙЧИВОСТИ ФУНКЦИОНИРОВАНИЯ ОТКРЫТОЙ СИСТЕМЫ СВЯЗИ

3.1. Выбор программных средств для проведения исследований

К программной среде, в которой должна быть реализована возможность обработки ИНС, предъявляются следующие требования [68-71]:

- понятный и простой интерфейс;
- иметь возможность ввода и вывода данных;
- включать библиотеку большинства математических функций, а также модулей по работе с ИНС;
- возможность сохранения результатов на жесткий диск и их распечатки;
- небольшая стоимость лицензии.

Наиболее популярные программные языки, такие как C++, Basic, Pascal, Delphi, Java не способны решить поставленные перед программой задачи без специальных библиотек математических функций, либо будут иметь большой объем программного кода, на создание которого уйдет много времени.

Математические пакеты, такие как MathCAD, MatLab, Wolfram Mathematica, Statistica и др., больше удовлетворяют требованиям, поставленным перед программной средой. Они имеют понятный пользовательский интерфейс, имеют большое количество математических функций в своих библиотеках и могут обрабатывать большой объем статистических данных.

Перечисленные математические пакеты имеют свой встроенный язык программирования, либо имеют возможность интегрирования с помощью программного средства, такого как MS NET Framework кода, написанного с помощью Borland Delphi, Visual Basic, C++, и C#.

Statistica

Statistica Enterprise (торговая марка – STATISTICA) – мощный пакет для статистического анализа, разработанный компанией StatSoft. В пакете STATISTICA Enterprise реализованы процедуры для анализа данных (data analysis), управления данными (data management), добычи данных (data mining), визуализации данных (data visualization). Имеются средства для работы с ИНС.

COM-архитектура STATISTICA открывает доступ к библиотекам функций, которые можно реализовать при помощи таких языков программирования как: Borland Delphi, Visual Basic, C#, и C++. В случае C++, разработчики могут интегрировать объектную модель STATISTICA также как и библиотеки Microsoft Foundation Classes, стандартные библиотеки C++, и Standard Template Library. Например, алгоритмы и функции библиотек STL можно достаточно легко объединить с библиотеками STATISTICA в пользовательском приложении.

Надстройки. Наиболее часто встречающийся случай использования C++ и библиотек STATISTICA является создание пользовательской динамической библиотеки (*.dll). Используя Active Template Library совместно с COM-архитетурой STATISTICA, можно создать свой собственный интерфейс, который в дальнейшем может быть интегрирован в STATISTICA. Использование C++ в пользовательском приложении STATISTICA увеличивает скорость работы программ, что связано со спецификой языка C/C++.

Wolfram Mathematica

Wolfram Mathematica – система для выполнения разноплановых технических вычислений.

Mathematica предоставляет пользователю огромный инструментарий:

- символьные и численные вычисления;
- библиотеки математических и статистических функций, теории групп и теории чисел;
- работа с графикой, в том числе инструменты визуализации и анимации, обработка и распознавание изображений;

− инструментарий для финансовых вычислений, анализа текстовых и графических данных и т.д.;

− база данных математической, научной и социально-экономической информации;

− встроенный язык программирования, поддерживающий функциональный, процедурный и объектно-ориентированный стили программирования;

− средства создания программ и пользовательских интерфейсов, параллельных вычислений, подключения внешних DLL и т.д.

MathCAD

Mathcad – система компьютерной алгебры из класса систем автоматизированного проектирования, ориентированная на подготовку проектов, интерактивных форм, содержащих элементы визуализации, отличается легкостью в использовании и возможностью совместной разработки.

Последние версии MathCAD имеют не очень мощный, но весьма элегантный собственный язык. Это позволяет программисту эффективно применять программный код в проектах MathCAD , а простота и интуитивность языка программирования позволяет ему быстро обучаться в процессе работы. В то же время программные модули внутри текста разработки сочетают в себе обособленность (поэтому их легко отличить от остальных формул) и простоту восприятия.

MatLab

Программное обеспечение MathWorks MATLAB представляет собой высокоуровневый язык технических расчетов, интерактивную среду разработки алгоритмов и современный инструмент анализа данных. MathWorks в MATLAB по сравнению с традиционными языками программирования (C/C++, Java, Pascal, FORTRAN) позволяет на порядок сократить время решения типовых задач и значительно упрощает разработку новых алгоритмов.

MathWorks MATLAB представляет собой основу всего семейства продуктов MathWorks и является главным инструментом для решения широкого

спектра научных и прикладных задач, в таких областях как: моделирование объектов и разработка систем управления, проектирование коммуникационных систем, обработка сигналов и изображений, измерение сигналов и тестирование, финансовое моделирование, вычислительная биология и другие.

Ядро MATLAB позволяет максимально просто работать с матрицами реальных, комплексных и аналитических типов данных. Содержит встроенные функции линейной алгебры (LAPACK, BLAS), быстрого Фурье преобразования (FFTW), функции для работы с полиномами, функции базовой статистики и численного решения дифференциальных уравнений. Все встроенные функции ядра MATLAB разработаны и оптимизированы специалистами и работают быстрее или так же, как их эквивалент на C/C++.

Язык программирования системы MATLAB вобрал в себя все средства, необходимые для реализации различных видов программирования:

- процедурного;
- операторного;
- функционального;
- логического;
- структурного (модульного);
- объектно-ориентированного;
- визуально-ориентированного.

NeuroPro – отечественная разработка института вычислительного моделирования СО РАН г. Красноярск автор: Царегородцев В.Г. Данный программный продукт представляет собой менеджер обучаемых искусственных нейронных сетей, работающий в среде MS Windows и позволяющий производить следующие базовые операции:

- подключение к проекту файла (базы) данных в формате dfb (dBase, FoxBase, FoxPro, Clipper) или db (Paradox);
- работа с ИНС слоистой архитектуры с числом слоев нейронов от 1 до 10, числом нейронов в слое – до 100;

− обучение нейронной сети решению задачи прогнозирования или классификации. Нейронная сеть может одновременно решать как несколько задач прогнозирования (прогнозирование нескольких чисел), так и несколько задач классификации, а также одновременно задач и прогнозирования, и классификации.

− тестирование нейронной сети на файле данных, получение статистической информации о точности решения задачи;

− вычисление показателей значимости входных сигналов сети, сохранение значений показателей значимости в текстовом файле на диске;

− упрощение нейронной сети;

− генерация и визуализация вербального описания нейронной сети, сохранение вербального описания в текстовом файле на диске;

− выбор алгоритма обучения, назначение требуемой точности прогноза, настройка нейронной сети.

В таблице 3.1 приведена стоимость лицензий математических пакетов. Анализируя приведенное описание пакетов, из принципа достаточности и простоты использования мной был выбран пакет NeuroPro.

Таблица 3.1 – Сравнение стоимости лицензий математических пакетов

Наименование	Стоимость лицензии, руб.
MathCAD Student Edition	4300
STATISTICA Base for Windows v.10 Russian	16700
Matlab 2011b for student use	3500
Wolfram Mathematica Student Version Educational Unbundled	5500
NeuroPro	Бесплатно

К важному достоинству пакета NeuroPro относится возможность целенаправленного упрощения ИНС с последующей генерацией вербального

описания. При упрощении нейронной сети возможно выполнение следующих операций:

− сокращение числа входных сигналов нейронной сети путем удаления входных сигналов, наименее значимых для принятия сетью решения;

− сокращение числа нейронов сети путем удаления нейронов, наименее значимых для принятия сетью решения;

− комплексное равномерное упрощение нейронной сети. Для каждого нейрона сети выполняется сокращение числа приходящих на него сигналов до максимально возможного числа, задаваемого пользователем;

− сокращение числа связей в нейронной сети путем удаления связей, наименее значимых для принятия сетью решения;

− бинаризация связей в нейронной сети – приведение весов синапсов к значениям –1 и 1 или к значениям из более широкого диапазона.

Наличие развитых возможностей по упрощению сети в совокупности с построением ее вербального описания позволяет понять процесс решения задачи с помощью нейронной сети и, таким образом, синтезировать алгоритм решения задачи.

3.2. Анализ угроз системам связи. Показатели устойчивости

Адаптация к новым, непредусмотренным внешним условиям, противостояние дестабилизирующим факторам систем связи с выполнением своих основных функций определяется запасом, увеличивающих устойчивость функционирования. Отказы компонентов систем связи могут происходить из-за повреждений, аварийных ситуаций и в результате реализации атак.

Устойчивость систем связи можно охарактеризовать с помощью оценки структуры (топологии) сети и надежности ее элементов. Запас по устойчивости сети будет определяться надежностью компонентов и топологией, а также условиями эксплуатации и нагрузкой на них. С помощью теории надежности такую оценку произвести не составляет большого труда.

Усложнение систем связи введением многофункциональных элементов, средств самодиагностики и защиты, а тем более самоорганизующихся компонентов приводит к тому, что общий показатель устойчивости сложной системы **Q** имеет интегральный и комплексный характер зависимости от параметров системы [72-76], представляя собой набор показателей Q_i:

$$\mathbf{Q} = Q(Q_1, Q_2, ..., Q_n). \qquad (3.1)$$

Для беспроводных систем связи увеличение времени противодействия атакам происходит при:

- усилении криптозащиты;
- уменьшении дальности связи;
- использовании направленных антенн;
- уменьшении объема передаваемых данных;
- изменении частоты и мощности сигнала;
- увеличении помехозащищенности аппаратуры и др.

Не смотря на защищенность протоколов связи, практически все они подвержены угрозам со стороны злоумышленников.

В качестве показателей устойчивости Q_i в (3.1) кроме коэффициента готовности могут служить: взломостойкость, время функционирования до установленного факта взлома, и т.д.

При обмене данными между БС и клиентской станцией, установленной на подвижном наземном объекте, по каналу связи происходит передача информации (см. Рисунок 3.1). Прямые угрозы информационной безопасности возникают при передаче данных от БС к клиентской станции и/или в обратном направлении [77]. Прямые угрозы были описаны в п. 1.2. К косвенным угрозам относятся:

- обнаружение БС и клиентских станций;
- маскировка под легальную базовую или клиентскую станцию;
- использование или захват каналов соседних БС;
- комбинации из приведенных угроз.

Косвенные угрозы опаснее прямых, так как при их реализации злоумышленнику проще скрыть свои действия.

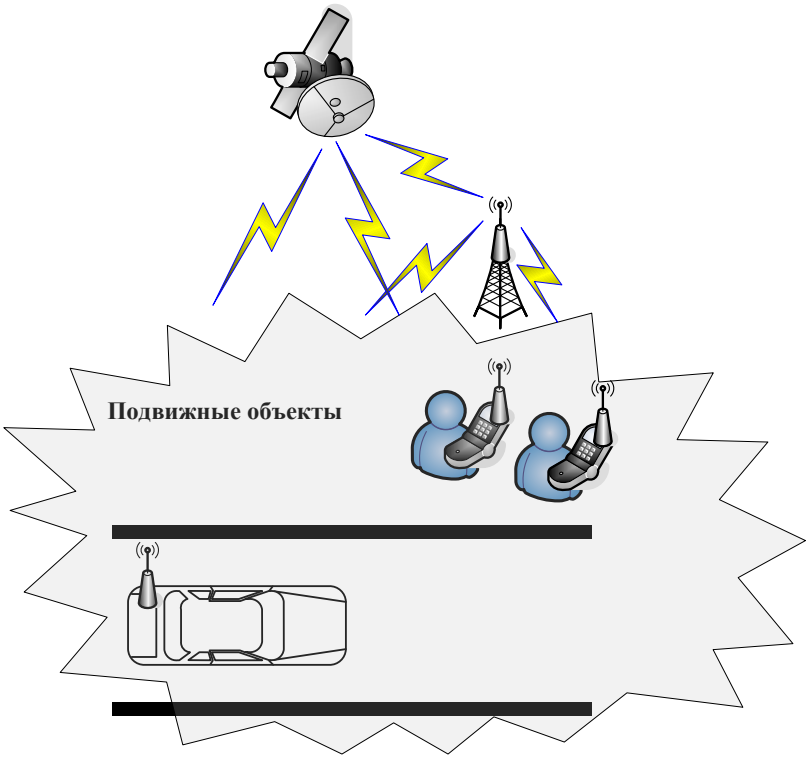


Рисунок 3.1

Для исследуемых протоколов были определены в данной работе возможности реализации угроз системе связи с подвижными наземными объектами, представленные в таблице 3.2.

Таблица 3.2 Возможность реализации угроз при использовании различных протоколов видов связи

Технология / Угрозы	WiFi	GSM	LTE	BlueTooth	DSRC	APCO P25
Подслушивание	+	+	+	+	+	+
Отказ в обслуживании	+	+	+	+	+	+
Глушение клиентской станции	+	+	+	+	+	+

Глушение базовой станции	+	+	+	+	+	+
Угрозы криптозащите	+	+	+	+	+	+
Анонимность атак	+	+	+	+	+	+
Вирусная атака	–	–	–	+	–	–
Взлом алгоритма	+	+	+	+	+	+
Косвенные угрозы	+	–	–	+	+	–

3.3. Определение значимости параметров протоколов для построения системы связи

Анализ основных протоколов, использование которых возможно для организации связи с наземными подвижными объектами, описанными подробно в главе 1, показал, что претендентами являются: WiFi, GSM, LTE, Bluetooth, DSRC, CDMA и APCO-P25 [78, 79]. Каждый протокол связи характеризуется большим числом параметров. В работе использован метод анализа оценок для определения тех параметров протоколов, которые сильнее влияют на защищенность протоколов. Для этого были определены пять наборов оценок, а результаты этого этапа работы сведены в таблицу 3.3. Величина $x_{ср}$ рассчитана по формуле (2.1). Вес j-го фактора w_j определим по выражению, полученного из (2.2) и (2.3):

$$w_j = \frac{1}{k}\sum_{i=1}^{k}\frac{x_{ji}}{\sum_{j=1}^{n} x_{ji}}, \qquad (3.2)$$

где $n = 13$, $k = 5$.

Результаты расчетов внесены в таблицу 3.4. СКО и коэффициент вариации υ рассчитан по формулам (2.5) и (2.6). Величина S рассчитана по соотношению:

$$S = \sum_{j=1}^{n} \left(\sum_{i=1}^{k} x_{ji} - 0{,}5k(n+1) \right)^2,$$

результаты расчетов также сведены в таблицу 3.4.

Так как в наборах оценок имеются связанные ранги, то коэффициент конкордации определим по соотношению (2.14) с использованием (2.15):

$$W = \frac{12 \cdot 1544}{5^2(13^3 - 13) - 5 \cdot 1716} = 0{,}403.$$

Из расчета можно сделать вывод, что оценки являются хорошо согласованными.

В связи с хорошей согласованностью оценок и из анализа таблиц 3.3 и 3.4 можно сделать вывод, что следующие параметры протоколов оказались значимыми:

- общее количество каналов;
- используемая полоса частот;
- мощность базовой станции;
- разнос каналов;
- идентификация абонента;
- типичный радиус ячейки;
- зависимость от ландшафта;
- ограничение по доступу;
- область применения связи;
- наличие шифрования;
- оплата за использование.

Параметры "Вид модуляции" и "Тип связи" исключаем из нашего рассмотрения из-за низких оценок значимости.

Таблица 3.3 – Данные формирования оценок значимости параметров протоколов связи

Параметр	Набор	Набор	Набор	Набор	Набор	$x_{ср}$

	оценок I	оценок II	оценок III	оценок IV	оценок V	
Общее количество каналов	10	9	10	10	9	9,6
Используемая полоса частот	10	10	8	9	10	9,4
Мощность базовой станции	10	10	9	10	10	9,8
Разнос каналов	10	9	10	10	10	9,8
Вид модуляции	7	8	6	7	8	7,2
Тип связи	6	7	7	6	8	6,8
Идентификация абонента	10	9	9	10	10	9,6
Типичный радиус ячейки	10	9	10	10	9	9,6
Зависимость от ландшафта	9	9	8	9	9	8,8
Ограничение по доступу	9	9	9	9	9	9
Область применения связи	8	9	8	10	10	9
Наличие шифрования	10	9	10	10	9	9,6
Оплата за использование	8	9	9	8	8	8,4
Сумма	117	116	113	118	119	—
H_i	222	726	144	360	264	—

Таблица 3.4 – Результаты расчетов значимости параметров

Параметр	Набор оценок I	Набор оценок II	Набор оценок III	Набор оценок IV	Набор оценок V	w_j	СКО	υ, %	S
Общее количество каналов	0,08547	0,07759	0,08850	0,08475	0,07563	0,08239	0,54772	5,71	169
Используемая полоса частот	0,08547	0,08621	0,07080	0,07627	0,08403	0,08056	0,89443	9,52	144
Мощность базовой станции	0,08547	0,08621	0,07965	0,08475	0,08403	0,08402	0,44721	4,56	196
Разнос каналов	0,08547	0,07759	0,08850	0,08475	0,08403	0,08407	0,44721	4,56	196
Вид модуляции	0,05983	0,06897	0,05310	0,05932	0,06723	0,06169	0,83666	11,62	1
Тип связи	0,05128	0,06034	0,06195	0,05085	0,06723	0,05833	0,83666	12,30	1
Идентификация абонента	0,08547	0,07759	0,07965	0,08475	0,08403	0,08230	0,54772	5,71	169
Типичный радиус ячейки	0,08547	0,07759	0,08850	0,08475	0,07563	0,08239	0,54772	5,71	169
Зависимость от ландшафта	0,07692	0,07759	0,07080	0,07627	0,07563	0,07544	0,44721	5,08	81
Ограничение по доступу	0,07692	0,07759	0,07965	0,07627	0,07563	0,07721	0,00000	0,00	100
Область применения связи	0,06838	0,07759	0,07080	0,08475	0,08403	0,07711	1,00000	11,11	100

Наличие шифрования	0,08547	0,07759	0,08850	0,08475	0,07563	0,08239	0,54772	5,71	169
Оплата за исполь-зование	0,06838	0,07759	0,07965	0,06780	0,06723	0,07213	0,54772	6,52	49
Сумма	—	—	—	—	—	—	—	—	1544

3.4. Анализ структурной устойчивости сети связи

Оценка устойчивости структуры распределенной в пространстве системы связи с подвижными объектами осуществляется в результате анализа графа ***G***, в котором вершинам *S* соответствуют базовые и клиентские станции, ретрансляторы, а ребрам *R* – каналы связи [80-82]. Тогда такой граф можно представить как:

$\boldsymbol{G}=\{S, R\}$.

Совокупность ребер, которую проходит сигнал от начальной точки ($S_{нач}$) к конечной ($S_{кон}$) образует путь. Длина пути (L) определяется как сумма длин ребер, входящих в путь:

$$L = \sum_{i=1}^{n} \left\| R_i \right\|, \quad i = \overline{1, n}, \tag{3.3}$$

где *n* – количество ребер в пути. Свойство связности графа на практике позволяет построить обходной путь, если невозможно проложить маршрут (при потере связи с определенными вершинами). Потеря связности графа, а также выполнение условия $S=\varnothing$ или $R=\varnothing$, приводит на практике к полной потере связи между удаленными объектами [80, 81]. Следовательно, связность графа – необходимое условие живучести сложной системы связи. Математически проверка графа на связность не представляет проблемы, необходимо проверить выполнение условия:

$$R \geq S - 1. \tag{3.4}$$

В то же время увеличение живучести происходит с ростом плотности графа:

$$\left|\frac{R}{S}\right| \to \max , \qquad (3.5)$$

то есть с ростом количества каналов связи относительно радиоточек. Максимум плотности достигается в случае полносвязного графа, когда:

$$R = 0{,}5S(S-1) .$$

С другой стороны с ростом числа станций S, может возникнуть ситуация:

$$S > S_{\max}, \qquad (3.6)$$

где $S_{\max}$ – количество станций, при котором произойдет отказ в обслуживании абонентов. Для закрытой линейной системы связи типа GSM, CDMA, WiMAX каждая БС с зоной покрытия (охвата) H_i может обслуживать только определенное число абонентов. Другими словами критическая плотность подвижных абонентов находится в зависимости:

$$\rho_{\text{крит}} = F(H_{\text{охв}}, \boldsymbol{N}, R_{max}), \boldsymbol{N} = \overline{N_1, N_2, ..., N_i} , \qquad (3.7)$$

от $H_{\text{охв}}$ – зоны охвата БС; N_i – количества абонентов (каналов), осуществляющих связь с i-ой станцией; R_{max} – наибольшего количества каналов для исследуемого протокола связи. Например, для Wifi 802.11 R_{max} = 14 каналов, Wifi 802.11a R_{max} = 38 каналов, а для DSRC до 5 шт. и т.д.

Отметим, что в выражении (3.7), во-первых, не учитывается влияние нескольких пользователей на БС, находящихся в ее зоне охвата (см. Рисунок 3.2). Эти пользователи занимают каналы БС, число которых R. Во-вторых, не учитывается мощность графа.

Примем для определенности, что линейная система связи состоит из нескольких промежуточных БС (БС2 и БС3), расположенных между источником информации и приемником.

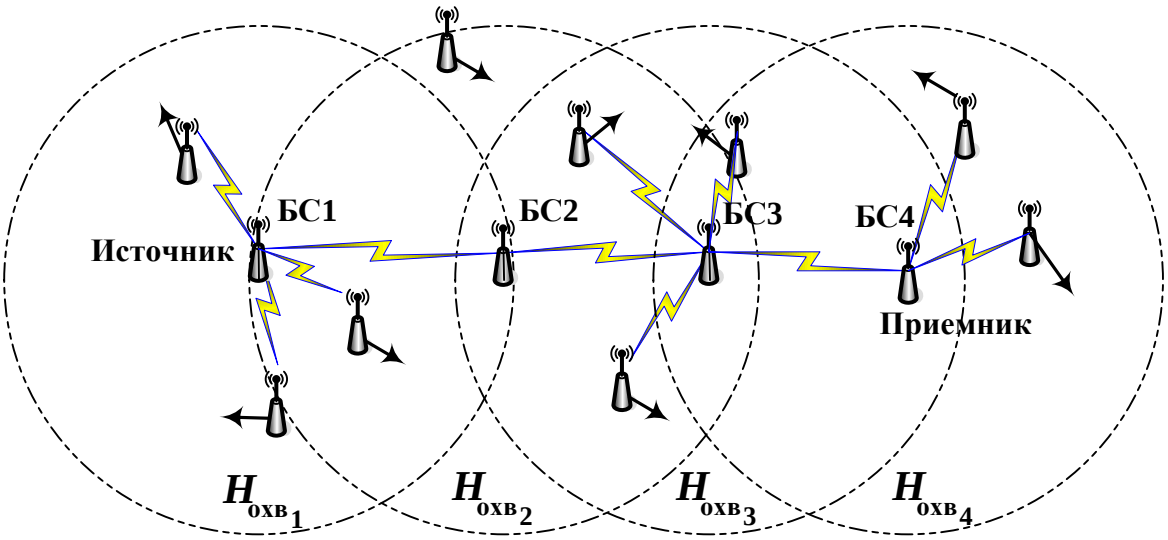


Рисунок 3.2. Линейная система связи с подвижными объектами

При нарушении условия (3.6) и с учетом (3.7) аппаратура закрытой системы беспроводной связи откажет в доступе абонентам, пытающимся установить связь. По-другому обстоит дело, когда беспроводная сеть организована с использованием открытого протокола (WiFi, DSRC), а также в случае микросотовых и сенсорных сетей [83, 84]. При активизации абонентских станций происходит установка связи как абонент–БС, так и абонент–соседняя БС. В итоге запас каналов базовых станций быстро расходуется, приводя к отказу в обслуживании, либо к снижению трафика. Причем плотность абонентов будет ниже, чем в случае с закрытой системы связи. Вдобавок к этому могут происходить конфликты (см. Рисунок 3.3), когда образуется два одинаковых по содержанию потока данных, получаемых от одного источника BS_1, от станций MS_1 и MS_2, предназначенных для одной БС BS_2.

В случае закрытой системы связи количество абонентов ограничено в зоне покрытия H_i, также как и трафик. Поэтому расчетным путем, а затем в результате испытаний с учетом местного ландшафта определяются частотный канал и зона покрытия конкретной БС. Поэтому устойчивость структуры у закрытых систем связи довольно высокая.

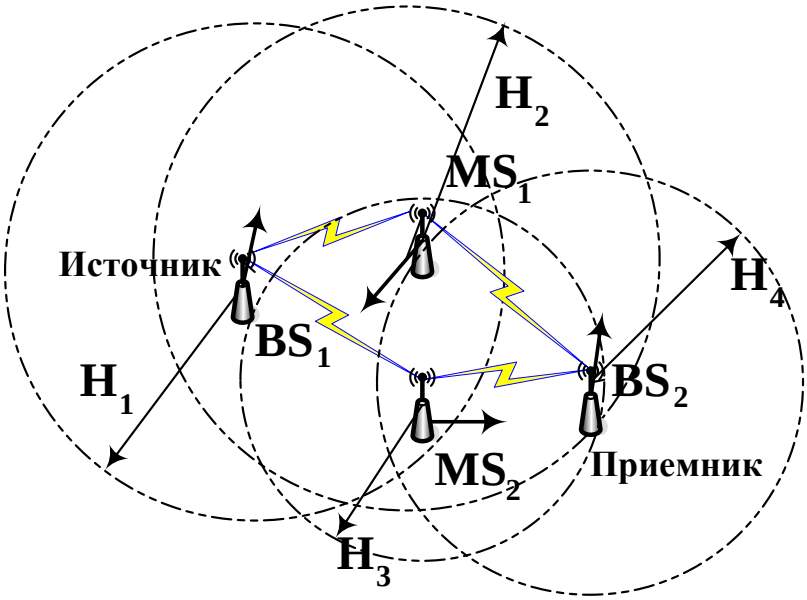


Рисунок 3.3. Конфликт в открытой системе связи с подвижными объектами

Для открытых систем связи с подвижными объектами количество каналов не ограничивается, что в результате роста плотности может привести к преодолению критической величины для данного протокола связи. Привязки к ландшафту подвижные объекты не имеют, следовательно, их зоны покрытия могут динамически изменяться, приводя к ситуациям уменьшения или увеличения плотности. Отключение канала связи аппаратурой не производится в случае перегрузки БС. Рост зоны охвата сети приводит к тому, что радиосигналы можно легко перехватить и/или заглушить. Таким образом, живучесть таких систем связи может снижаться из-за роста числа абонентов [85, 86].

Для открытой системы связи (см. Рисунок 3.2), представляющей цепочку базовых станций: БС1–БС2–БС3–БС4, по которой передается информация от источника к приемнику, будут заняты каналы: у БС1 и БС4 – по одному, у БС2 и БС3 – по два. Обозначив с помощью индексов количество мобильных станций, связанных с соответствующей БС, получим систему:

$$\begin{cases} N_1 + 1 \le R_{\max} \\ N_2 + 2 \le R_{\max} \\ N_3 + 2 \le R_{\max} \\ N_4 + 1 \le R_{\max} \end{cases}. \qquad (3.8)$$

В системе (3.8) не учтено влияние мобильных пользователей, также занимающих каналы БС открытой беспроводной сети. Действительно, если расстояние такого абонента до БС меньше ее зоны покрытия:

$$r(X,Y) < H_{\text{охв}}, \tag{3.9}$$

где

$$r(X,Y) = \sqrt{(x - x_0)^2 + (y - y_0)^2}$$

евклидово расстояние от абонента до БС с координатами (x_0, y_0), то канал связи у соседней БС также будет занят.

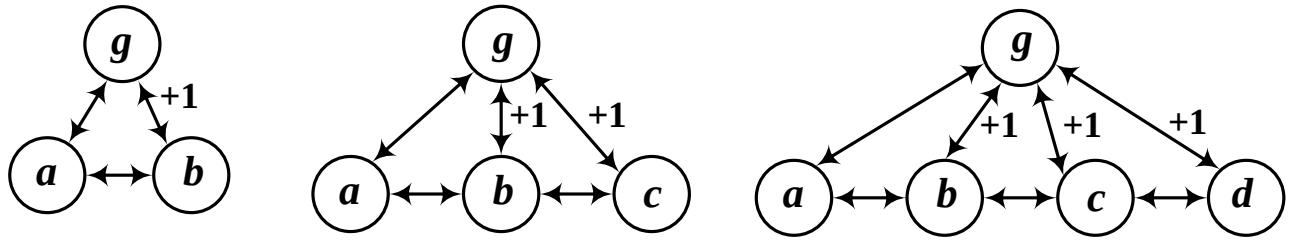
Рост числа занимаемых каналов отражен на рисунке 3.4. При охвате мобильного абонента *g*, находящегося в зоне БС *a*, активизируется связь *g* со станцией *b*. При этом у станции *b* расходуется еще один канал связи (см. Рисунок 3.4. (а)). Если абонент находится еще и в зоне доступа БС *c*, то и у этой станции расходуется канал (см. Рисунок 3.4. (б)). Аналогичная ситуация – в случае (рис. 3.4. (в)). Рассмотренные варианты становятся актуальными при уменьшении расстояний между базовыми станциями. Таким образом, для четырех рассматриваемых БС сформирована модель следующего вида (см. Рисунок 3.5). Пирамида поясняет лавинообразное число занимаемых каналов базовых станций при росте пользовательских станций, находящихся в зоне охвата нескольких станций. Причем рост числа пользователей *e, g* и *n*, занимающих по одному каналу у базовых станций *a, b, c* и *d* (отображено в виде линии связи) менее опасен, чем рост числа абонентов типа *k* и *l*, а тем более типа *m*. Чем выше по пирамиде тип пользователя, тем быстрее падает устойчивость функционирования системы связи.

С учетом приведенных соображений систему (3.8) преобразуем следующим образом:

$$\begin{cases} N_1 + 1 \le R_{\max} \\ N_2 + 2 + N_{12} + N_{123} + N_{1234} \le R_{\max} \\ N_3 + 2 + N_{23} + N_{123} + N_{234} + N_{1234} \le R_{\max} \\ N_4 + 1 + N_{34} + N_{234} + N_{1234} \le R_{\max} \end{cases}, \qquad (3.10)$$

где N_{12} – количество мобильных станций, связанных и с БС1, и БС2, N_{123} – связанных и с БС1, и с БС2 и с БС3 и т.д.

Нарушение любого условия в выражении (3.10) приведет к отказу в обслуживании одной из БС (или сразу нескольких), и цепь, по которой передается информация, прервется.



а) б) в)

Рисунок 3.4.

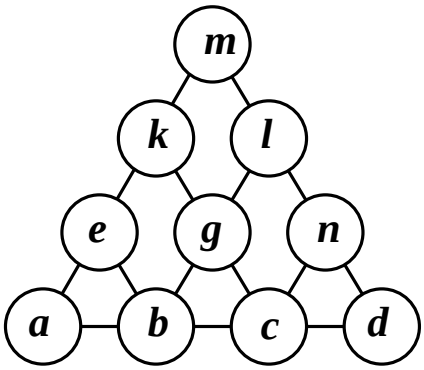


Рисунок 3.5. Лавинообразный рост занятых каналов с увеличением числа многосвязных станций

Выражение (3.10) не учитывает случая, когда происходит превышение величины $R_{\max}$ у станций, не участвующих в передаче информации от источника к приемнику, так как это и не влияет на устойчивость канала источник–приемник.

3.5. Разработка методики обучения и нахождения наилучшего варианта структуры нейронной сети

Использование аппарата ИНС предполагает следующие этапы:

- формирование обучающего множества – справочника;
- определение структуры ИНС;
- подбор параметров ИНС;
- выбор метода оптимизации ошибки;
- выбор наилучшего варианта ИНС.

На каждом этапе: выбор числа слоев; подбор параметров и метода оптимизации – необходимо каждый раз проводить заново обучение, так как сеть преобразуется. В итоге каждый этап представляет собой отдельную задачу, для которой требуется проведение экспериментов на ЭВМ.

Разработанная методика обучения ИНС состоит из нескольких этапов (см. Рисунок 3.6).

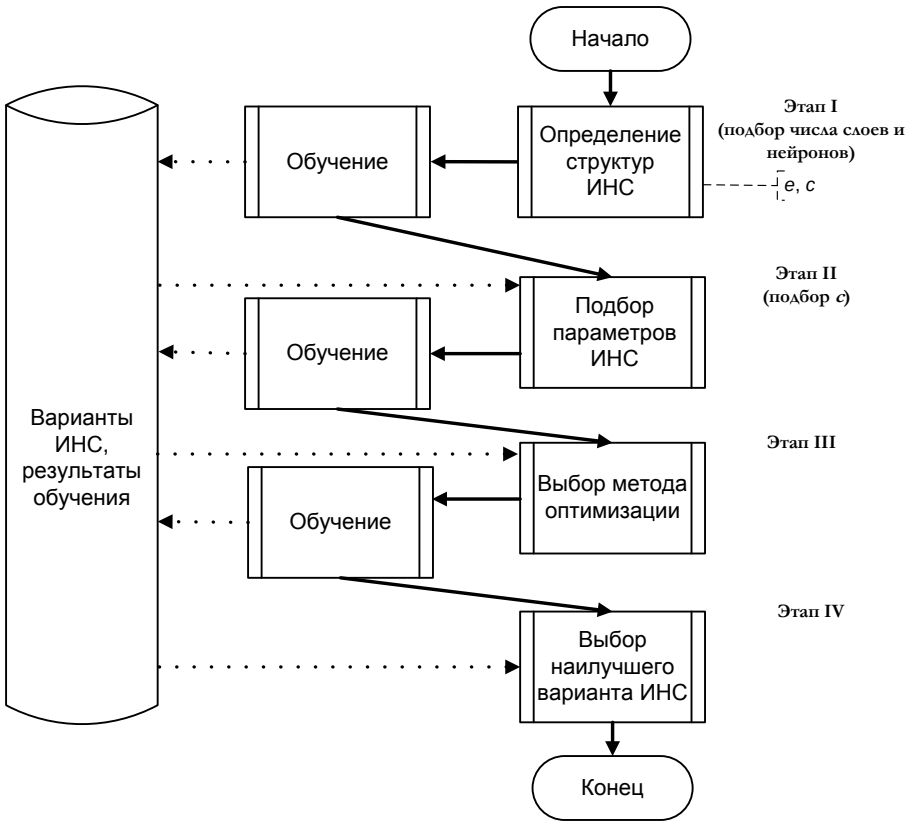


Рисунок 3.6. Этапы обучения и нахождения наилучшего варианта ИНС

Для исследования влияния количества мобильных пользователей разных типов на устойчивость беспроводной сети связи был разработан алгоритм для формирования обучающего множества. Схема алгоритма показана на рисунке 3.7 для системы связи, изображенной на рисунке 3.8.

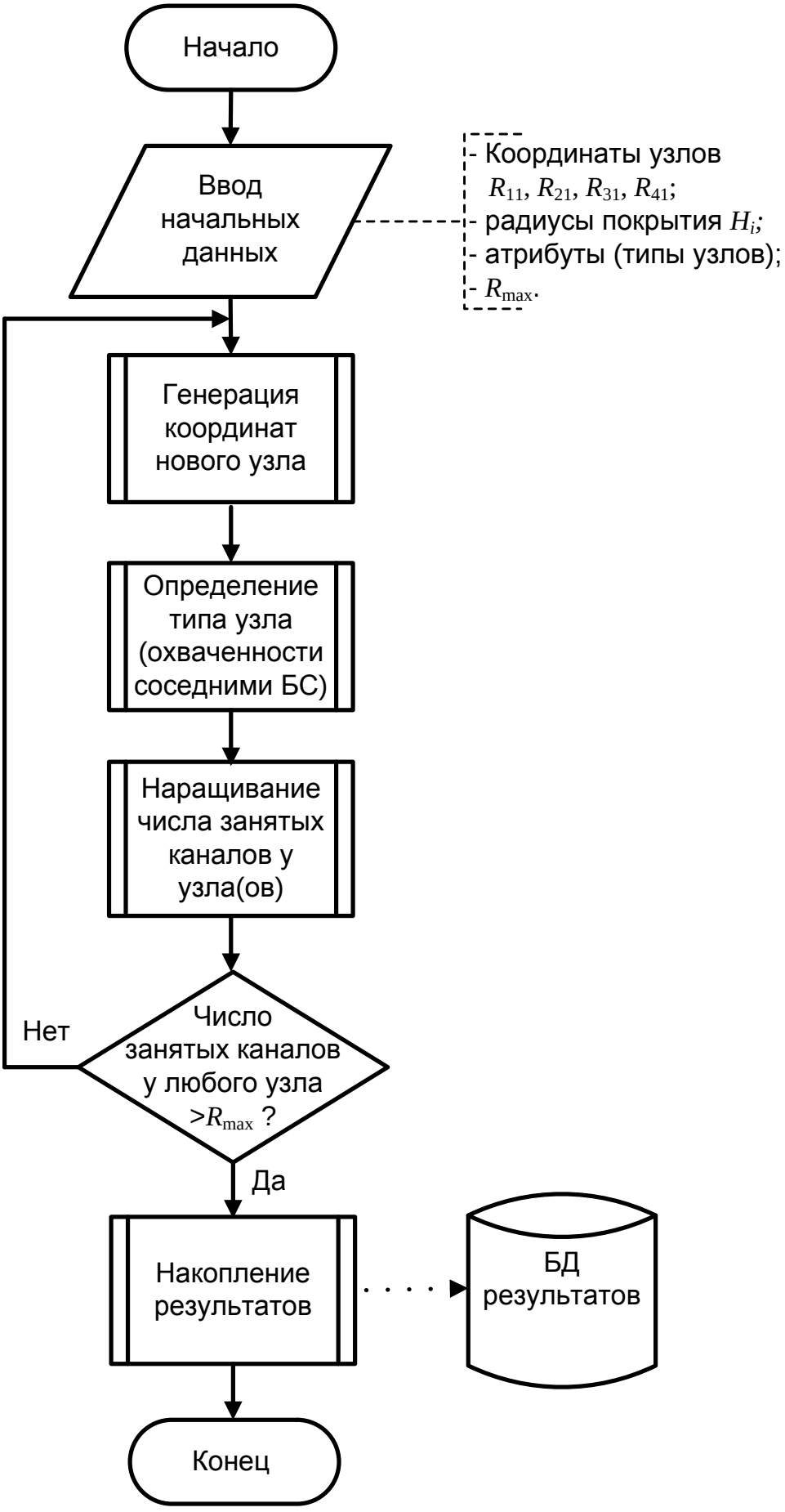


Рисунок 3.7. Структурная схема разработанного алгоритма

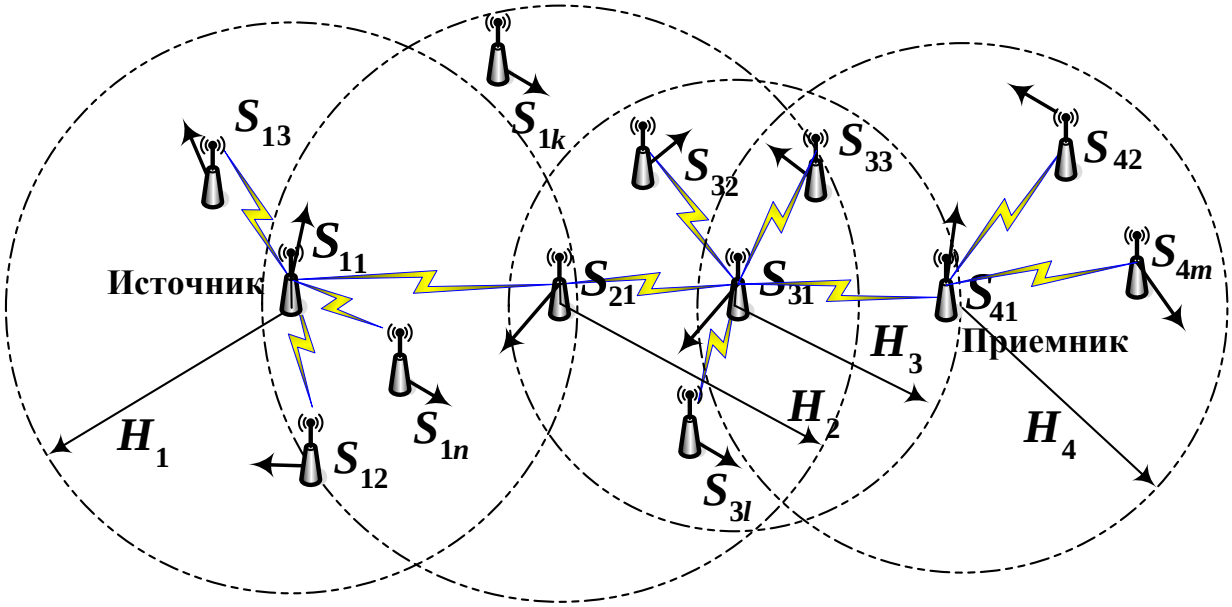


Рисунок 3.8. Структурная схема исследуемой системы связи

В некоторых источниках [79, 83] для генерации координат станций абонентов предложено использовать распределение Пуассона. Но стохастический характер появления новых подключений мобильных абонентов обуславливает применение в моей работе генератора случайных чисел. Попадание абонентов в зону действия БС также получается случайно. При эксперименте не учитывалось перемещение абонентов по территории и ландшафт местности. Для конкретного исследования был выбран протокол WiFi 802.11, для которого R_{max} = 14 каналов. Зоны покрытия базовых станций были приняты одинаковыми: H_i=300/2=150 м. Число абонентов варьировалось в пределах 15…20 шт. За координаты БС были приняты следующие значения: (150; 150), (200; 150), (320; 150), (450; 150).

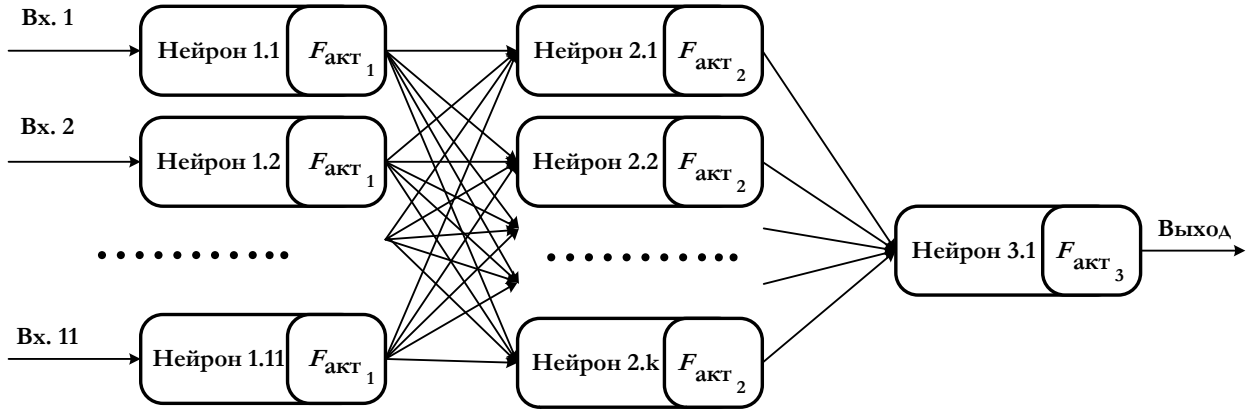
На результаты экспериментов сильно влияют протяженность линии связи и количество сгенерированных пользователей, что отражает таблица 3.5. Даже при N_{1234}=0 может наступить отказ в обслуживании беспроводной линии связи (опыты 15, 16, 18 и др.).

Таблица 3.5. Сравнительная таблица экспериментальных данных

№ опыта	Протяженность линии связи, м	Сгенерированных пользователей	Число занятых каналов, находящихся в зоне покрытия				Превышение R_{max}
			Одной БС (N_1+ N_2+ N_3+ N_4)	Двух БС (N_{12}+ N_{23}+ N_{34})	Трех БС (N_{123}+ N_{234})	Четырех БС (N_{1234})	
1	360	20	23	7	0	0	Нет
2			28	9	0	0	Нет
3			29	9	2	0	Нет
4			30	10	1	0	Нет
5			30	10	2	0	Есть
6			30	11	1	0	Есть
7			32	12	2	0	Есть
8			32	12	3	0	Есть
9			33	14	4	0	Есть
10	300	20	23	8	2	0	Нет
11			24	9	1	0	Нет
12			25	8	2	0	Нет
13			25	9	2	0	Нет
14			26	10	0	0	Нет
15			26	11	2	0	Есть
16			27	9	2	0	Есть
17			27	10	1	0	Нет
18			28	10	1	0	Есть
19			28	10	2	0	Нет
20			28	12	2	0	Есть
21			29	10	0	0	Нет
22			29	11	2	0	Есть
23			29	12	4	0	Есть
24			29	13	2	0	Есть
25	200	20	24	12	7	2	Есть
26			29	13	3	1	Есть
27			39	22	9	1	Есть

28		15	15	5	2	0	Нет
29			16	5	0	0	Нет
30			18	7	2	0	Нет
31			18	9	5	1	Есть
32			19	8	2	0	Нет
33			20	7	2	0	Нет
34			20	8	3	0	Нет
35			21	9	4	0	Нет
36			23	9	3	0	Нет
37			24	11	4	0	Есть

Так как структура ИНС заранее не известна, то начинается исследование с предполагаемой структуры ИНС, или с наиболее простой (см. Рисунок 3.9). Если обучающее множество обладает свойством непротиворечивости, то усложнение структуры ИНС производится наращиванием числа скрытых слоев и/или нейронов в них. При появлении возможности решить задачу с требуемой точностью, структура сети может упрощаться. В итоге получается ИНС с минимальным количеством слоев и нейронов в них.



Ри

Рисунок 3.9. Начальная топология ИНС

Сигмоидальные элементы нелинейности (см. Рисунок 3.9) или активационные функции $F_{\text{акт}_i}$ – определяют крутизну сигмоиды i-го слоя ИНС с помощью параметра c по соотношению:

$$F_{акт_i} = \frac{w_{ij}}{c_i + \left| w_{ij} \right|}, \qquad (3.11)$$

где w_{ij} – весовые коэффициенты для *j*-го нейрона, находящегося в *i*-м слое ИНС.

При постановке имитационных экспериментов введем обозначение вариантов исследуемых ИНС в виде:

_a_/_b_/…_/z_,

где *a* – количество нейронов в первом слое; *b* – во втором (скрытом) слое, … , *z* – число нейронов в выходном слое.

Для выбора наилучшего метода оптимизации ошибки из следующих: градиентного спуска, параллельных касательных, сопряженных градиентов и BFGS также необходимо проведение экспериментов на ЭВМ.

Выбор наилучшего варианта ИНС основан на сравнении вариантов между собой по оценке прогноза и минимальной средней ошибке.

3.6. Основные результаты и выводы по главе

1. В III главе для исследуемых протоколов были определены угрозы системе связи с подвижными наземными объектами. В качестве показателя устойчивости системы связи, построенной на определенном протоколе было выбрано время функционирования системы до установленного факта взлома.

2. Были выбраны значимые параметры протоколов для последующего анализа с помощью метода анализа оценок. Проанализирована устойчивость структуры сети связи, зависящая от числа абонентов и радиуса ячейки конкретного протокола связи.

3. Разработанная методика обучения и выбора наилучшего варианта сети позволяет определить наилучшую структуру нейронной сети методом последовательного приближения к оптимальному варианту.

4. Для подтверждения теоретических положений далее необходимо провести имитационные эксперименты на ПК с помощью выбранного пакета

NeuroPro, работающего под управлением операционной системы MS Windows, позволяющего производить настройку и тестирование слоистых нейронных сетей, вычислять значимость входных сигналов, производить упрощение нейронной сети, а также проверку обучающего множества на непротиворечивость.

Глава 4

ПРОГНОЗИРОВАНИЕ УСТОЙЧИВОСТИ ФУНКЦИОНИРОВАНИЯ ОТКРЫТОЙ СИСТЕМЫ СВЯЗИ

4.1. Прогнозирование параметров устойчивости с помощью аппарата ИНС

В результате анализа таблиц 3.2 и 3.3 было определено множество параметров протоколов для организации беспроводной связи. В результате, после сбора информации, была сформирована таблица 4.1 со значимыми параметрами.

Время устойчивого функционирования протоколов для беспроводной системы связи было определено по дате опубликования методики их взлома, опубликованных в открытых источниках информации: СМИ и сети интернет. В случае отсутствия данных брался интервал до настоящего времени. По таблице 4.1 определяем количество входных нейронов – 11 (параметры протоколов), выходных – 1 шт. (время жизни протокола в годах). Далее с учетом вариации параметров была составлена обучающая выборка объемом 47 наборов (см. Приложение I).

Таблица 4.1. Основные параметры протоколов, влияющие на устойчивость функционирования беспроводных систем связи

Технология / Пара-метр (номер входа)	GSM (900/1800)	Wifi (802.11/802.11a)	Blue tooth	LTE	CDMA	DSRC	APCO-P25
Общее количество каналов (1)	124/374	14/38	79	200	64	До 5	512
Использу-емая полоса частот (2)	(895-915,935-960) МГц / (1710-1785, 1805-1880)	(2,4-2,4835) ГГц / (5,15-5,35, 5,65-6,425) ГГц	2,4-2,4835 ГГц	1,4-20 МГц	(824- 849) / (869 - 894) МГц	5,85-5,925 ГГц	(138-174, 406-512, 746-869) МГц

	МГц						
Мощность базовой станции (3)	2 Вт	2 Вт	100 мВт	20 Вт	2 Вт	100 мВт	100 Вт
Разнос каналов (4)	200 кГц	10 МГц	40-175 кГц	20 МГц	45 МГц	7,5 МГц	12,5 кГц
Идентифи-кация абонента (5)	Жесткий аппаратный ID	Аппаратный MAC и настраиваемый MAC	Аппаратный MAC и настраиваемый MAC	Жесткий аппаратный ID	Жесткий аппаратный ID	Аппаратный MAC и настраиваемый MAC	Жесткий аппаратный ID
Типичный радиус ячейки (6)	1-5 км	300 м	100 м	5-20 км	30 км	300 м	30 км
Зависимость от ландшафта (7)	Слабая/ сильная	Сильная	Сильная	Слабая	Слабая	Сильная	Слабая
Ограниче-ние по доступу (8)	Есть	Нет	Нет	Нет	Есть	Нет	Нет
Область применения связи (9)	Коммерческая	Не коммерческая	Не коммерческая	Коммерческая	Коммерческая	Не коммерческая	Коммерческая
Наличие шифрования (10)	Есть	Есть	Нет	Есть	Есть	Нет	Есть
Оплата за использова-ние (11)	Есть	Нет	Нет	Есть	Есть	Нет	Есть

Время живучести (выход)	(1991-2013) 22 года	(1991-2008) 17 лет	(2002-2006) 4 года	(2011-настоящее время) 25 лет	(1998-настоящее время) 25 лет	(2010-настоящее время) 20 лет	(1991-настоящее время) 25 лет

Таким образом, обучение нейронной сети проводится на обучающем множестве – наборе векторов данных, содержащих входные и соответствующие им выходные значения. Каждый сигнал с входов сети подается всем нейронам последующего слоя. В программе NeuroPro после нейронов выходного слоя строится слой адаптивных сумматоров с числом сумматоров, равным числу выходных сигналов, и с этих сумматоров снимаются выходные сигналы сети.

Перед подачей сети все входные сигналы нормируются в диапазон [-1;1], а сигналы выходных сумматоров нормируются в диапазон истинных значений выходных сигналов.

Минимизируется функция ошибки по всем векторам обучающего множества. Минимизация происходит путем такой подстройки изменяющихся параметров сети, чтобы сеть выдавала выходные сигналы, наиболее близкие к требуемым.

Эксперименты начинались со структуры ИНС вида 11/5/1 с последовательным усложнением. Анализ обучающей выборки показал отсутствие противоречивости.

Результаты расчетов с помощью NeuroPro сведены в таблицу 4.2. В качестве ошибки принято расхождение прогноза сети от ответа в определенном наборе исходных данных. Успех обучения показывает: сколько наборов в процентах приблизилось к прогнозируемым ИНС значениям с требуемой точностью.

Анализируя результаты экспериментов можно сделать следующие выводы.

1. Успешность обучения должна быть на уровне 87 %, который является максимальным для проверенных вариантов структур ИНС.

2. Добавление внутренних слоев не оказывает влияния на успешность обучения (табл. 4.2 четырехслойные варианты).

3. Увеличение количества нейронов во внутренних слоях не уменьшает ошибку.

4. Наилучшим решением можно считать вариант ИНС 11/8/1, минимизирующий среднюю ошибку до значения 1,798 с минимальным количеством циклов, необходимых для обучения: 52 шт.

В таблице 4.3 приведены результаты моделирования ИНС со структурой 11/8/1 для разных значений параметров *c* (3.11) для слоев. В некоторых литературных источниках [87, 88] из возможного диапазона изменения крутизны 0,0001…1 рекомендуется выбирать значения, близкие к единице, но это, теоретически, должно приводить к увеличению числа циклов обучения. Сеть обучалась (с дообучением) до достижения значения успеха не менее 46/47 (или 98 %), или до исчерпания 5 000 циклов обучения.

Из таблицы 4.3 можно сделать выводы: для исследуемой ИНС параметр крутизны должен составлять менее 0,1; количество команд на дообучение ИНС возрастает с уменьшением параметра *c*.

В таблицах 4.2 и 4.3 приведены значения, полученные для метода сопряженных градиентов при оптимизации ошибки (как начальный).

Последним фактором варьирования в процессе настройки ИНС является метод оптимизации ошибки. В работе были исследованы методы: градиентного спуска, параллельных касательных, сопряженных градиентов и BFGS. Исследованы только наилучшие варианты сетей со структурой 11/8/1 из таблицы 4.3. Результаты моделирования приведены в таблице 4.4. Подчеркнутые значения параметров для тех вариантов ИНС, для которых успех обучения составил 100%.

Наилучшими для решаемой задачи оказались методы: сопряженных градиентов и BFGS. Остальные методы – малоэффективны из-за наличия недостатков, изложенных во II главе работы.

На рисунке 4.1 имеется возможность сравнить варианты ИНС при выборе метода оптимизации ошибки. На диаграмме размер окружности соответствует количеству циклов обучения. Наилучшим считаем вариант, выделенный жирным в таблице 4.4, для которого максимальная ошибка минимальна.

Настроенная на 100 % ИНС в дальнейшем позволяет определить по параметрам беспроводного протокола время до взлома системы беспроводной связи на их основе с подвижными объектами с минимально возможной ошибкой.

Таблица 4.2. Результаты расчетов различных вариантов ИНС (при крутизне сигмоиды c = 0,9 и e = ±2 %)

Вариант ИНС	Циклов обучения	Успешность обучения, %	Средняя ошибка	Максимальная ошибка
Трехслойные варианты				
11/5/1	220	87	2,011	9,39
11/6/1	107	85	2,054	9,46
11/7/1	337	60	2,201	9,48
11/8/1	**52**	**87**	**1,798**	**9,54**
11/9/1	109	87	2,022	9,46
11/10/1	136	87	1,944	9,48
11/11/1	112	87	1,920	9,50
11/12/1	186	87	1,992	9,44
11/13/1	105	87	1,978	9,43
11/14/1	86	85	1,999	9,48
11/15/1	199	85	2,000	9,49
11/16/1	107	55	2,155	9,46
Четырехслойные варианты				
11/5/5/1	671	38	2,298	9,38
11/6/6/1	242	40	2,189	9,45
11/7/7/1	97	43	2,169	9,56
11/8/8/1	205	77	1,943	9,56
11/9/9/1	116	60	2,146	9,48
11/10/10/1	208	83	2,050	9,53
11/11/11/1	292	87	2,030	9,51
11/12/12/1	124	85	1,965	9,47
11/13/13/1	194	64	2,150	9,48
11/14/14/1	180	85	2,046	9,48
11/15/15/1	225	85	2,009	9,42

Таблица 4.3. Результаты расчетов для ИНС 11/8/1 с разными значениями крутизны сигмоидальных функций (e = ±2 %)

Значение параметра крутизны			Циклов обучения	Успешность обучения, %	Средняя ошибка	Максимальная ошибка
Во вх. слое	В скрытом слое	В вых. слое				
0,001	0,0001	0,0001	5000	87	1,469	4,30
0,0001	0,001	0,001	5000	75	1,724	10,39
0,0001	0,0001	0,001	5000	87	1,825	9,63
0,0001	0,001	0,0001	5000	43	2,689	8,40
0,0001	0,0001	0,001	5000	87	1,733	9,62
0,0001	0,0001	0,0001	5000	72	2,538	17,12
0,001	0,01	0,001	5000	89	1,824	3,97
0,001	**0,01**	**0,01**	**740**	**100**	**1,560**	**1,98**
0,001	0,001	0,01	5000	87	1,814	9,62
0,001	0,001	0,001	5000	75	1,808	10,40
0,01	0,01	0,01	5000	72	1,225	3,87
0,01	0,01	0,1	3250	98	1,149	2,22
0,01	0,1	0,01	1150	100	1,145	2,00
0,01	0,1	0,1	1100	100	1,499	2,00
0,1	0,01	0,01	5000	87	1,595	5,60
0,1	0,01	0,1	3550	98	1,332	2,82
0,1	0,1	0,01	5000	77	1,510	3,78
0,1	0,1	0,1	5000	77	1,620	4,60
0,1	0,1	0,5	5000	51	1,889	5,88
0,1	0,5	0,1	5000	79	1,477	4,25
0,1	0,5	0,5	5000	87	1,902	8,20
0,5	0,1	0,1	5000	62	1,607	5,14
0,5	0,1	0,5	5000	87	1,926	8,73
0,5	0,5	0,1	5000	70	1,752	5,81
0,5	0,5	0,5	5000	85	1,855	9,19
0,1	0,5	0,9	5000	74	1,700	8,30
0,1	0,1	0,9	5000	51	1,803	5,46
0,5	0,5	0,9	5000	85	1,875	9,19

0,1	0,9	0,1	5000	64	1,508	4,75
0,1	0,9	0,5	5000	70	1,909	7,52
0,1	0,9	0,9	5000	85	1,744	8,45
0,9	0,5	0,1	5000	74	1,796	6,57
0,9	0,5	0,9	5000	87	1,881	9,28
0,9	0,1	0,9	5000	60	2,008	9,14
0,9	0,9	0,9	5000	87	1,899	9,41

Таблица 4.4. Результаты расчетов для ИНС 11/8/1 с разными методами оптимизации (e = ±2 %)

Метод оптимизации	Значение параметра крутизны			Циклов обучения	Успешность обучения, %	Средняя ошибка	Макси-мальная ошибка
	Во вх. слое	В скры-том слое	В вых. слое				
Градиентный спуск	0,001	0,01	0,01	5000	91	1,815	7,71
	0,01	0,01	0,1	5000	83	1,675	6,62
	0,01	0,1	0,01	5000	72	1,809	6,95
	0,01	0,1	0,1	5000	87	1,785	7,12
	0,1	0,01	0,1	5000	83	1,776	7,20
Параллельных касательных	0,001	0,01	0,01	5000	74	1,922	7,00
	0,01	0,01	0,1	5000	74	1,447	6,07
	0,01	0,1	0,01	5000	72	1,667	6,16
	0,01	0,1	0,1	5000	49	1,721	3,90
	0,1	0,01	0,1	5000	43	2,017	5,86
Сопряженных градиентов	0,001	0,01	0,01	5000	87	1,591	9,62
	0,01	0,01	0,1	2980	100	1,412	1,99
	0,01	0,1	0,01	5000	47	1,672	3,77
	0,01	0,1	0,1	2437	100	1,387	2,00
	0,1	0,01	0,1	2042	100	1,341	2,00
BFGS	**0,001**	**0,01**	**0,01**	**524**	**100**	**1,017**	**1,65**
	0,01	0,01	0,1	1747	100	1,249	1,99

	0,01	0,1	0,01	5000	51	1,618	3,15
	0,01	0,1	0,1	425	100	1,324	1,99
	0,1	0,01	0,1	2343	100	1,123	1,97

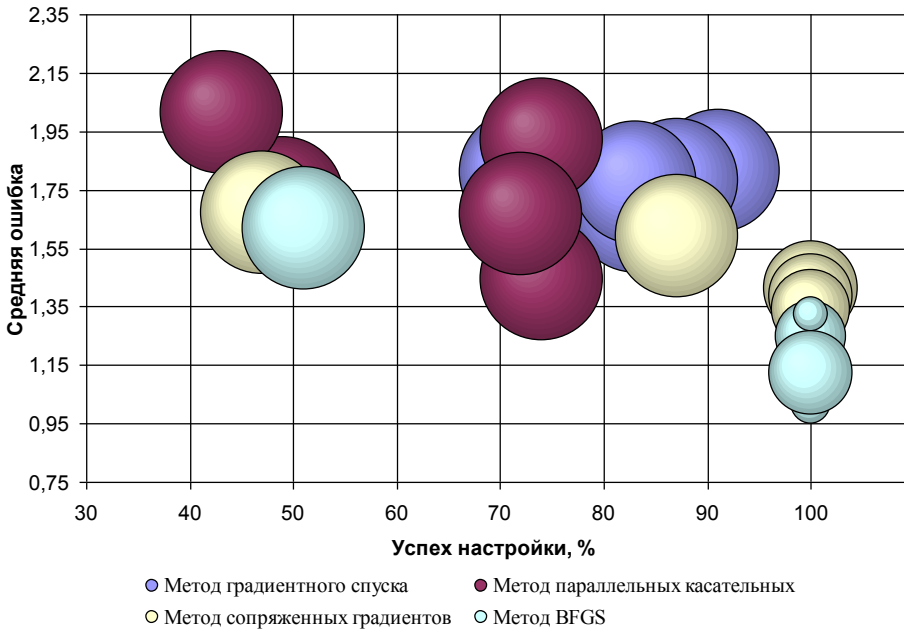


Рисунок 4.1. Сравнение вариантов ИНС на этапе выбора метода оптимизации

Не смотря на то, что в программах по исследованию ИНС имеются средства оценки значимости элементов ее структуры, решить какие компоненты (нейроны, связи) можно исключить – сложная задача. Известны методики организации процессов свертки ИНС, но они заслуживают отдельного рассмотрения, и в моей работе не описывались. Так как при принудительном обращении в ноль отбрасываемого компонента исключается корреляция с другими данными, то правильнее заменить исключаемые компоненты на функцию от оставшихся, что крайне затруднительно для большего числа задач.

С помощью программы NeuroPro была сделана оценка значимости входов ИНС. Результаты приведены на рисунке 4.2. Из рисунка видно, что на решение сети сильнее всего влияют (с вероятностью больше 50 %) разнос каналов, идентификация абонентов, ограничение по доступу и наличие шифрования.

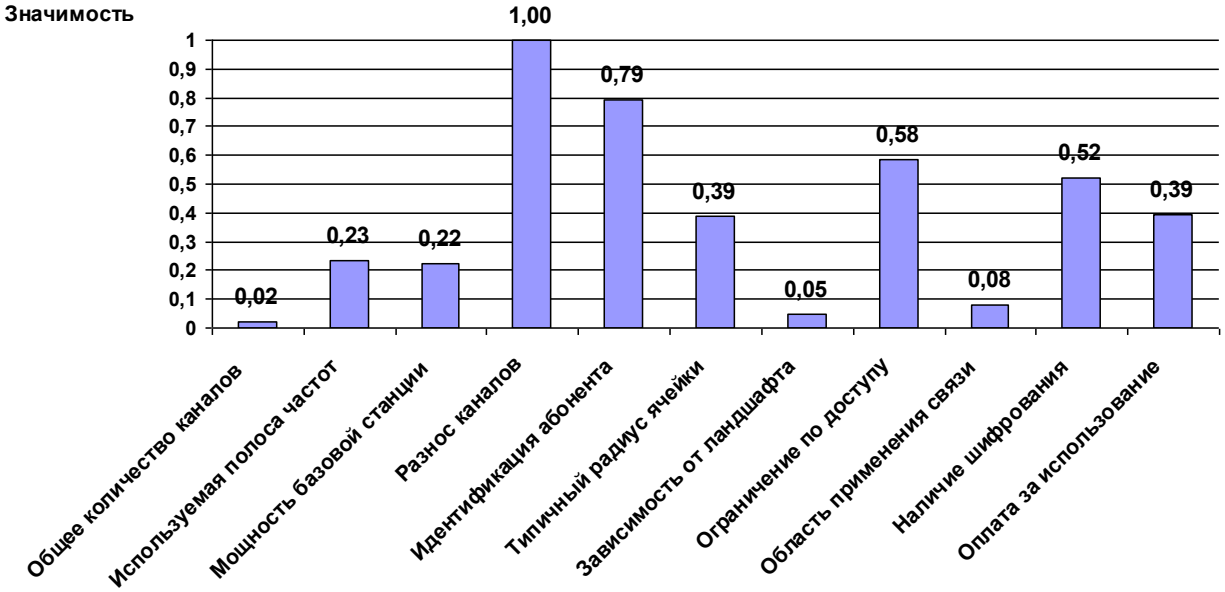


Рисунок 4.2. Оценка значимости входов ИНС

4.2. Прогнозирование устойчивости структуры сети

Для проведения экспериментов использовалась несколько другая методика подбора параметров ИНС, нежели описанная в п. 4.1 из-за того, что выход ИНС – дискретный.

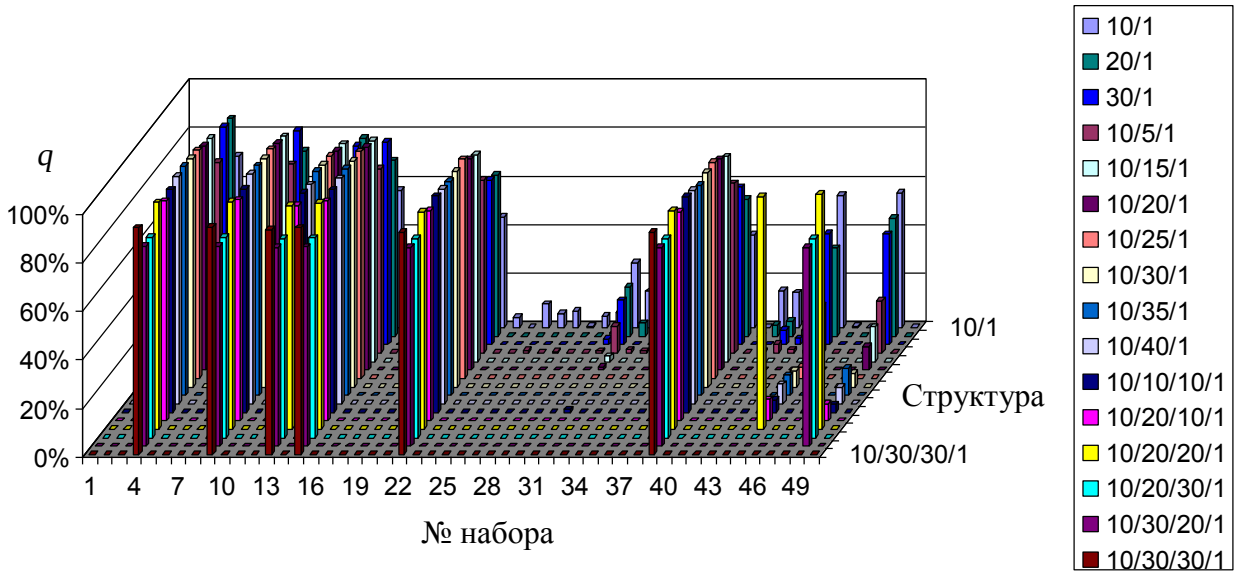
С помощью разработанного алгоритма, изображенного на рис. 3.7, было сгенерировано 50 наборов обучающего множества при протяженности линии связи 300 м (см. Приложение II). Номера входов ИНС обозначены в соответствии с таблицей 4.5.

Таблица 4.5. Соответствие параметров задачи входам ИНС

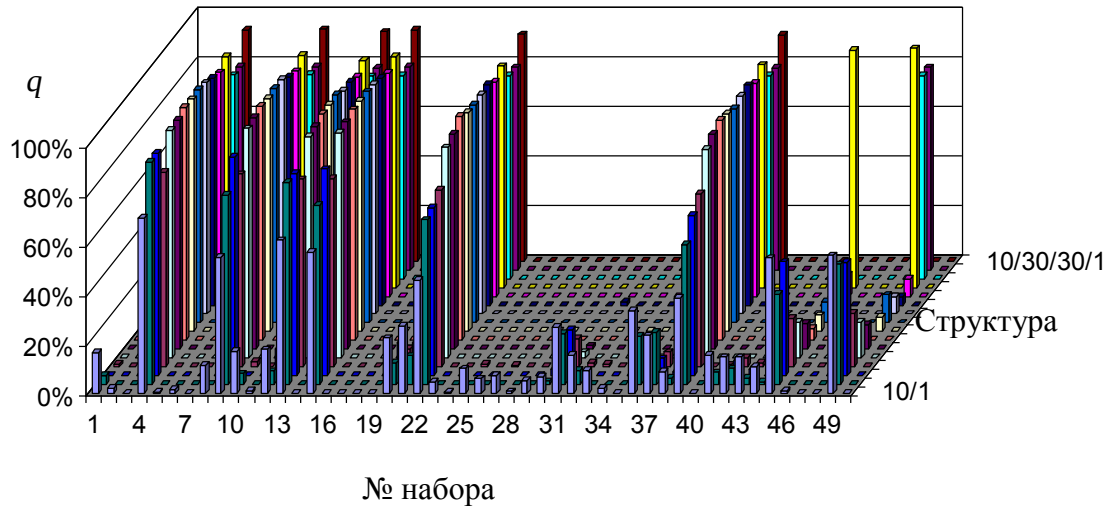
Число занятых каналов	N_1	N_2	N_3	N_4	N_{12}	N_{23}	N_{34}	N_{123}	N_{234}	N_{1234}
Номер входа ИНС	1	2	3	4	5	6	7	8	9	10

Проверка работы ИНС с разным количеством слоев выполнялась с помощью того же обучающего множества только без выходного значения. На выходе ИНС формировался прогноз в процентах.

В результате проведенных экспериментов полученные данные представлены в виде гистограмм при крутизне сигмоид $c = 0{,}9$ и $e = \pm 1$ % (см. Рисунок 4.3). Качество прогнозирования настроенной ИНС контролировалось подсчетом ошибок – ложных срабатываний. Исходя из анализа обучающего множества (см. Приложение II) отказы в обслуживании сети (q) должны наблюдаться в наборах №№ 4, 13, 15, 22 и 39. Как видно из рисунка 4.3, количество ложных срабатываний больше при меньшем числе нейронов в структуре, но они происходят с меньшей вероятностью, и, наоборот, при большем числе нейронов количество ложных срабатываний меньше: у ИНС со структурой 10/30/30/1 – всего одно (девятый набор), но с вероятностью 92 %.



а)



б)

Рисунок 4.3. Гистограмма ((б) – обратный порядок структур ИНС)

Далее подбирались значения крутизны сигмоидов, с использованием методики, аналогичной описанной ранее; метод оптимизации BFGS выбран как наилучший. Результаты исследований представлены в таблице 4.6 после 1000 циклов обучения (подчеркнуты лучшие варианты, жирным выделен оптимальный вариант). Из данного исследования можно сделать вывод: наилучшее обучение ИНС происходит при значениях крутизны 0,1; 0,01 и 0,1, что позволяет на выходе добиться 6 % неуверенного прогноза и 2 % – неправильного; это соответствует трем и одному набору соответственно. Хорошим результатом можно считать значения крутизны, занимающие нижнюю половину таблицы 4.6. Здесь достигается достоверность 93,1 %, что соответствует 10 % неуверенного прогноза и 2 % – неправильного; это соответствует пяти и одному набору соответственно. Последний результат проиллюстрирован на рис. 4.3.

Таблица 4.6. Результаты расчетов для ИНС 10/30/30/1 с разными значениями крутизны сигмоидальных функций (метод оптимизации BFGS, e = ±1 %)

Значение параметра крутизны			Достоверность классов решений, %	Оценка прогноза, %		
Во вх. слое	В скрытых слоях	В вых. слое		Правильно	Неуверенно	Неправильно
0,001	0,0001	0,0001	93,1	88	10	2
0,0001	0,001	0,001	24,4	70	10	20
0,0001	0,0001	0,001	50,1	0	90	10
0,0001	0,001	0,0001	63,2	82	10	8
0,0001	0,0001	0,001	50,3	0	90	10
0,0001	0,0001	0,0001	50,3	0	90	10
0,001	0,01	0,001	50,3	0	90	10
0,001	0,01	0,01	50,3	0	90	10
0,001	0,001	0,01	50,3	0	90	10
0,001	0,001	0,001	50,3	0	90	10
0,01	0,01	0,01	93,1	88	10	2
0,01	0,01	0,1	50,3	0	90	10
0,01	0,1	0,01	19,5	68	10	22
0,01	0,1	0,1	93,1	88	10	2
0,1	0,01	0,01	93,1	88	10	2
0,1	**0,01**	**0,1**	**98**	**92**	**6**	**2**
0,1	0,1	0,01	93,1	88	10	2
0,1	0,1	0,1	93,1	88	10	2
0,1	0,1	0,5	93,1	88	10	2
0,1	0,5	0,1	93,1	88	10	2
0,1	0,5	0,5	93,1	88	10	2
0,5	0,1	0,1	93,1	88	10	2
0,5	0,1	0,5	93,1	88	10	2
0,5	0,5	0,1	93,1	88	10	2
0,5	0,5	0,5	93,1	88	10	2
0,1	0,5	0,9	82,1	86	10	4

0,1	0,1	0,9	93,1	88	10	2
0,5	0,5	0,9	50,3	0	90	10
0,1	0,9	0,1	93,1	88	10	2
0,1	0,9	0,5	93,1	88	10	2
0,1	0,9	0,9	93,1	88	10	2
0,9	0,5	0,1	93,1	88	10	2
0,9	0,5	0,9	50,3	0	90	10
0,9	0,1	0,9	93,1	88	10	2
0,9	0,9	0,9	93,1	88	10	2

С помощью программы NeuroPro была сделана оценка значимости входов ИНС. Результаты приведены в таблице 4.7 и на рисунке 4.4. Из рисунка видно, что на решение сети сильнее всего влияют (с вероятностью больше 50 %) количество мобильных станций в зоне покрытия БС3, БС4, БС2 и БС3 одновременно, БС1, БС2 и БС3 одновременно. Как и предсказывалось, мобильные станции, находящиеся в зоне действия сразу нескольких БС, сильнее влияют на вероятность отказа в доступе, чем находящиеся только в зоне действия одной БС.

Таблица 4.7. Полученные значения значимости входов ИНС со структурой 10/30/30/1

Число занятых каналов	N_1	N_2	N_3	N_4	N_{12}	N_{23}	N_{34}	N_{123}	N_{234}
Значимость	0,018	0,296	0,546	0,753	0,191	0,737	0,221	1	0,096

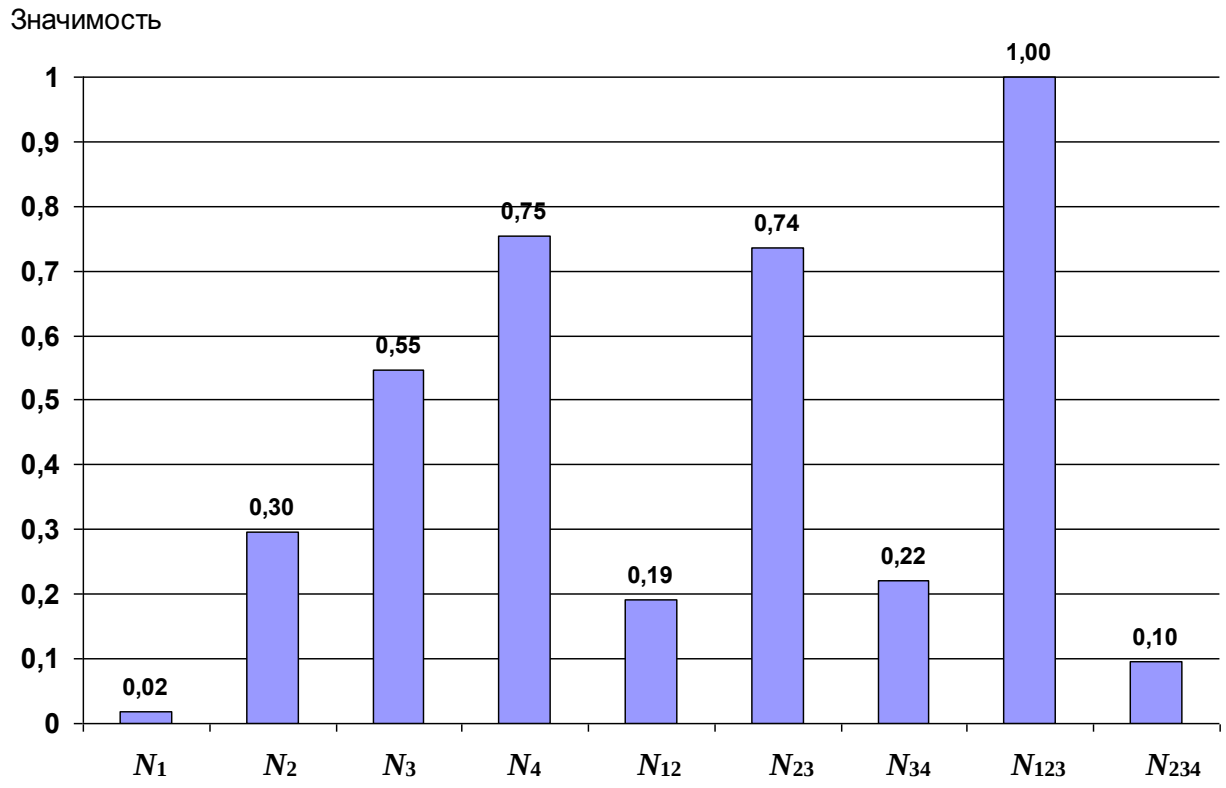


Рисунок 4.4. Оценка значимости входов ИНС со структурой 10/30/30/1

4.3. Апробация разработанной методики на протоколе NFC

Технология беспроводной связи ***NFC*** (Near Field Communication) для высокочастотной связи малого радиуса действия (см. Рисунок 4.5) разработана сравнительно недавно, в 2003г. Является аналогом технологий BlueTooth и Zigbee. Максимальная скорость передачи данных 424 кбит/с осуществляется на не требующем лицензирования диапазоне частот 13,56 МГц на расстоянии до 0,2 м [89-92]. То есть используется ближняя зона, в отличие от описанных в первой главе технологий. Для повышения надежности передачи данных используется Манчестерский, NRZ-L (non-return-to-zero level) – уровень кодирования без возврата к нулю, или модифицированный код Миллера. Канал передачи является плохо защищенным. Скорость передачи данных зависит от метода кодирования и от расстояния между устройствами (максимальная скорость достигается при дистанции до 4 см).

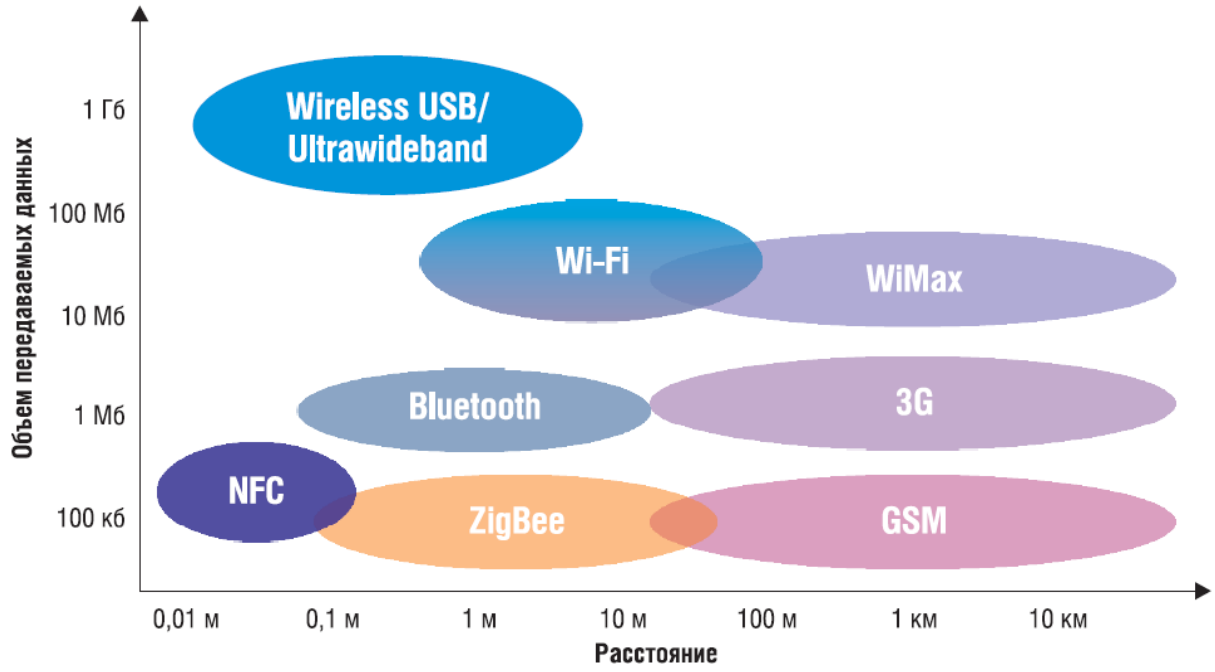


Рисунок 4.5. Области действия беспроводных протоколов

Типовая ширина занимаемой полосы частот (F_c) составляет 14 кГц, которая может быть расширена до 3,6 МГц. Новые устройства на основе NFC могут осуществлять передачу на двукратной скорости 848 Кбит/с. Дальнейшее усовершенствование технологии направлено на повышение скорости до 6,8 Мбит/с.

На основе технологии NFC возможны два режима работы: пассивный и активный. При пассивном режиме переносное устройство (метка, брелок) не получает питания от аккумулятора, а использует ток, полученный от антенны. При этом используется модуляция данных на поднесущей частоте 848 кГц (см. табл. 4.8) [93-98].

Основной режим работы при технологии NFC – полудуплексный при котором инициатор производит опрос устройств, посылая запрос. Находящееся рядом с ним целевое устройство принимает сигналы от инициатора и отвечают. Передача данных происходит только в том случае, если отсутствуют другие передачи.

Дополнительными режимами являются: чтение/запись, точка-точка, эмуляция карт. Причем чтение/запись может производиться как пассивными, так

и активными устройствами при осуществлении сеанса связи инициатор-целевое устройство. В режиме точка-точка устанавливается связь для обмена данными между однотипными устройствами. В этом случае и инициатор и целевое устройство работают в режиме приема-передачи и мощность устройств увеличивается до сотен милливатт. Дальность связи при этом может достигать уже нескольких метров (3…10). Это дает дополнительные возможности злоумышленнику при реализации атак [99, 100].

Режим эмуляции карт – считывание данных кредитной карты или метки.

Таблица 4.8. – Параметры стандартов NFC

Стандарт	Тип устройства	Вид кодирования	Скорость передачи данных, Кбит/с	Несущая частота, МГц
NFC-A	Инициатор	Код Миллера	106	13,56
	Целевое	Манчестер	106	13,56 848 кГц поднесущая
NFC-B	Инициатор	NRZ-L	106	13,56
	Целевое	NRZ-L	106	13,56 848 кГц поднесущая
NFC-F	Инициатор	Манчестер	212/424	13,56
	Целевое	Манчестер	212/424	13,56

Технология NFC проходит в нашей стране сертификацию в момент написания данной работы [101, 102].

NFC регламентируется стандартом ECMA 340 Европейской ассоциации стандартизации информационно-коммуникационных систем. Интерфейс и протокол NFCIP-1 принят NXP, Phillips MIFARE и Infineon как 18092.

Недостатками технологии NFC являются:

− низкая скорость передачи данных (на практике считывание 15 КБ данных занимает примерно 20 с);

− низкая защищенность данных (отсутствие шифрования данных) – возможность перехвата передаваемой информации с помощью направленных антенн, подмены клиентских данных и передачи ложной информации от злоумышленника, глушения приемника;

− малый объем памяти хранения данных в пассивных метках – 144 байт, (реже 4 КБ);

− отсутствие совместимости у различных производителей ПО для формата NFC.

Основными достоинствами протокола являются:

− бесконтактная передача данных на небольшие расстояния;

− низкая потребляемая мощность;

− низкая стоимость расходных материалов.

Поэтому при передаче данных протокол NFC используется производителями для поиска и установки соединения устройств, а сама передача данных ведется с помощью протоколов WiFi, или Wi-Fi Direct, или по Blue tooth [90, 91, 103].

Настроенная в п. 4.1 на 100 % ИНС позволяет спрогнозировать по параметрам беспроводного протокола время до взлома системы связи, поэтому на ее вход были поданы параметры, присущие для технологии NFC (см. табл. 4.9).

Таблица 4.9. – Исходные данные для прогнозирования устойчивости протокола NFC

Номера входов ИНС											**Выход ИНС**
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	
1	14	200	0	1	10	1	1	0	1	0	X

На 100% обученной ИНС со структурой 11/8/1 вышло, что протокол NFC будет взломан через 23,5 года с точностью ±2%, или время его использования рекомендовано до 2026…2027 года.

4.4. Основные результаты и выводы по четвертой главе

В четвертой главе моей диссертационной работы были проведены имитационные эксперименты на ПК с целью подтверждения теоретических положений и разработанной методики. По четвертой главе можно сделать следующие выводы.

1. С помощью разработанной методики была обучена искусственная нейронная сеть для решения задачи прогнозирования устойчивости – времени до взлома протокола для беспроводной системы связи. При настройке нейронной сети решался комплекс оптимизационных задач в результате чего была определено количество нейронов, количество слоев, вид сжимающей функции и ее параметр крутизны, тип алгоритма оптимизации ошибки сети при обучении методом обратного распространения ошибки. На выходе нейронной сети было получено значение вероятного времени взлома внедряемого в настоящее время протокола NFC для высокочастотной связи малого радиуса действия. В результате дообучения, сеть удалось обучить на 100%.

2. Расчет значимости входов сигналов искусственной нейронной сети показал, что на решение сети сильнее всего влияют параметры протокола: разнос каналов, идентификация абонентов, ограничение по доступу и наличие шифрования.

3. Оценка устойчивости структуры открытого протокола на примере технологии для беспроводной связи WiFi 802.11 была произведена с помощью аппарата нейронных сетей с использованием разработанного алгоритма для формирования обучающего множества. С помощью полученного множества была произведена настройка нейронной сети, а затем были получены значения прогноза отказа протокола из-за превышения числа смоделированных пользователей. Отказ в доступе к системе связи быстрее наступает при увеличении числа пользователей в особенности тех, которые находятся в зоне покрытия сразу нескольких станций.

4. В целом проведенные эксперименты показали возможность достижения цели, поставленной в работе.

Заключение

В моей работе была поставлена цель: разработать алгоритмы и методику для прогнозирования целесообразности использования компонентов беспроводных сетей для определения устойчивости системы связи с подвижными наземными объектами на этапе их разработки. Так как разработка систем связи ведется с использованием известных протоколов, или их модификаций, то учет всех параметров компонентов представляет сложную задачу.

В диссертационной работе была решена научно-техническая задача прогнозирования целесообразности использования компонентов беспроводных сетей на основе анализа показателей устойчивости системы связи: времени устойчивого функционирования до разработки методики взлома технологии беспроводной системы связи и структурной устойчивости сети, построенной на открытом протоколе.

Прогнозирование показателей устойчивости осуществлялось с применением теорий множеств, графов, искусственных нейронных сетей, вероятности и математической статистики.

В результате проведенных исследований и экспериментов в диссертационной работе получены следующие результаты.

1. Исследованы особенности, современное состояние и перспективы развития беспроводных систем связи с наземными подвижными объектами.

2. Проведена оценка применимости открытых и закрытых протоколов связи для целей, сформулированных в диссертации. Показано, что использование закрытых технологий для систем радиосвязи, не смотря на их высокую защищенность, не подходит для систем связи с наземными подвижными объектами из-за возможности реализации угроз типа DDOS. Использование же открытых протоколов сопряжено с их ограничениями по зоне покрытия и количеству мобильных абонентов, а также множеству характеристик протоколов, требующих детального анализа влияния их друг на друга. Для этого необходимо привлечение коллектива специалистов

определенной предметной области.

3. Анализ методов, пригодных для решения задач работы, показал, что аппарат искусственных нейронных сетей подходит наилучшим образом. Во-первых, он позволяет находить сложные зависимости между переменными задачи без решения сложных вероятностных уравнений. Во-вторых, обладает свойством обучения, что позволяет достаточно быстро настроиться на специфику решаемой задачи. В-третьих, не требует от пользователя специальных знаний предметной области, доступных только экспертам. С другой стороны, аппарат нейронных сетей не лишен недостатков. Среди них основными являются: необходимость разработки методики обучения с подбором параметров нейронной сети правильно оптимизирующих функцию ошибки; неопределенность при построении структуры сети, вследствие чего необходимо проведение многочисленных экспериментов на каждой стадии настройки сети, а также возможность ее недообучения и переобучения. Постанализ полученной структуры нейронной сети требует еще больших вычислительных и временных затрат. Метод анализа оценок также имеет положительные стороны, такие, как высокая скорость принятия решений и простота. Недостатком является возможность расслоения решений на рассогласованные и противоположные варианты.

4. Анализ структуры сети беспроводной системы связи является также сложной задачей из-за влияния на работу мобильной станции как ландшафта реальной местности, так и параметров протокола связи. Основной проблемой при наличии связи мобильных станций как с базовыми станциями, так и с другими пользователями, является возможный отказ в обслуживании из-за превышения максимального числа каналов.

5. В работе разработана формальная процедура, в которой метод анализа оценок использован для выбора значимых параметров технологий для организации беспроводной связи, а для прогнозирования параметров устойчивости – аппарат искусственных нейронных сетей.

6. Разработанные алгоритмы для обучения искусственной нейронной сети

методом последовательного приближения позволила решить задачу неопределенности при настройке и подборе ее параметров. Разработанная методика является универсальным средством для решения комплексных задач анализа и прогнозирования устойчивости функционирования сложных многосвязных систем.

7. В результате применения разработанной методики были получены оптимальные параметры сети: количество слоев – 3, 11 нейронов во входном слое, 8 – в скрытом, 1 – в выходном слое; метод оптимизации ошибки при обучении по методу обратного распространения ошибки – BFGS, а также оптимальные параметры крутизны сжимающей функции. При 2% точности искусственную нейронную сеть удалось настроить на 100%. Полностью обученная сеть была использована для прогнозирования времени до официального взлома технологии NFC, активно внедряемой некоторыми промышленными производителями мобильных устройств, например, Apple и Samsung. Получено значение прогноза 23,5 года с учетом параметров протокола. разработан метод оценки защищенности систем связи с наземными подвижными объектами. Это позволило на стадии разработки систем повысить скорость и объективность производимого анализа, снизить трудозатраты на 15% относительно традиционной методики с использованием специалистов.

8. Для анализа структурной устойчивости, на примере протокола WiFi 802.11, для которого $R_{\max} = 14$ каналов, был разработан алгоритм для формирования обучающей выборки. Затем, с помощью разработанной методики, осуществлена настройка искусственной нейронной сети с полученными: 4-х слойной структурой с 30 нейронами в двух скрытых слоях, 10 нейронами на входе и одним на выходе; достоверностью классов решений 98% и с оценкой правильности решений 92%.

9. Разработан метод определения показателей защищенности систем связи с наземными подвижными объектами. Это позволило на стадии разработки систем повысить скорость и объективность производимого анализа, снизить трудозатраты на 15% относительно традиционной методики.

10. Разработан алгоритм настройки искусственных нейронных сетей для определения показателей защищенности систем связи, который позволяет подстраивать веса нейронов в соответствии с решаемой задачей, повышая точность прогноза и снижая ее время обучения на 20 %.

11. Разработан алгоритм прогнозирования устойчивости беспроводной сети в изменяющихся условиях, который отличается от известных подходов сокращением времени получения пользователем необходимых данных.

12. После настройки сети в обоих случаях была проведена проверка избыточности сети, которая подтвердила оптимальность структуры. Оценка значимости входов показала, что набор подаваемых на вход нейронной сети является полным, а задачник – непротиворечивый.

Необходимо отметить, что поскольку имитационная модель описывает ландшафт и распределение пользователей по виртуальной территории, которая отличается от реальной, то проверка адекватности в классическом виде не представляется возможным. В моей работе проверка адекватности осуществлялась путем проведения имитационного эксперимента.

Таким образом, можно сделать итоговый вывод, что все поставленные задачи работы были выполнены, а предложенные метод и алгоритмы могут быть использованы для ускорения получения оценки прогноза без привлечения экспертов, а также при изменении компонентов для систем связи с наземными подвижными объектами, например при создании новых протоколов. Разработанные алгоритмы и метод в целом позволяют сократить время анализа защищенности беспроводных систем связи, построенных на базе известных и вновь разрабатываемых протоколов передачи информации, а также проводить мониторинг систем связи при изменении оперативной обстановки.

Список литературы

1. Змитрович А.И. Интеллектуальные информационные системы. – Минск: – ТетраСистемс, 1997. – 368 с.

2. Щербаков В.Б.. Безопасность беспроводных сетей: стандарт IEEE 802.11/ В.Б. Щербаков, С.А. Ермаков. – М.: РадиоСофт, 2010. – 255с.

3. Гордейчик С.В. Безопасность беспроводных сетей/ С.В. Гордейчик, В.В. Дубровин - М.: Горячая линия - Телеком, 2008. – 288с.

4. Пролетарский А.В. Беспроводные сети Wi-Fi / А.В. Пролетарский, И.В. Баскаков, Д. Н. Чирков – М.: БИНОМ, 2007. – 178 с.

5. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. / [Электронный ресурс]: https://docs.cntd.ru/document/1200058320. Дата обращения [15.02.2015].

6. Белорусов Д.И., Корешков М.С. WIFI-сети и угрозы информационной безопасности // Специальная техника. 2009. № 6. С. 2–6.

7. Борисов В.И., Щербаков В.Б., Ермаков С.А. Спектр уязвимостей беспроводных сетей стандарта IEEE 802.11 // Информация и безопасность. 2008. Т. 11. № 3. С. 431–434.

8. habrahabr.ru [Электронный ресурс] / Сайт для публикации новостей, статей, связанных с информационными технологиями, бизнесом и Интернетом.

9. cisco.com [Электронный ресурс] / Сайт компании Cisco Systems, Inc., специализирующейся в области сетевых технологий.

10. Стив Такер Цифровая радиосвязь в стандарте APCO 25./ [Электронный ресурс] http://www.xserver.ru/computer/sv/radiost/4/.

11. Бабков В.Ю., Цикин И.А. Сотовые системы мобильной радиосвязи – 2-е изд., перераб. и доп. – СПб.: БХВ-Петербург, 2013. – 432 с.

12. Новые сетевые технологии в системах управления военного назначения / Под редакцией Н.И. Буренина. – СПб: Военная академия связи имени Маршала Советского Союза С. М. Будённого, 2000. – 200 с.

13. Емельянов В.В., Курейчик В.М., Курейчик В.В. Теория и практика эволюционного моделирования. – М.: ФИЗМАТЛИТ, 2003. – 432 с.

14. Малик А.А. Информационная безопасность: концептуальные и методологические основы защиты информации /А.А. Малик.- М.: ИНФРА-М, 2004.-282с.

15. Мельников В.П. Информационная безопасность и защита информации В.П. Мельников, С.А. Клейменов, А.М. Петраков – 3-е изд., стер. – М.: Академия, 2008. – 336 с.

16. Сидорин Ю.С. Технические средства защиты информации / Ю.С. Сидорин. – СП. : Издательство Политехнического института, 2005. – 108 с.

17. Салома Арто. Криптография с открытым ключом / Арто Салома.-М.: Мир, 1995. – 320с.

18. Шнайер Б. Секреты и ложь. Безопасность данных в цифровом мире / Б. Шнайер.-СПб.: Питер, 2003.- 370 с.

19. Громаков Ю.А. Сотовые системы подвижной радиосвязи. Технологии электронныхкоммуникаций Т. 48. / Ю.А. Громаков. – М. : Эко-Трендз,1994 – 205 с.

20. A Related-Key Rectangle Attack on the Full KASUMI, Eli Biham, Orr Dunkelman, Nathan Keller, 2005, p 14.

21.Карманов А.Г., Бондаренко И.Б., Чжао Л., Ткачев К.О. Оценка живучести сложных информационных систем связи с подвижными объектами// Информация и Космос, №3 – 2015. – 180с., стр. 36-41.

22. Каган Б.М., Долкарт В.М., Каневский М.М. Управляющий вычислительный комплекс с автоматической реконфигурацией для ответственных АСУ ТП // В кн.: Кибернетические проблемы АСУ ТП. Материалы семинара. - М.: Знание, МДНТП,-1978. С. 3-11.

23. Надежность систем энергетики: Терминология. Сборник рекомендуемых терминов. - Вып. 95. - М.: Наука, 1980. - 42 с.

24. Руденко Б.Н., Ушаков И.Н. Надежность систем энергетики. -М.: Наука, 1986. - 252 с.

25. Рябинин И. А. Теоретические основы проектирования ЭЭС кораблей. - Ленинград: Воен.-мор. ордена Ленина акад., 1964.- 240 с.

26. Словарь по кибернетике/ Под ред. В.М.Глушкова. - Киев: Гл. , ред. Укр. сов. энциклопедии, 1979.

27. Горшков В.В. Логико-вероятностный метод расчета живучести сложных систем. - Кибернетика АН УССР.-1982. -№ 1. - С. 104-107.

28. Волик Б.Г., Рябинин Й.А. Эффективность, надежность и живучесть управляющих систем // Автоматика и телемеханика. -1984.- № 12.

29. Надежность, в технических системах. Справочник/ Под ред. И.Н.Ушакова. - М.: Радио и связь, 1985. - 606 с.

30. Рябинин И.А., Парфенов Ю.Н. Надежность и эффективность структуры сложных технических систем // В кн.: Основные вопросы теории и практики надежности. - Минск: Наука и техника, 1982. -С 25-40.

31. Рябинин И.А., Черкесов Г.Н. Логико-вероятностные методы исследования надежности структурно-сложных систем. - М.: Радио и связь, 1984. – 238 с.

32. Астров В.В., Симаков И.П., Черкесов Г.Н. Применение методов вероятностной логики и исследования операций к анализу живучести пространственно распределенных энергетических систем. // В кн.: Методические вопросы исследования надежности больших систем энергетики. – Вып. 20. - Иркутск: СЭИ С0 АН СССР, 1980. - С. 32-42.

33. Г.Н.Черкесов. Методы и модели оценки живучести сложных систем. – М.: Знание, 1987. – 35 с.

34. Синтез и анализ живучести сетевых систем: монография / Ю.Ю. Громов, В.О. Драчев, К.А. Набатов, О.Г. Иванова. – М.: «Издательство Машиностроение-1», 2007. – 152с.

35. Орлов А.И. Экспертные оценки. // Заводская лаборатория. − 1996. − Т. 62. − №1. − С. 54-60.

36. Орлов А.И. Экспертные оценки. Учеб. пособие. – М.: 2002.

37. Бешелев С.Д., Гурвич Ф.Г. Экспертные оценки в принятии плановых решений. Учеб. пособие. – М.: Экономика, 1976. − 287 с.

38. Евланов Л.Г., Кутузов В.А. Экспертные оценки в управлении. – М.: Экономика, 1978. − 133 с.

39. Менеджмент. Учеб. пособие. / Под ред. Ж.В. Прокофьевой. – М.: Знание, 2000. – 288 с.

40. Бешелев С.Д., Гурвич Ф.Г. Экспертные оценки. – М.: Наука, 1973. – 79 с.

41. Статистические методы анализа экспертных оценок. [Сборник статей] / Ред. коллегия: Т.В. Рябушкин (отв. ред.) [и др.] ; [Науч. ред. Ю.Н. Тюрин, А.А. Френкель] – М.: Наука, 1977. – 384 с.

42. Моисеев Н.Н. Математические задачи системного анализа. – М.: Наука, 1981. – 487 с.

43. Литвак Б.Г.Экспертные оценки и принятие решений. – М.: Патент, 1996.

44. Характеристики методов экспертных оценок [Электронный ресурс]: http://examen.od.ua/upravlen/page116.html. Дата обращения [05.03.2015].

45. Экспертные оценки. // StatSoft: SPC Consulting. [Электронный ресурс]: http://www.spc-consulting.ru/app/expert.htm. Дата обращения [05.03.2015].

46. Управленческая диагностика: теория и практика: Монография / А.М. Григан. Ростов н/Д: Изд-во РСЭИ, 2009. – 316 с.

47. Вагин В. Н., Головина Е. Ю., Загорянская А. А., Фомина М. В. Достоверный и правдоподобный вывод в интеллектуальных системах/ Под ред. В. Н. Вагина, Д. А. Поспелова. – М.: ФИЗМАТЛИТ, 2004. – 704 с.

48. Осипов Г.С. Искусственный интеллект: состояние исследований и несколько слов о будущем// Новости искусственного интеллекта, 2001. –№1. – С. 2-13.

49. Аверин А. И., Вагин В. Н. Параллелизм в дедуктивном выводе на графовых структурах// Известия РАН. Автоматика и телемеханика. 2001.– №10. – С. 54-64.

50.Гаврилова Т. А., Хорошевский В. Ф. Базы знаний интеллектуальных систем. – СПб.:Питер, 2000. – 382 с.

51. Рыбина Г. В. Особенности современных подходов к построению экспертных систем// Труды конгресса «Искусственный интеллект в XXI веке». Научное издание. – М.: Изд. Физ.-мат. Лит., 2001. – С. 383-390.

52. Галушкин А. И. Теория нейронных сетей – М.: ИСПЖР, 2000. – 325 стр.

53. Васильев А.Н., Тархов Д.А. Нейросетевое моделирование. Принципы. Алгоритмы. Приложения. – СПб.: Изд-во Политехн. ун-та, 2009. – 527с.

54. Алиева Д.И., Крыжановский Б.В. Векторная модель нейронной сети с переменным порогом// Нейрокомпьютеры: разработка, применение. – 2005. – №3. – С.5-11.

55. Антонов В.И., Васильев А.Н., Тархов Д.А. Нейросетевые подходы к решению нестандартных задач моделирования теплообмена в системе «сосуды – ткани»// Известия ТРТУ. – 2006. – №16(71). – С.54-58.

56. Балухто А.Н. и др. Нейрокомпьютеры в системах обработки изображений. – М.: Радиотехника, 2003. – 192 с.

57. Бахвалов Н.С., Жидков Н.П., Кобельков Г.М. Численные методы. – М.: Лаборатория Базовых Знаний, 2002. – 632 с.

58. Бэстенс Д.-Э. и др. Нейронные сети и финансовые рынки. – М.: ТВП, 1997. – 236 с.

59. Васильев А.Н. Новые нейросетевые подходы к решению краевых задач в областях, допускающих декомпозицию// «Нейрокомпьютеры»: разработка, применение. – 2006. – №7. – С.32-39.

60. Головко В.А. Нейронные сети: обучение, организация и применение. – М.: Журнал «Радиотехника» издательства РАДИОТЕХНИКА, 2001. – 256 с.

61. Горбань А.Н. Обучение нейронных сетей. – М.: Параграф, 1990. – 160 с.

62. Каллан Р. Основные концепции нейронных сетей. – М.: Вильямс, 2001. – 288 с.

63. Нечаев Ю.И. Нейросетевые технологии в бортовых интеллектуальных системах реального времени// В сб.: ”Лекции по нейроинформатике”. – М.: Национальный исследовательский ядерный университет «МИФИ», 2002. – Часть 1. – С.114-163.

64. Калинина В.Н., Панкин В.Ф. Математическая статистика. – М.: Высш. шк., 2001. – 336 с.

65. Алексахин С.В. и др. Прикладной статистический анализ данных. Теория. Компьютерная обработка. Области применения. В 2-х томах. – М.: ООО Издательство «Приор», 2002. – 688 с.

66. Тарасов В. Б. От многоагентных систем к интеллектуальным организациям: философия, псохология, информатика. – М.: Эдиториал УРСС, 2002. – 352 с.

67. Вагин В.Н., Еремеев А.П. Некоторые базовые принципы построения интеллектуальных систем поддержки принятия решений реального времени// Известия РАН. Теория и системы управления. 2001. – №6. – С.114-123.

68. Гладун В. П. Партнерство с компьютером. Человеко-машинные целеустремленные системы. – Киев: «Port-Royal», 2000.

69. Редько В. Г. Эволюционная кибернетика. – М.: Наука, 2001. – 156 с.

70. Корпоративные информационные системы и методы их разработки/ Е.Ю. Головина. – М.: Издательский дом МЭИ, 2008. – 94 с.

71. Боровиков В.П. Statistica для студентов и инженеров. – М.: КомпьютерПресс, 2001. – 301 с.

72. Чжао Л., Карманов А.Г., Бондаренко И.Б., Ткачев К.О. Разработка модели угроз информационной безопасности при организации системы связи с наземным подвижным объектом // Актуальные вопросы науки и техники: Сборник научных трудов по итогам международной научно-практической конференции, Самара, 7 апреля 2015 г. Том II – 2015. – с. 194-196.

73. Щербаков В.Б.. Безопасность беспроводных сетей: стандарт IEEE 802.11/ В.Б. Щербаков, С.А. Ермаков. – М.: РадиоСофт, 2010. – 255с.

74. Борисов В.И., Щербаков В.Б., Ермаков С.А. Спектр уязвимостей беспроводных сетей стандарта IEEE 802.11//Информация и безопасность. 2008. Т. 11. № 3. С. 431–434.

75. Столлингс В. Беспроводные линии связи и сети.: Пер. с англ. – М.: Издательский дом «Вильямс», 2003. – 640 с.

76. Григорьев В.А., Лагутенко О.И., Распаев Ю.А. Сети и системы радиодоступа. – М.:Эко-Трендз, 2005. – 384 с.

77. Максим М. Безопасность беспроводных сетей / Мерит Максим, Дэвид Полино; Пер. с англ. Семенова А.В. – М.: Компания АйТи; ДМК Пресс, 2004. – 288с.

78. Владимиров А.А.Wi-фу: «боевые» приемы взлома и защиты беспроводных сетей /Андрей А. Владимиров, Константин В. Гавриленко, Андрей А. Михайловский; пер. с англ. АА. Слинкина. – М.: НТ Пресс, 2005. – 463с.

79. Маковеева М.М., Шинаков Ю.С. Системы связи с подвижными объектами: Учебное пособие для вузов.–М.:Радио и связь, 2002. – 440 с.

80. Чжао Лэй., Карманов А.Г., Бондаренко И.Б., Ткачев К.О. Оценивание живучести систем связи линейного типа с наземными подвижными объектами// Известия вузов. Приборостроение. Университет ИТМО2016. Т.59, №3, 2016, с.173-180.

81. Чжао Лэй., Карманов А.Г., Бондаренко И.Б., Ткачев К.О. Определение вероятности отказа в обслуживании при росте числа наземных подвижных объектов открытой системы связи линейного типа// Информация и Космос, №1 – 2016.–192с., стр. 62-66.

82. Синтез и анализ живучести сетевых систем: монография / Ю.Ю. Громов, В.О. Драчев, К.А. Набатов, О.Г. Иванова. – М.: «Издательство Машиностроение-1», 2007. – 152с.

83. Трифонов С.В., Холодов Я.А. Исследование и оптимизация работы беспроводной сенсорной сети на основе протокола ZigBee//Компьютерный исследования и моделирование. Т.4, №4, 2012. – стр.855-869.

84. Хрусталев Д.А. Новейшее руководство по сотовой связи. – М.: СОЛОН-Пресс, 2004. – 176с.

85. Максименко В. Н., Афанасьев В. В., Волков Н. В. Защита информации в сетях сотовой подвижной связи. Под ред. д.т.н., проф. О. Б. Макаревича. – М.: Горячая линия – Телеком, 2007. – 360 с.

86. Бабков, В.Ю., Цикин И.А. Сотовые системы мобильной радиосвязи. – 2-е изд., перераб. и доп. – СПб.: БХВ-Петербург, 2013. – 432 с.

87. Шитиков В.К., Розенберг Г.С., Зинченко Т.Д. Количественная гидроэкология: методы системной идентификации. – Тольятти: ИЭВБ РАН, 2003. – 463 с.

88. Морозов В.Г. Эволюционное моделирование рядов произвольной вариабильности: необходимость и методика прогнозирования // Изв. СамНЦ РАН. 2000. Т. 2. № 2. С. 206-215.

89. Технология NFC в смартфонах и ее практическое использование. [Электронный ресурс]: http://www.ixbt.com/mobile/nfc-2013.shtml. Дата обращения [15.09.2014].

90. Lou Frenzel NFC Lets You Leave Your Cash And Credit Cards At Home. [Электронный ресурс]: http://www.rlocman.ru/review/article.html?di=150991. Дата обращения [15.09.2014].

91. Еруслан Каронский Коммуникация ближнего поля. [Электронный ресурс]: http://karonskiy.ru/2011/06/11/kommunikaciya-blizhnego-polya. Дата обращения [05.06.2015].

92. Александр Калачев Для учета и идентификации: решения NFC от Texas Instruments// Новости электроники № 10, 2014, стр. 13-18. Дата обращения [05.06.2015].

93. ГОСТ Р ИСО/МЭК 14443. Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты близкого действия. - М.: Издательство стандатов, 2011.

94. Джхунян Л.В., Шангинь В.Ф. «Электронная идентификация. Бесконтактные электронные идентификаторы и смарт-карты» , - М.: NT Press , 2010.

95. Yanhai Cao, «A New Transmitter Circuit for the 13.56MHz RFID Reader Based on ISO14443».

96. Ortiz, C. Enrique, «An Introduction to Near-Field Communication and the Contactless Communication API», Self Press, London 2010.

97. Kasper, Timo; Dario Carluccio, Christof Paar, «An embedded system for

practical security analysis of contactless smartcards.», May 2011.

98. Григорьев В.А., Лагутенко О.И., Сети и системы радиодоступа. Изд-во Экотрендз, М.: 2010. – 385 с.

99. Федоров М., Технология RFID. Опыт использования и перспективные направления, «Компоненты и технологии» №9, 2011. – стр. 45-60.

100. Оценка влияния условий эксплуатации на параметры NFC-системы.// Компоненты и технологии. №2, 2012, http://www.kit-e.ru/asset/files/pdf/2012_2_104.pdf. Дата обращения [05.06.2015].

101. Историография радиочастотной идентификации (RFID)-российские корни // Современные наукоемкие технологии, ООО "Издательский дом "Академия естествознания" (Москва), Бондаревский А.С., Золотов Р.В. 2009. - №8, - стр. 11-15.

102. Стандарты NFC, Интернет-страница сайт IXBT интернейшнл [Электронный ресурс]: http://www.ixbt.com/mobile/nfc-2013.shtml. Дата обращения [25.09.2015].

103. Чжао Лэй, Иванова Е.А., Карманов А.Г., Бондаренко И.Б. Обзор методов, применяемых при проектировании защищенных систем связи геоинформационных систем // Информация и Космос, №2 – 2017. – 194с., стр. 53-56.

104. Чжао Лэй. Модели оценки защищенности системы связи с наземными подвижными обьектами // Информация и Космос, №4 – 2019.

ПРИЛОЖЕНИЕ А

Обучающая выборка

№п/п	Номера входов ИНС											Выход ИНС
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	
1	124	900	2000	200	0	5000	1	1	1	1	1	22
2	374	1700	2000	200	0	4000	2	1	1	1	1	22
3	124	960	2000	200	0	5000	1	1	1	1	1	22
4	14	2400	2000	10000	1	300	2	0	0	1	0	17
5	38	5200	2000	10000	1	300	2	0	0	1	0	17
6	14	2460	2000	10000	1	300	2	0	0	1	0	17
7	38	6000	2000	10000	1	300	2	0	0	1	0	17
8	14	2480	2000	10000	1	300	2	0	0	1	0	17
9	14	2460	2000	10000	1	300	2	0	0	1	0	17
10	79	2400	100	40	1	100	2	0	0	0	0	4
11	79	2480	100	100	1	100	2	0	0	0	0	4
12	38	5600	2000	10000	1	300	2	0	0	1	0	17
13	129	2300	2000	11	0	5000	2	0	1	1	1	4
14	64	820	2000	45000	0	30000	1	1	1	1	1	25
15	1024	3400	2000	11	0	4000	2	0	1	1	1	4
16	48	2300	2000	11	0	4000	2	0	1	1	1	4
17	5	5800	100	7500	1	300	2	0	0	0	0	20
18	512	140	100000	13	0	30000	1	0	1	1	1	25
19	79	2480	100	40	1	100	2	0	0	0	0	17
20	124	900	2000	200	0	5000	1	1	1	1	1	22
21	64	870	2000	45000	0	30000	1	1	1	1	1	25
22	124	960	2000	200	0	5000	1	1	1	1	1	22
23	79	2450	100	170	1	100	2	0	0	0	0	4
24	4	5925	100	7500	1	300	2	0	0	0	0	20

№п/п	Номера входов ИНС											Выход ИНС
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	
25	64	895	2000	45000	0	30000	1	1	1	1	1	25
26	512	870	100000	13	0	30000	1	0	1	1	1	25
27	2048	3500	2000	11	0	5000	2	0	1	1	1	4
28	374	1880	2000	200	0	3000	1	1	1	1	1	22
29	1024	3400	2000	11	0	5000	2	0	1	1	1	4
30	5	5900	100	7500	1	300	2	0	0	0	0	20
31	64	824	2000	45000	0	30000	1	1	1	1	1	25
32	512	406	100000	13	0	30000	1	0	1	1	1	25
33	124	935	2000	200	0	3000	2	1	1	1	1	22
34	79	2400	100	120	1	100	2	0	0	0	0	4
35	64	830	2000	45000	0	30000	1	1	1	1	1	25
36	5	5870	100	7500	1	300	2	0	0	0	0	20
37	512	137	100000	13	0	30000	1	0	1	1	1	25
38	5	5900	100	7500	1	300	2	0	0	0	0	20
39	79	2470	100	80	1	100	2	0	0	0	0	4
40	64	850	2000	45000	0	30000	1	1	1	1	1	25
41	512	840	100000	13	0	30000	1	0	1	1	1	25
42	512	2500	2000	11	0	4000	2	0	1	1	1	4
43	3	5850	100	7500	1	300	2	0	0	0	0	20
44	512	450	100000	13	0	30000	1	0	1	1	1	25
45	64	825	2000	45000	0	30000	1	1	1	1	1	25
46	5	5925	100	7500	1	300	2	0	0	0	0	20
47	512	750	100000	30000	1	0	1	1	1	1	1	25

ПРИЛОЖЕНИЕ Б

Обучающая выборка

№п/п	Номера входов ИНС										Выход ИНС
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	
1	9	9	8	6	6	3	4	2	0	0	1
2	6	6	10	7	5	4	4	3	0	0	1
3	9	12	12	10	9	7	7	4	3	0	1
4	10	6	4	6	4	2	2	0	0	0	0
5	8	10	9	7	8	4	3	2	0	0	1
6	8	10	7	11	8	3	6	1	2	0	1
7	10	10	11	7	8	9	3	7	1	0	1
8	7	7	8	9	5	3	5	1	1	0	1
9	5	4	3	9	4	0	3	0	0	0	1
10	8	7	7	7	5	4	4	3	1	0	1
11	8	9	8	9	8	3	5	4	1	0	1
12	6	6	6	10	6	2	3	2	0	0	1
13	9	6	5	9	6	0	4	0	0	0	0
14	9	9	10	8	9	7	3	7	0	0	1
15	6	6	3	9	5	1	2	0	1	0	0
16	7	7	11	9	5	5	6	3	1	0	1
17	7	7	9	8	5	6	4	4	1	0	1
18	4	7	9	10	3	5	7	1	3	0	1
19	10	11	11	8	8	8	6	5	3	0	1
20	6	6	5	12	5	2	3	2	0	0	1
21	7	5	8	11	5	1	6	1	0	0	1
22	7	5	8	5	5	2	1	2	0	0	0
23	11	11	6	8	10	4	3	3	1	0	1
24	7	7	11	7	5	5	4	3	0	0	1

№п/п	Номера входов ИНС										Выход ИНС
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	
25	8	8	6	7	8	3	1	3	0	0	1
26	11	12	7	5	8	6	3	3	2	0	1
27	8	6	7	11	6	3	4	3	0	0	1
28	11	13	9	5	11	6	2	4	0	0	1
29	6	8	7	9	5	4	5	1	3	0	1
30	5	7	9	7	5	3	4	1	0	0	1
31	6	5	6	7	5	4	1	4	0	0	1
32	10	8	6	7	7	4	2	3	0	0	1
33	8	8	5	10	8	2	3	2	0	0	1
34	12	12	12	4	10	7	4	5	1	0	1
35	2	6	12	13	1	5	7	1	0	0	1
36	8	7	5	7	6	4	1	3	0	0	1
37	5	7	6	11	3	3	5	0	2	0	1
38	5	6	5	12	4	4	2	2	1	0	1
39	6	6	5	9	4	2	3	1	0	0	0
40	11	12	12	8	10	9	4	7	1	0	1
41	11	10	5	7	9	3	3	2	1	0	1
42	5	8	6	8	5	3	2	2	0	0	1
43	7	8	7	7	6	3	4	1	0	0	1
44	8	6	10	8	6	2	7	2	0	0	1
45	7	6	7	9	6	1	3	1	0	0	1
46	10	9	10	9	9	4	6	4	0	0	1
47	8	12	9	7	8	5	6	1	2	0	1
48	8	10	10	7	7	6	4	4	0	0	1
49	6	7	6	5	4	4	2	2	0	0	1
50	5	8	11	12	5	6	6	3	1	0	1

УНИВЕРСИТЕТ ИТМО

МИНОБРНАУКИ РОССИИ

федеральное государственное автономное
образовательное учреждение высшего образования
«Санкт-Петербургский национальный
исследовательский университет
информационных технологий,
механики и оптики» (Университет ИТМО)

Кронверкский проспект, д. 49, г. Санкт-Петербург,
Российская Федерация, 197101
тел.: (812) 232-97-04 | факс: (812) 232-23-07
od@mail.ifmo.ru | www.ifmo.ru

09.10.2017 № 1016/093

УТВЕРЖДАЮ
Ректор Университета ИТМО,
В.Н. Васильев

«09» 10 2017 г.

М.П.

АКТ

внедрения в учебный процесс кафедры «Геоинформационных систем» (ГИС) Университета ИТМО результатов диссертации Чжао Лэя на тему «Метод и алгоритмы повышения безопасности открытой сети связи с наземными подвижными объектами».

Комиссия в составе председателя, заведующего кафедрой ГИС д.т.н., профессора Присяжнюка Сергея Прокофьевича, а так же её членов: к.т.н., доцента Аванесова Михаила Юрьевича, к.т.н., доцента Долговой Маргариты Петровны, к.т.н., доцента Овчинникова Георгия Ревмировича удостоверяет, что результаты диссертационного исследования Чжао Лэя, а именно, метод определения показателей защищенности разрабатываемых вариантов построения беспроводных сетей связи с наземными мобильными объектами с использованием статистических и смоделированных данных, а также алгоритм настройки искусственной нейронной сети для решения задачи определения показателей защищенности систем связи на основе принципа последовательного приближения внедрены в учебный процесс кафедры ГИС при разработке учебных пособий, курсов лекций по дисциплинам «Геоинформационные технологии моделирования сетей связи», «Защита данных геоинформационных систем».

Председатель:
заведующий кафедрой ГИС
д.т.н., профессор — Присяжнюк С.П.

Члены комиссии:
доцент, к.т.н. — Аванесов М.Ю.

доцент, к.т.н. — Долгова М.П.

доцент, к.т.н.,
старший научный сотрудник — Овчинников Г.Р.

Подписи членов комиссии заверяю,
начальник УК — Котусева О.В.

Экз. № 1

ЗАКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО «ИНСТИТУТ ТЕЛЕКОММУНИКАЦИЙ»

ул. Кантемировская, д.5,
Санкт-Петербург, 194100
тел. (812) 740-77-07, факс 740-77-08
office@itain.ru
ОКПО 59452298,
ОГРН 1027801538600
ИНН/КПП 7802199182/780201001

УТВЕРЖДАЮ
Заместитель генерального директора по стратегическому развитию

А. Н. Соколов

«23» 04 2021 г.

М.П.

АКТ РЕАЛИЗАЦИИ

результатов диссертационной работы Чжао Лэя,
представленной на соискание учебной степени кандидата технических наук,
в ОКР «Улей», выполненной в ЗАО «Институт телекоммуникаций»
по государственному контракту № 14411.169999.11.047 от 28.02.2014 г.
с Министерством промышленности и торговли РФ

Научно-техническая комиссия в составе: председателя – начальника НИО-1 Кондратьева А.В. и членов: ведущего специалиста Баскакова Д.В., ведущего специалиста Пономарева В.А., составила настоящий акт о том, что при выполнении ОКР «Улей» были использованы рабочие материалы Чжао Лэя, подготовленные им при проведении исследований по диссертационной работе, а именно:

- метод определения показателей защищенности вариантов построения беспроводных сетей связи с наземными объектами с использованием статистических и смоделированных данных;
- алгоритм настройки искусственной нейронной сети для решения задачи определения показателей защищенности систем связи на основе принципа последовательного приближения;
- алгоритм прогнозирования устойчивости беспроводной сети при изменении ее параметров.

Указанные научные результаты вошли в состав методического комплекса моделирования широкодиапазонных пакетных радиосетей, входящего в методологический комплекс обеспечения моделирования, маршрутизации, коммутации и передачи информации для широкодиапазонных пакетных радиосетей повышенной живучести и помехозащищенности, совместимых с изделиями 15Э1836, 15Э1391 и геоинформационным комплексом «Виолит-М», и были реализованы в программном комплексе моделирования и планирования ШДФИ.00520-01.

Председатель комиссии:
Начальник НИО-1 А. В. Кондратьев

Члены комиссии:
Ведущий специалист Д. В. Баскаков
Ведущий специалист В. А. Пономарев