На правах рукописи

Чжао Лэй

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

Специальность: 2.2.15. Системы, сети и устройства телекоммуникаций

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата технических наук

Санкт-Петербург – 2021

Работа выполнена в федеральном государственном автономном образовательном учреждении высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения»

Научный руководитель: кандидат технических наук, доцент
Карманов Андрей Геннадьевич

Официальные оппоненты: **Рогозин Евгений Алексеевич**
доктор технических наук, профессор, профессор кафедры автоматизированных информационных систем органов внутренних дел федерального государственного казенного образовательного учреждения высшего образования «Воронежский институт Министерства внутренних дел Российской Федерации»

Платонов Владимир Владимирович
кандидат технических наук, доцент Института кибербезопасности и защиты информации федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский политехнический университет Петра Великого»

Ведущая организация: Федеральное государственное бюджетное образовательное учреждение высшего образования «Российский государственный гидрометеорологический университет»

Защита состоится «15» февраля 2022 г. в 14:00 часов на заседании диссертационного совета 24.2.384.01 при Санкт-Петербургском государственном университете аэрокосмического приборостроения по адресу: 190000, Санкт-Петербург, ул. Большая Морская, д.67.

С диссертацией можно ознакомиться в библиотеке Санкт-Петербургского государственного университета аэрокосмического приборостроения по адресу: 190000, Санкт-Петербург, ул. Большая Морская, д.67 и на сайте http://dissov.guap.ru/defense/chzhao_lej

Автореферат разослан «15» декабря 2021 г.

Ученый секретарь
диссертационного совета 24.2.384.01,
кандидат технических наук, доцент  **Овчинников Андрей Анатольевич**

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

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 совершенствованию защиты 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 способствует бурному развитию и повсеместному развертыванию мобильных систем; на этапе разработки потребность в определении показателей защищенности 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, 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.

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.

Область исследования. Содержание диссертационной работы соответствует паспорту специальности 2.2.15. 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;

− 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 актами.

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.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность работы, сформулированы цель и задачи исследования, научная новизна и практическая значимость результатов, определены объект, предмет и методы исследования, приведена информация о достоверности, внедрении и апробации работы, а также ее структура.

В первой главе рассмотрены возможные виды реализации систем связи с наземными подвижными объектами. Проанализированы классификации систем связи по диапазонам частот, наличию базовых станций (БС), по дальности связи абонент-БС и БС-БС, и др. Базовые станции также могут быть мобильными и стационарными, а мобильные профессиональные станции могут осуществлять связь между собой, не используя БС, при этом образуются группы и подгруппы. Профессиональные средства связи имеют дополнительные функции и защиту от действия внешних факторов; подлежат регистрации в органах надзора за связью. В итоге выделены основные параметры для разделения на классы профессиональных средств связи.

Классификация беспроводных сетей, которые делятся на сухопутные, морские, авиационные, спутниковые и общего пользования, показала, что наземные сети подвижной связи являются основой для построения систем подвижной связи общего пользования. Сдерживающие факторы развития спутниковых систем связи, такие как сложность передающей аппаратуры и высокая стоимость связи, являются

причиной использования таких систем только для радиовещания, передачи данных сети интернет, радиолокации и в системах связи специального назначения.

Показано, что при разработке новых стандартов беспроводных сетей преимущественно используются или готовые протоколы связи, или с небольшими изменениями, причем открытого типа.

В результате проведенных исследований сделан вывод, что для выполнения поставленных в работе задач необходимо использовать цифровые системы связи, обладающие большими скоростями передачи данных, поддержкой пакетных режимов, отсутствием фоновых помех, малым временем установки связи. Протоколы для цифровых систем связи делятся на закрытые (корпоративные) и открытые.

Анализ современных протоколов, использующихся в беспроводных системах передачи данных, таких как: BlueTooth, Wireless USB, Wireless HD, WiGig, WHDi, DASH7, WirelessHART, MiWi, RuBee, HiperLAN, Wi-Fi, Zigbee, RONJA, Classic WaveLAN, NMT, AMPS, Mobitex, GSM, TDMA, GPRS, EDGE, CDMA, WCDMA, CDMA 2000, HSPA, LTE, TETRA и APCO 25, показал, что они имеют множество однотипных параметров, в той или иной степени эволюционируют и используются для организации беспроводных систем связи. Из-за большой конкуренции среди производителей открытые системы связи получают большее распространение, чем закрытые.

В главе рассмотрены угрозы и уязвимости для систем радиосвязи с подвижными наземными объектами. Основными угрозами являются: внешняя помеха, перехват (прослушивание) информации, искажение информации, DDoS-атака, подмена информации, клонирование SIM-карт, аппаратуры. В результате злоумышленнику может стать доступными не только данные, но и ресурсы аппаратуры сети. Анализ подходов при организации защиты систем связи показал, что основными принципами защиты являются: кодирование и шифрование данных, использование паролей с помощью описанных в работе алгоритмов.

Далее были проанализированы требования, предъявляемые к системам связи. Основными показателями служат: готовность – обеспечивается живучестью, помехозащищенностью, помехоустойчивостью и электромагнитной совместимостью; устойчивость функционирования – обеспечивается надежностью; пропускная способность, мобильность, защищенность; доступность и управляемость.

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

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

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

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

вероятность подавления канала связи помехой:

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

В свою очередь:

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

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.

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.

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

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

$$\gamma(K_{П}, \nu) = \frac{1 - q(A)}{1 - q(A) + B\left(1 + \frac{K_{П}(1 - q(A))}{B + \nu(1 - q(A))}\right)}$$

где $K_{\text{П}}$ – коэффициент отсутствия готовности системы связи, или коэффициент простоя, ν – относительная интенсивность восстановления отказов.
Тогда запас структурной устойчивости, который необходимо поддерживать в пределах 0,2…0,3:

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

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

В качестве показателей надежности системы связи с наземными подвижными объектами использованы:

− вероятность связности сети – вероятность, что имеется хотя бы один канал для передачи информации по каналу связи:

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

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

− 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).

Целевая функция для 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 перечисленные показатели противоречивы и связаны сложными математическими соотношениями, представить которые в аналитическом виде затруднительно. При условии воздействия внешних дестабилизирующих факторов устойчивость зависит от: защищенности, плотности размещения объектов связи, устойчивости средств управления, готовности аппаратуры к работе в экстремальных условиях.

В конце главы описаны проблемы систем связи, как сложных эволюционирующих объектов, для которых показатели защищенности – многопараметрические сложные функции.

Во **второй** главе сделан аналитический обзор и выбор методов исследования уровня защищенности систем радиосвязи. Такими методами являются: иерархические деревья решений, метод оценок, генетические алгоритмы, алгоритмы корреляционного анализа, искусственные нейронные сети (ИНС) и другие.

Окончательное решение принимается с помощью методов: предпочтения (ранжировки), задания весовых коэффициентов, парных сравнений и последовательных сравнений. Рассмотрены достоинства и недостатки каждого из методов. Для использования методики ранжирования рассчитывался коэффициент конкордации (W) – общий коэффициент ранговой корреляции для группы из k наборов оценок.

$$W = \frac{12S}{k^2(n^3 - n)}, \qquad (1)$$

где

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

где n – число сравниваемых критериев; x_{ji} – ранг, присвоенный j-му фактору i-го набора оценок; $x_{ср}$ – среднее арифметическое оценок по группе из множества k наборов оценок.

Максимум значения коэффициента W (равный 1) означает, что все оценки согласованы, а минимум (значение 0) – их рассогласованность.

Далее в работе раскрыты аспекты методики решения задач с использованием ИНС. Каждый нейрон в составе ИНС представляет собой элемент, имеющий вход, и выход. Уравнение связи для выражения зависимости выходного сигнала (OUT) нейрона от входного x – однопараметрическая функция произвольного вида:

$$OUT = w\, x, \quad (3)$$

где w – синаптический вес.

Если на вход нейрона подается несколько входных сигналов (j), то формула (1) будет иметь вид:

$$OUT = \sum_{j=1}^{m} w_j x_j. \quad (4)$$

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:

$$Y = f(OUT) = \frac{1}{1 + \exp(\Theta - OUT)}. \quad (5)$$

В работе показано, что определение числа нейронов в скрытых слоях, выбор варианта топологии и методы настройки весов ИНС – являются трудноформализуемыми задачами, решаемыми в настоящее время путем подбора, или выбором заведомо избыточного варианта ИНС. С ростом сложности структуры сети растет ее "гибкость" и точность результатов, но в тоже время возрастают и объемы вычислений, и трудоемкость настройки весов.

Сигнал на выходе j-го нейрона:

$$y_j(N) = \varphi_j(v_j(N)), \quad (6)$$

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 (6) 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:

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

Величина коррекции весов:

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

где k – параметр скорости обучения.
Градиент представим в виде:

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

Для сигмоидальной активационной функции:

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

или через $y_j(N)$ по (6), избавимся от экспоненты и получим:

$$\varphi_j'(v_j(N))=ay_j(N)(1-y_j(N)). \quad (7)$$

Далее показано, что:

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

Следовательно, это свойство сигмоидальной функции в алгоритме использованного метода обратного распространения ошибки вносит наибольший вклад в его устойчивость при обучении ИНС.

Принцип работы метода обратного распространения ошибки основан на минимизации ошибки, получаемой как разность получаемых значений рассогласования выхода сети и заранее известных обучающих наборов:

$$\varepsilon_{\text{опт}}=\min\left[\frac{1}{2N_S}\sum_{i=1}^{N_S}\left(OUT_i-E_i\right)^2\right], \quad (8)$$

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 (8):

$$\varepsilon=\frac{1}{2N_S}\sum_{i=1}^{N_S}\Delta_i^2, \quad (9)$$

которую можно оптимизировать методами: наискорейшего (градиентного) спуска, параллельных касательных, сопряженных градиентов, BFGS (Бройдена, Флетчера,

Гольдфарба и Шанно), DFP (Давидона-Флетчера-Пауэлла); их работа кратко описана в диссертации.

В работе описаны вероятностные методы. В данной работе могут использоваться методы с построением деревьев решений (Decision Trees), которые в настоящее время решают следующие типы задач: точное описание объектов, классификация и регрессия, прогнозирование.

В работе показано, что наибольшая сложность для этого метода – определить в ситуации неопределенности способ отнесения к тому или иному узлу варианта решения. В связи с этим рассмотрены алгоритмы: *CART* –Classification and regression Tree (Л. Брейман), *C* 4.5 (Р. Куинлен) *QUEST* (разработан В. Ло и И. Ши на основе улучшенного варианта метода рекурсивного квадратичного дискриминантного анализа). Также рассмотрен алгоритм отсечения ветвей, который при движении от листов к вершине дерева отсекает или заменяет поддеревьями те ветви, которые не приведут к возрастанию ошибки.

В конце второй главы приведены выводы о достоинствах и недостатках методов, пригодных для исследования уровня защищенности систем радиосвязи. Наиболее подходящим инструментом для проведения исследований является аппарат ИНС.

В **третьей главе** было выбрано программное средство для проведения имитационных экспериментов. Из анализа математических пакетов сделан вывод, что наиболее подходящей является отечественная разработка NeuroPro, распространяемая на бесплатной основе. Она содержит необходимый функционал и не требует навыков программирования.

Далее были проанализированы угрозы системам связи на основе рассмотренных протоколов и показателей защищенности. 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. В качестве показателей защищенности систем связи с наземными подвижными объектами могут служить: взломостойкость, время функционирования до установленного факта взлома, и другие параметры. Для исследуемых протоколов в работе была определена возможность реализации угроз (табл. 1).

Таблица 1. Возможность реализации угроз при использовании различных протоколов видов связи

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

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

Для определения значимости параметров протоколов для построения систем связи были определены пять наборов оценок. Целью статистической обработки оценок был выбор тех параметров, которые сильнее влияют на защищенность протоколов. По выражениям:

$$w_j = \frac{1}{k}\sum_{\mathrm{i=1}}^{\mathrm{k}} \frac{x_{ji}}{\sum_{\mathrm{j=1}}^{\mathrm{n}} x_{ji}},$$

где $n = 13$; $k = 5$,

определяя величины среднеквадратического отклонения и коэффициента вариации, вычисляя параметр:

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

в работе определен дисперсионный коэффициент конкордации: $W = 0{,}4$ значение которого показывает, что оценки являются хорошо согласованными.

В итоге значимыми являются следующие параметры: 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.

Далее были проанализированы условия структурной устойчивости сети связи с подвижными объектами. Выполнение условия связности графа сети, где ребрам соответствуют каналы связи, а вершинам базовые и клиентские станции, определяет возможность передачи информации от источника к приемнику. Для оценки распределенной в пространстве системы линейной радиосвязи с подвижными объектами (рис. 1), где БС1 является источником а БС4 – приемником сигнала, была разработана модель для определения вероятности отказа в обслуживании беспроводной сети линейного типа при росте числа наземных мобильных абонентов.

Для открытых систем связи с подвижными объектами количество каналов не ограничивается, что в результате роста плотности обонентов может привести к преодолению критической величины для данного протокола связи. Рост зоны охвата сети приводит к тому, что радиосигналы можно легко перехватить и/или заглушить.

Таким образом, структурная устойчивость таких систем связи снижается с ростом числа абонентов.

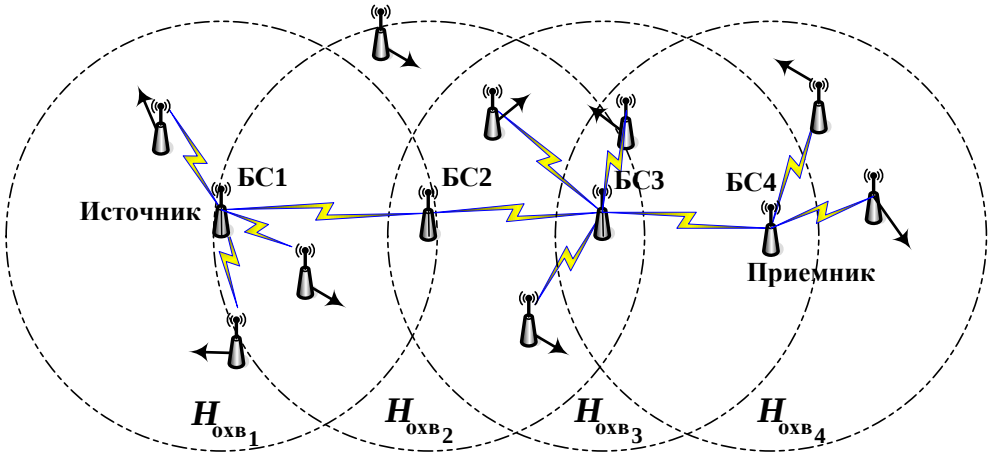


Рис. 1. Линейная система связи с подвижными объектами

Получено условие отказа БС при превышении числа каналов R_{max} для определенного протокола связи:

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

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

Для исследования влияния количества мобильных пользователей разных типов на устойчивость беспроводной сети связи был разработан алгоритм формирования обучающего множества. Он представлен на рис. 2.

Координаты новых подключений мобильных абонентов генерировались случайным образом, с проверкой условия:

$$r(X,Y) < H_{\text{охв}},$$

где $r(X, Y)$ – евклидово расстояние от абонента до БС, X и Y– координаторы абонента.

Для проведения эксперимента были использованы следующие исходные данные: протокол WiFi 802.11, для которого $R_{\max} = 14$ каналов; зоны покрытия БС 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).

Сделан вывод о корреляции результатов экспериментов с параметрами линии связи.

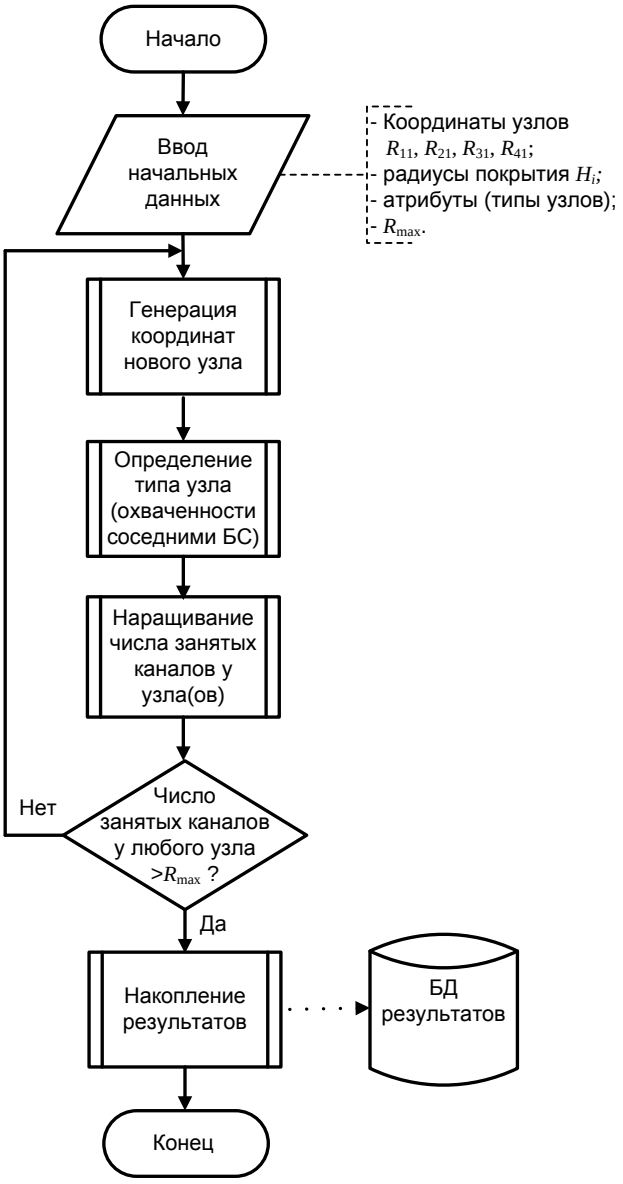


Рис. 2. Структурная схема разработанного алгоритма

В **четвертой главе** с помощью разработанной методики подбора параметров ИНС, а также в результате отбора параметров протоколов беспроводной связи для открытых сетей была решена задача прогнозирования времени устойчивого функционирования системы связи до ее взлома. Параметры протоколов, определенные в третьей главе, были поставлены в соответствие входам ИНС, а выходом являлось время до взлома протокола. Для известных систем связи оно было определено по дате опубликования методики взлома в открытых источниках информации: СМИ и сети интернет.

В итоге, с учетом вариации параметров, было составлено 47 наборов данных, использованных в качестве обучающего множества. Структура ИНС подбиралась, начиная с конфигурации 11/5/1 (11 – количество входов, 5 – количество скрытых слоев, 1 – количество выходов) с контролем числа циклов, необходимых для обучения при дообучении. Наилучшим решением стал вариант ИНС 11/8/1, минимизирующий среднюю ошибку до значения 1,798 с минимальным количеством циклов, необходимых для обучения: 52 шт.

Далее были определены значения крутизны для отдельных слоев 0,01; 0,1; 0,1(входной слой, скрытый слой и выходной слой соответственно), при которых достигалась наименьшая ошибка 1,145 при 100% успешности обучения. Наилучшим методом оптимизации ошибки при настройке ИНС также оказался BFGS.

Оценки значимости входов ИНС приведены на рис. 3.

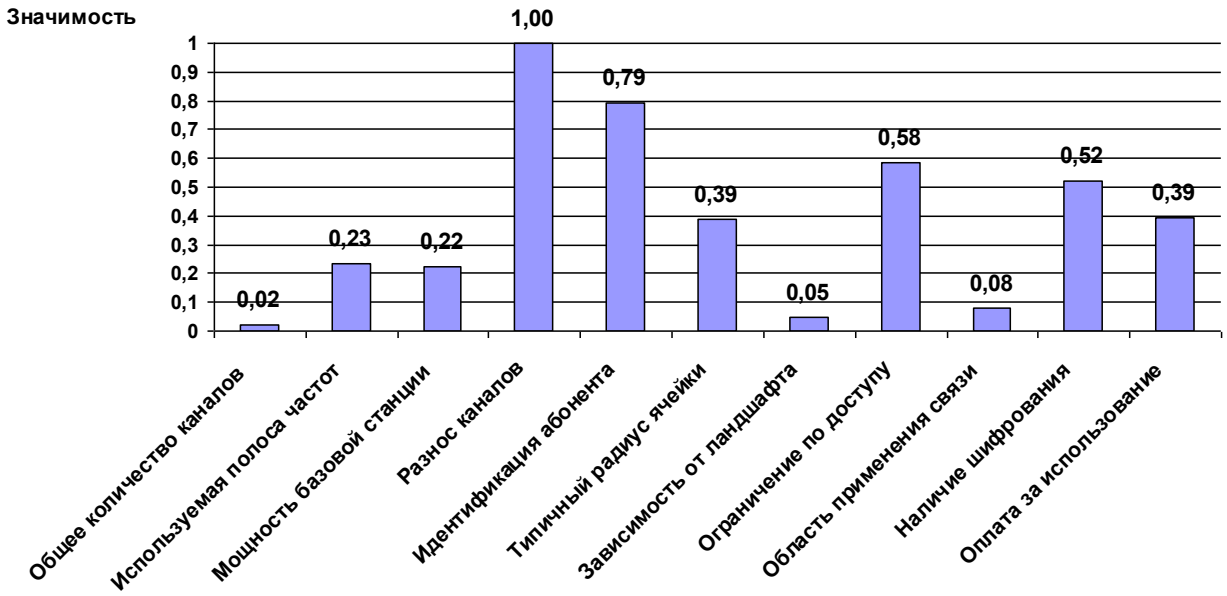


Рис. 3. Оценка значимости входов ИНС

Апробация разработанной методики была произведена для прогнозирования времени устойчивого функционирования протокола беспроводной связи ***NFC*** (Near Field Communication) для высокочастотной системы связи малого радиуса действия, разработанного в 2003г. Протокол характеризуется низкой скоростью передачи данных, малой мощностью передатчика и плохой защищенной канала связи. Благодаря низкой стоимости комплектующих, протокол *NFC* нашел применение в системах доступа. В настоящее время его планируют использовать для проведения банковских операций с внедрением в мобильные устройства.

Для проверки состоятельности протокола, исходные данные для него были поданы на вход настроенной ИНС с топологией 11/8/1. В результате прогноза получено, что с точностью ±2% протокол будет взломан через 23,5 года от 2003 года (время разработки), то есть время живучести – до 2026…2027 года.

Задача прогнозирования структурной устойчивости сети связи также решалась с помощью ИНС. Входами ИНС являлись значения N (10 входов), выход – вероятность превышения R_{max}.

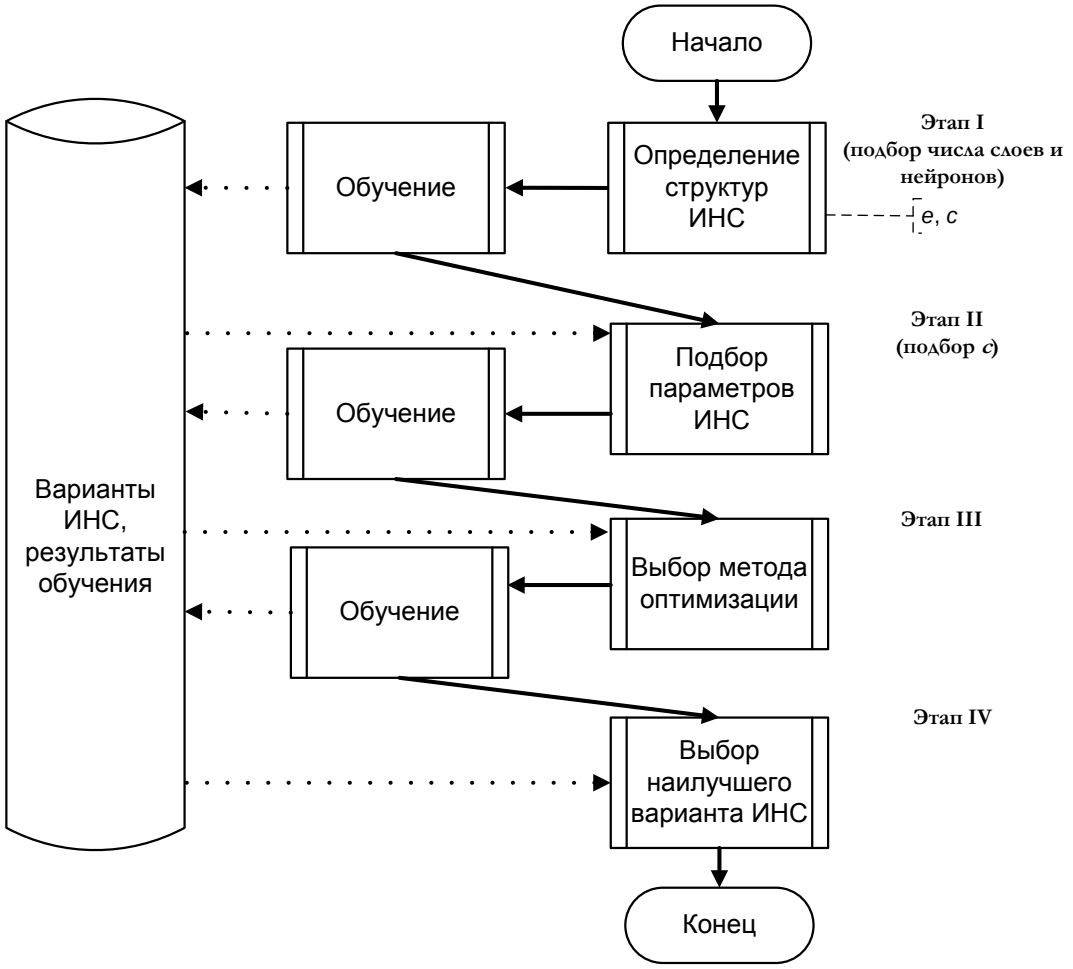
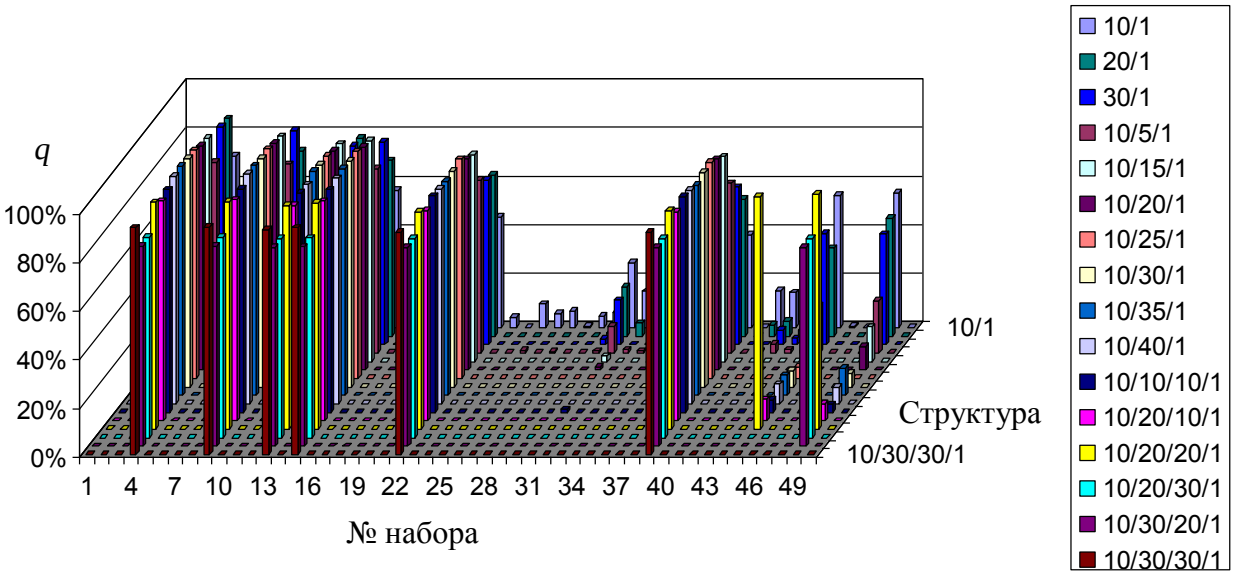


Рис. 4. Этапы поиска наилучшего варианта ИНС

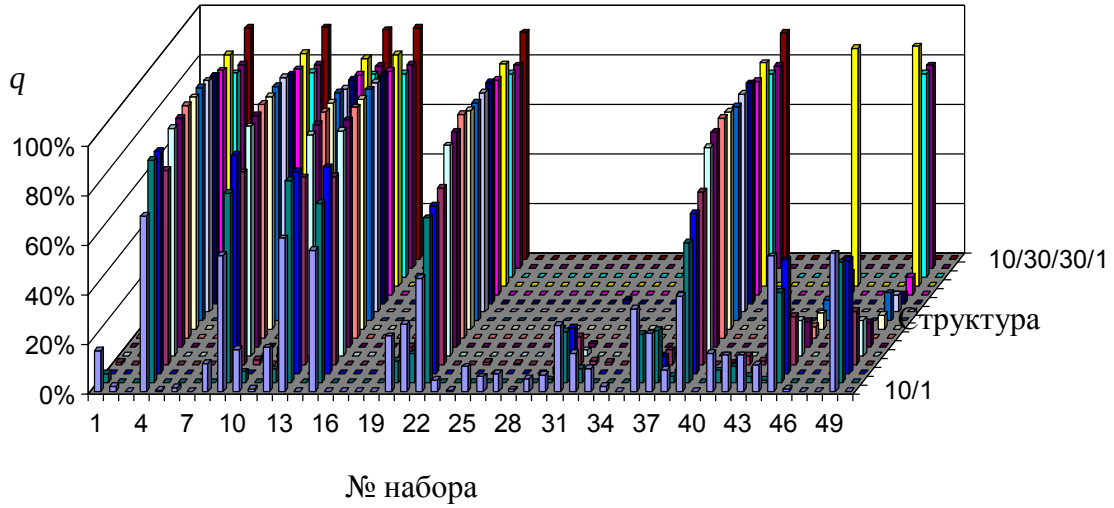
В результате проведенных экспериментов по разработанной методике обучения (см. рис. 4), получены данные, представленные в виде гистограмм на рис. 5 при крутизне сигмоид $c = 0{,}9$ и $e = \pm 1$ %. Качество прогнозирования настроенной ИНС контролировалось подсчетом ошибок – ложных срабатываний. Отказы в обслуживании сети (q) должны наблюдаться в наборах №№ 4, 13, 15, 22 и 39. У ИНС с двумя скрытыми слоями по 30 нейронов в каждом: 10/30/30/1 – всего одно ложное срабатывание (девятый набор), с вероятностью 92 %.

Далее с помощью последовательного приближения подбирались значения крутизны сигмоидов и метода оптимизации. В итоге были получены значения крутизны 0,1; 0,01; 0,1, при которых на выходе ИНС получено: 6 % неуверенного прогноза и 2 % – неправильного; это соответствует третьему и первому наборам соответственно. В качестве наилучшего метода оптимизации ошибки был экспериментально определен BFGS.

Полученные значения значимости входов ИНС со структурой 10/30/30/1 представлены в таблице 2.



а)



б)

Рис 5. Результаты прогнозирования с помощью моделирования на ИНС ((а) – прямой порядок структур ИНС, (б) – обратный порядок структур ИНС)

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.

Таблица 2. Полученные 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

В **заключении** сформулированы основные результаты диссертационной работы:

− 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 методики с использованием экспертных оценок.

− 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 %;

− разработан алгоритм прогнозирования устойчивости беспроводной сети в изменяющихся условиях, который отличается от известных подходов сокращением времени получения пользователем необходимых данных;

− с помощью разработанной методики была решена задача определения времени устойчивого функционирования системы связи до ее взлома.

Таким образом, 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.

ПЕРЕЧЕНЬ ОПУБЛИКОВАННЫХ АВТОРОМ РАБОТ ПО ТЕМЕ ДИССЕРТАЦИИ

Публикации в изданиях из перечня, рекомендованного ВАК:

1. Чжао Лэй, Карманов А.Г., Конев А.С. Прототип алгоритма посадки беспилотного летательного аппарата в условиях сложного рельефа // Информация и Космос, том №2, 2015. С. 96-98.

2. Чжао Лэй, Карманов А.Г., Бондаренко И.Б., Ткачев К.О. Оценка живучести сложных информационных систем связи с подвижными объектами // Информация и Космос, том №3, 2015. С. 36-41.

3. 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, том №1, 2016. С. 62-66.

4. Чжао Лэй, Иванова Е.А., Карманов А.Г., Бондаренко И.Б. Обзор методов, применяемых при проектировании защищенных систем связи геоинформационных систем // Информация и Космос, том №2, 2017. С. 53-56.

5. Чжао Лэй. Модели оценки защищенности системы связи с наземными подвижными обьектами // Информация и Космос, том №4, 2019. С. 90-93.

Публикации в прочих изданиях:

6. Чжао Лэй, Карманов А.Г., Бондаренко И.Б., Ткачев К.О. Оценивание живучести систем связи линейного типа с наземными подвижными

объектами // Известия высших учебных заведений. Приборостроение, том 59, №3, 2016. С.173-180.

7. Чжао Лэй, 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 II международной научно-практической конференции. Самара, 7 апреля 2015 г. С. 194-196.

8. Чжао Лэй. Безопасный интернет в китайской народной республике // Актуальные проблемы организации и технологии защиты информации: Сборник научных трудов по итогам межвузовская научно-практической конференции. Санкт-Петербург, 30 ноября 2012 г. С. 60-61.

9. Чжао Лэй, Карманов А.Г., Бондаренко И.Б., Ткачев К.О. Исследование живучести систем связи линейного типа с подвижными обьектами на транспорте // Сборник трудов V Всероссийского конгресса молодых ученых. Санкт-Петербург, Университет ИТМО, 2016. С. 24-27.

10. Чжао Лэй, Карманов А.Г., Бондаренко И.Б., Ткачев К.О. Анализ угроз информационной безопасности при организации системы связи с наземным подвижным обьектом // Сборник трудов IV Всероссийского конгресса молодых ученых. Санкт-Петербург, Университет ИТМО, 2015. С. 78-80.

11. Чжао Лэй. Безопасная информационная технология в Китае // Сборник трудов II Всероссийского конгресса молодых ученых. Санкт-Петербург, Университет ИТМО, 2013. С. 44-45.