18 - Приборы и методы экспериментальной физики. Информационные технологии в физических исследованиях

Полянский Дмитрий Александрович, доцент
Владивосток, Дальневосточный федеральный университет, ИНТиПМ
Оценка возможности утечки информации, обрабатываемой на моноблоках, по каналу ПЭМИН
e-mail: *polyanskiy.da@dvfu.ru* стр. 280

Свинцицкий Михаил Юрьевич, 4 курс
Владивосток, Дальневосточный федеральный университет, Институт математики и компьютерных технологий
Разработка программного обеспечения сканера для поиска закладных устройств
Полянский Дмитрий Александрович, к.ф.-м.н.
e-mail: *bandirart@gmail.com* стр. 283

Шауро Виталий Павлович
Красноярск
Обзор эксперимента Google на 53-кубитном процессоре Sycamore
e-mail: *Shaurkin@hotmail.com* стр. 283

Создание контроля неисправности систем кондиционирования и поддержания температуры и влажности центров обработки данных

Абдурахимов Муслимбек Абдулбоки угли
Северный Арктический федеральный университет им. М. В. Ломоносова
Лагунов Алексей Юрьевич
Abdurahimov.m@edu.narfu.ru

Центры обработки данных (ЦОД) — это критически важные инфраструктуры, в котором размещено оборудование для обработки и хранения данных и которое подключено к высокоскоростным каналам связи. Эти центры потребляют большое количество энергии для работы и обслуживания серверов, вычислительного оборудования и систем охлаждения. Однако кондиционеры склонны к сбоям и могут повлиять на производительность, потребление энергии и контроль влажности. В данном исследовании мы предлагаем разработку автоматической системы оповещения, которая выявляет отказы кондиционеров в центрах обработки данных и предупреждает пользователей.

Сегодня, по мере роста компаний, географически распределенные местоположения, такие как филиалы и новые подразделения, создают новые потребности в обширных ИТ-инфраструктурах из-за значительного увеличения объема информации, увеличения количества используемых бизнес-приложений, а также удаленного хранения и обработки. данных [1].

Когда возникает необходимость консолидации обработки данных и централизации ИТ-инфраструктуры и информационных систем, компаниям приходится задумываться о том, строить ли собственный центр обработки данных [2] или арендовать (передать на аутсорсинг) коммерческий центр обработки данных. Таким образом, реальная потребность в центре обработки данных возникает тогда, когда становятся важными высокая эффективность использования ресурсов ИТ-инфраструктуры, высокая доступность, масштабируемость, непрерывность, управляемость и предсказуемость прикладных услуг. Именно тогда стабильность некоммерческого предприятия или бизнеса начинает зависеть от его ИТ-инфраструктуры.

Таким образом, аутсорсинг становиться очень важным предприятием для современного бизнеса и приносить очень высокий прибыл владельцу. Наш проект тоже проведут такое приложения и расширить основных станции для реализации проекта.

Структурную схему ЦОД можно представить следующим образом (рис. 1).

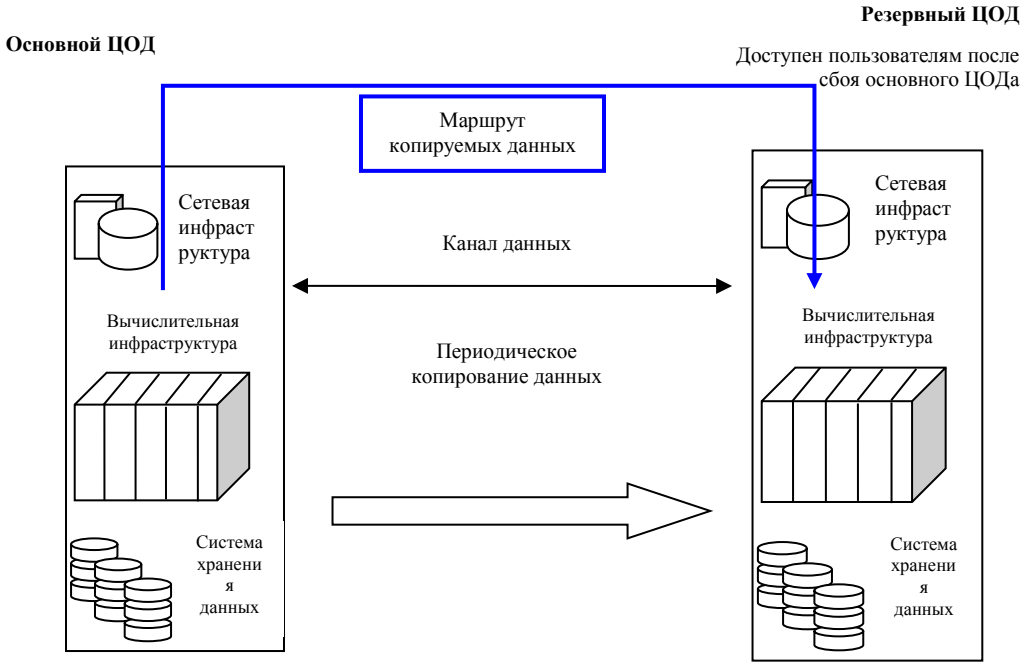


рис. 1 – Структурная схема центра обработки данных

Структура ЦОД включает в себя три уровня: модуль ядра, модуль доступа к внешним сетям и модуль управления сетевой инфраструктурой. Среди основных функций центра обработки данных как комплексной отказоустойчивой централизованной системы находятся хранение, обработка и распространение информации.

Учитывая вышеперечисленные проблемы и все информации, для нас было бы большим достижением создать такие относительно дешевые и качественные дата-центры. Именно этому и посвящена наша работа.

Для создания этого устройства после рассмотрения различных критериев, таких как цена, размер и гибкость, мы выбрали микроконтроллер Arduino Uno, датчик температуры и влажности DHT11, Пищалка (Buzzer) и Микроконтроллер ESP8266. Систему мониторинга создали в Arduino IDE, подключив микроконтроллер Arduino Uno и необходимые датчики. На рисунке 2 показаны некоторые результаты эксперимента:

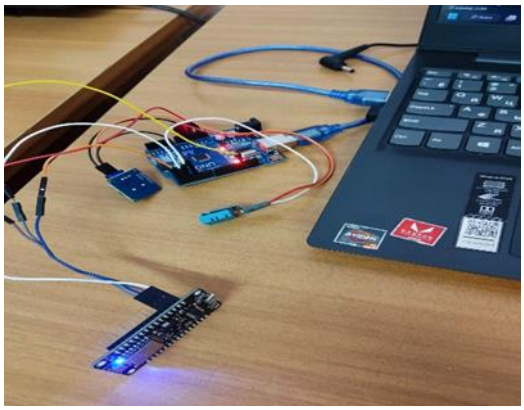


рис 2. Внешний вид экспериментальной устройства и полученные данные от датчиков

Как видно из картинок выше, созданная программа позволяет получать все данные в полном объеме и предупреждать, когда эти данные превышают определенный уровень.

Поскольку разрабатываемая система мониторинга направлена исключительно на решение текущих неполадок в работе ЦОД вследствие нарушения климатических условий в его помещениях, с появлением новых проблем возможно совершенствование системы путем добавления новых датчиков и оборудования в состав системы.

Список публикаций:

[1] Ташпулатов Ж.Ж., Назиров С.С Анализ подходов построения cloud дата-центров // Аллея Науки, 2018, стр. 212-216.
[2] Венгловская Э.С. Создание дата- центра // Экономика. Менеджмент. Инновации, 2019, стр. 76- 82.

Исследование одноканальной оптической линии связи со скоростью передачи информации 10 Гбит/с

Ахняпов Эмиль Шамилович
Мухамедов Диёр Илхомжонович, Лопатюк Алёна Викторовна
Уфимский университет науки и технологий
Лопатюк Алёна Викторовна
emilakhnyapov5@gmail.com

Волоконно-оптические системы передачи информации являются дорогой и сложной частью системы электросвязи. Поэтому применение систем автоматизированного проектирования (САПР) очень важно. Нужны они для разработки, исследования и проектирования волоконно-оптических линий и их компонентов.

Собранная и исследуемая в данной работе одноканальная линия в САПР имеет вид, представленный на рисунке 1. [1]

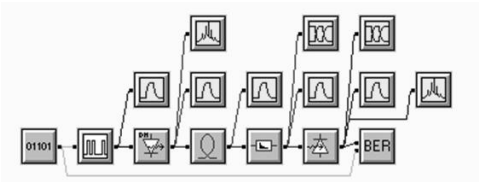
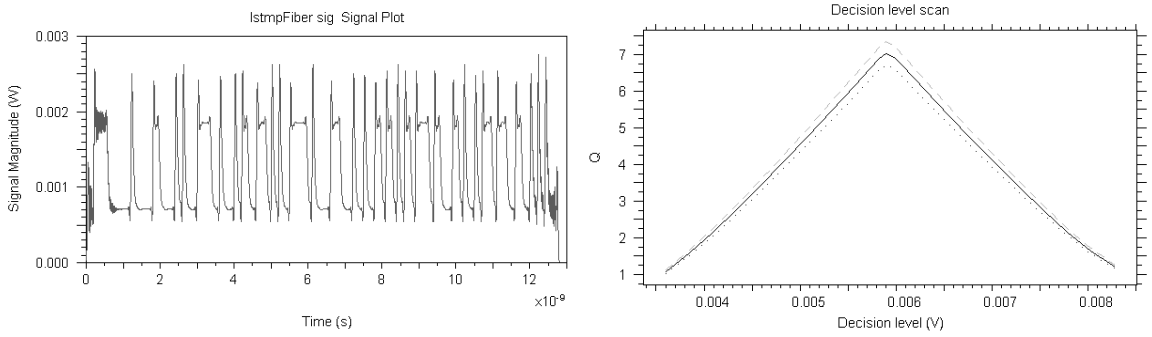


рис.1. Одноканальная оптическая линия связи

Эта линия состоит из генератора испытательного сигнала, сигнал-генератора, оптического волокна, оптического нормализатора мощности, приёмо-передающих модулей. А также в схему добавлены устройства

контроля параметров линии связи: устройство для отображения формы сигналов, анализатор глаз-диаграммы, анализатор спектра сигнала и тестер битовых ошибок (BER).

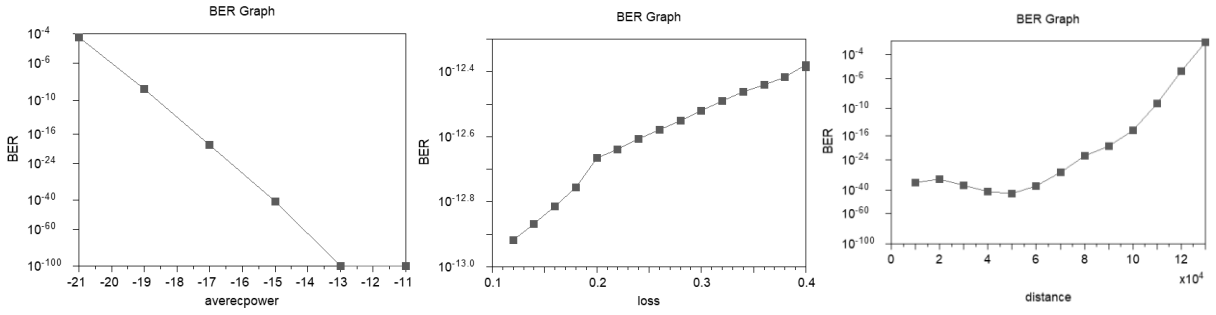


а) *б)*

рис.2. а) Вид сигнала после оптического волокна и б) зависимость Q-фактора от уровня принятия решения.

Максимальное значение Q-фактора наблюдается при уровне принятия решения, равным 0,0059 В. Q-фактор – параметр, отражающий качество сигнала цифровой системы передачи. (рис. 2. б)

Построим графики зависимостей битовой ошибки BER от различных параметров системы:



а) *б)* *в)*

рис.3. Графики зависимостей битовой ошибки BER от а) средней мощности нормализатора мощности, б) затухания сигнала в оптическом волокне и в) длины проектируемой линии связи.

Битовые ошибки являются одними из основных источников ухудшения качества передаваемой информации. Его значения имеют следующую характеристику [2]:

Номинальное для одноканальной линии - BER < 10^{-9};

- нормальное - BER < 10^{-6};
- пониженное – 10^{-6} < BER < 10^{-3} (предаварийное состояние):
- неприемлемое - BER > 10^{-3} (аварийное состояние).

Оптимальная работа линии осуществляется при значении средней мощности не ниже -18,5. (рис. 3. а)

Одним из основных параметров, влияющих на уровень битовых ошибок BER, является затухание сигнала в оптическом волокне. Видим, что уровень битовых ошибок увеличивается практически линейно с ростом затухания в оптическом волокне. (рис. 3. б)

Немаловажную роль в битовых ошибках играет и длина линии связи. Поэтому важнейшей задачей проектирования линий связи является расчёт длин регенерационных участков. Исходя из графика видно, что длина регенерационного участка составляет около 115 км. Наименьшее значение уровня битовой ошибки достигается при длине линии в 50 км. (рис. 3. в)

Список публикаций:

[1] Ахняпов Э.Ш., Мухамедов Д.И., Лопатюк А.В. // Разработка волоконной оптической системы передачи информации на базе DSF волокна. Фундаментальная математика и ее приложения в естествознании: спутник Международной научной конференции «Уфимская осенняя математическая школа-2022»: тезисы докладов XIII Международной школы-конференции студентов, аспирантов и молодых ученых, посвященной 50-летию образования математического и физического факультетов БашГУ (г. Уфа, 19 – 22 октя 2022 г.) / Л.А. Габдрахманова. – Уфа: РИЦ БашГУ, 2022. – С.57-58.

[2] Ахняпов Э.Ш., Куликовский Н.А., Лопатюк А.В. // Исследование цифрового кольца, обеспечивающего межстанционную связь на ГТС. Теоретические и экспериментальные исследования нелинейных процессов в конденсированных средах: материалы VIII Межрегиональной школы-конференции студентов, аспирантов и молодых ученых (г. Уфа, 22 – 23 апреля 2022 г.) с.185-186.

Разработка аппаратной части сканера для поиска закладных устройств

Бережной Данила Александрович
Дальневосточный федеральный университет
Полянский Дмитрий Александрович, к.ф.-м.н.
berezhnoi.da@students.dvfu.ru

Состояние защищенности в организациях обеспечивается множеством средств и методов, которые затрагивают различные области информационной безопасности и одной из важнейших областей является защита технических каналов утечки информации. Актуальность задач, решаемых в данной области, обуславливается большим количеством рисков, связанных с реализацией угроз информационной безопасности с применением устройств негласного съема информации, которые не требуют от злоумышленника большого уровня компетенций, а также вложений на создание устройства.

Одной из таких задач является защита организации от кражи злоумышленниками данных с помощью радиозакладных устройств. При решении данной задачи возникает необходимость в приборах контроля радиочастотного диапазона, а также подходящем наборе антенн, которые позволят вести контроль нужного диапазона частот. Одним из наиболее эффективных решений данной задачи являются промышленные поисковые комплексы, однако ввиду большой стоимости они не доступны большинству организаций малого и среднего бизнеса. Исходя из вышесказанного, можно утверждать, что наиболее рациональным решением задачи борьбы с радиозакладными устройствами является использование недорогих радиоприемников, которые в совокупности с общедоступным программным обеспечением и правильным набором антенн позволяют выявлять радиозакладные устройства.

Целью данной работы является разработка аппаратной части сканера для поиска радиозакладных устройств. В ходе выполнения данной работы необходимо определить диапазон частот, в котором будут анализироваться сигналы. Также необходимо определить аппаратную базу, на основе которой будет функционировать сканер закладных устройств.

Главной особенностью радиозакладных устройств является их многообразие, являющееся следствием существующих запретов на свободный их оборот, а также самодельного производства злоумышленниками. Ввиду вышесказанного приходится констатировать тот факт, что во многих классификациях значения показателей классификации могут разниться. Например, радиозакладные устройства способны работать как на низких, так и сверхвысоких частотах [1]. Поэтому для решения задачи защиты от радиозакладных устройств логичным решением было бы учитывать технические возможности той аппаратной базы, использование которой было бы рациональным с точки зрения финансовых возможностей организации.

В качестве основы аппаратной базы выступает программно-определяемая радиосистема (SDR приемник), выполненная в виде печатной платы с USB коннектором. Такой тип приемника, позволяет изменять различные настройки радиочастотных параметров. Данный вид приемников имеется в разных ценовых сегментах, но даже многие низкобюджетные варианты плат способны работать в диапазоне 20-1700 МГц, что позволяет закрыть ощутимый диапазон частот вплоть до диапазонов работы систем GPS и ГЛОНАСС. USB коннектор в свою очередь позволяет использовать приемник вместе с ноутбуком. Благодаря этому мы также экономим на приборе, так как модели со встроенным дисплеем стоят дороже, к тому же у нас появляется возможность запускать на ноутбуке программное обеспечение с открытым исходным кодом, что позволит работать с приемником более эффективно.

Так же необходимо подобрать оптимальную для работы устройства антенну. В поисковых устройствах антенное устройство используется в первую очередь для приема сигнала. Ввиду того, что съем информации злоумышленниками с радиозакладных устройств происходит за счет излучаемого устройствами сигнала, этот сигнал и является главным демаскирующим фактором. Радиозакладные могут работать на разной частоте поэтому главным критерием выбора антенны является ее полоса частот. Исходя из этого выбор пал на логопериодическую антенну. Она является распространенной, не дорогой и ее не сложно рассчитать и сделать самостоятельно при необходимости. Данный тип антенн обладает широким диапазоном рабочих частот, за счет использования длинных и коротких вибраторов, увеличение количества которых, увеличивает ее полосу частот.

В статье представлена концепция сканера для поиска закладных устройств. Определены основные составные элементы данного поискового устройства. Будут проведены эксперименты по обнаружению имитаторов радиозакладных устройств. Для этого будет использоваться SDR приемник, ноутбук и программное обеспечение, с помощью которых будет происходить считывание, обработка и анализ данных радиочастотного контроля.

Список публикаций:

[1] Классификация электронных устройств перехвата информации [Текст]: / Хорев А.А. – М.: Спецтехника и связь. 2009. - №1. - С.46 – 50.

Об алгоритме поиска траектории трассы катодно-поляризуемого магистрального трубопровода на основе БПЛА-мониторинга распределения магнитного поля

Валитов Денис Русланович
Сафаргалиева Ралина Ринатовна
Стерлитамакский филиал Уфимского университета науки и технологий
Викторов Сергей Владимирович, к.ф.-м.н.
ssilverufa@yandex.ru

Математические модели распределения магнитных полей, регистрируемых в воздушном пространстве над поверхностью грунта, в котором размещен катодно-поляризуемый магистральный трубопровод [1, 2], положены в основу решения актуальной в настоящее время проблемы износа магистральных трубопроводов.

Интерпретация информации, полученной при регистрации магнитной составляющей поля, может быть использована для неразрушающего контроля за состоянием трубопровода.

Для решения вопроса эффективного поиска дефектных участков изоляции магистральных трубопроводов предлагается использовать программно-аппаратный комплекс [3], где в качестве измерительной аппаратуры выступает магнитный градиентометр, а в качестве ПО – программное средство, реализующее математические модели электрических и магнитных полей катодной защиты магистральных трубопроводов в изотропных кусочно-однородных и анизотропных средах [1, 2].

Использование в качестве носителя измерительной системы беспилотного летательного аппарата позволит существенно снизить затраты на обслуживание трассы. В этом случае возникает ряд дополнительных задач, связанных с управлением БПЛА в автоматизированном режиме определения траектории полета (режиме трассометрии).

На основе данной модели построен алгоритм, по которому может быть произведен облет беспилотного летательного аппарата (БПЛА) с закрепленным на нем градиентометром для измерения магнитного поля трубопровода в режиме трассометрии.

На основе предложенного алгоритма может быть построено полетное задание на возврат БПЛА к оператору по найденным точкам оси трубы. Пролетая максимально точно над трассой возможно провести детальные измерения, интерпретация которых позволит определять проблемные участки изоляции без физического нарушения трассы трубопровода.

Список публикаций:
[1] Кризский В.Н., Александров П.Н., Ковальский А.А., Викторов С.В. Моделирование электромагнитных полей систем катодной защиты трубопроводов в горизонтально-слоистых средах // Наука и технологии трубопроводного транспорта нефти и нефтепродуктов. – 2019. – Т. 5. № 9 – С. 558 567
[2] Кризский В.Н., Александров П.Н., Ковальский А.А., Викторов С.В. Математическое моделирование электрических полей катодной защиты магистральных трубопроводов в анизотропных средах // Наука и технологии трубопроводного транспорта нефти и нефтепродуктов. – 2020. – Т. 1 №10 – С. 52 – 63.
[3] Кризский В.Н., Викторов С.В., Лунтовская Я.А. Математическое моделирование переходного сопротивления изоляции магистрального трубопровода по данным измерений модуля вектора магнитной индукции // Математическое моделирование. – 2022. – Т. 34 №9 – С. 107 – 122.

Создание генератора пространственного зашумления для защиты информации от утечки по каналу ПЭМИН при использовании HDMI

Евтихов Владислав Викторович
Дальневосточный федеральный университет
Полянский Дмитрий Александрович, к.ф.-м.н.
molodegka_rulit@mail.ru

В области технической защиты особое влияние имеет такой технический канал утечки информации как побочные электромагнитные излечения и наводки (ПЭМИН). Актуальность данной утечки обуславливается тем, что с помощью данного канала, в большинстве случаев, похищается информация, относящаяся к государственной тайне, так как все устройства, обрабатывающие такую информацию, изолированы от сети, поэтому кибератаки малоэффективны. Оценочно, по каналу ПЭМИН может быть похищены всего 1-2 процента данных, хранимых и обрабатываемых на персональных компьютерах и других технических средствах передачи информации (ТСПИ). С одной стороны, этот канал менее опасен, чем, например, акустический, по которому может произойти утечка до 100% речевой информации, циркулирующей в помещении. Но с другой стороны,

стоит помнить, что специфика канала ПЭМИН такова, что те самые два процента информации, уязвимые для технических средств перехвата — это данные, вводимые с клавиатуры компьютера или отображаемые на дисплее, то есть довольно значительная часть сведений, подлежащих защите, может оказаться доступна для чужих глаз.

Целью данной работы является создание генератора пространственного зашумления (ГПЗ) для защиты информации от утечек по каналу ПЭМИН при использовании такого видеоинтерфейса, как HDMI. В ходе работы необходимо определить частоты, на которых работает данный видеоинтерфейс при использовании с различными разрешениями мониторов. Был выбран именно данный интерфейс по нескольким причинам: большая популярность в использовании, высокая интенсивность излучения и дальность распространения побочных электромагнитных излучений.

Данная цель будет достигнута за счет помехи типа «белого шума» или «синфазные помехи». Системы пространственного зашумления, использующие помехи данного вида, применяются для защиты персональных компьютеров (ПК). В качестве сигнала помех в данных системах используются импульсы случайной амплитуды, которые синхронизированы по форме и времени существования с импульсами информационного сигнала. Таким образом, сигнал помех по своему спектральному составу является идентичным спектру побочный электромагнитных излучений ПЭВМ. Иными словами, система пространственного зашумления вырабатывает «имитационную помеху», которая соответствует по спектральному составу скрываемому сигналу.

Стоит учитывать, что генератор пространственного зашумление должен покрывать всю выбранную нами контролируемую зону (КЗ) – зона, в которой возможен перехват информации, обрабатываемой ПК, с помощью различных разведывательных приемников и дальнейшая расшифровка этой информации. Также в пределах контролируемой зоны отношение «информационный сигнал/помеха» не должно превышать допустимое нормированное значение.

Для создания генератора шума будет использоваться передающая антенна, так как ГПЗ работает на передачу. Вид нужной антенны будет определен после определения частот, на которых работает видеоинтерфейс HDMI. Что известно на данный момент, что нам не потребуется широкополосная антенна, так как нам достаточно работы на узкой полосе частот, но в разных частотных диапазонах.

Подводя итоги к вышесказанному, в результате будет создан самопальный генератор пространственного зашумления для частот работы HDMI. Сначала будет подобрана подходящая схема для создания ГПЗ, потом подобрана антенна, сигнал будет проанализирован на осциллографе и на анализаторе спектра. После всего перечисленного будет произведена попытка съема побочного электромагнитного излучения видеоинтерфейса для проверки работоспособности нашей системы зашумления.

Разработка алгоритмов поиска и создания внеплановых гидродинамических исследований методами гидропрослушивания и анализа добычи и давления

***Ефимова Милана Владимировна*[1,2]**
***Фахреева Регина Рафисовна*[1]**
[1]ООО «РН-БашНИПИнефть», [2]Уфимский университет науки и технологий
Питюк Юлия Айратовна, к.ф.-м.н.
MV_Efimova2@BNIPI.rosneft.ru

В настоящее время для эффективного управления разработкой месторождений необходимо повышать информативность о гидродинамических параметрах пласта. Этого можно добиться путем увеличения количества и качества проводимых гидродинамических исследований скважин (ГДИС). Однако проведение традиционных плановых ГДИС является трудозатратным и дорогостоящим процессом, который влечет за собой значительные потери нефти. В связи с увеличением количества и качества динамических данных эксплуатации скважин со скважинной телеметрии становится возможным использование внеплановых событий на скважинах для проведения ГДИС [1,2]. Таким образом, автоматизация проведения внеплановых исследований является актуальной задачей. Целью работы является применение разработанных подходов для поиска и создания внеплановых ГДИС методами гидропрослушивания (ГП) и анализа добычи/давления (АДД) на месторождении республики Башкортостан.

Метод гидропрослушивания позволяет оценивать гидродинамическую связь между скважинами по пласту, выявлять непроницаемые границы и определять ФЕС пласта [3]. Основной принцип ГП заключается в следующем – одна из скважин выступает в роли возмущающей, остальные – реагирующие. На возмущающей

скважине происходит смена режима работы, т.е. в пласте создается импульс давления, который распространяется от возмущающей скважины и регистрируется на реагирующей скважине.

Анализ добычи и давления позволяет получить те же самые параметры пласта и заканчивания скважины, что и при проведении традиционных методов ГДИС (кривая восстановления давления/кривая восстановления уровня), но без потерь в добыче нефти [4]. Суть метода заключается в анализе динамических данных эксплуатации скважины и в настройке модели системы скважина-пласт-область дренирования с известным значением начального пластового давления.

Концепция проведения внеплановых исследований методами гидропрослушивания (ГП) и анализа добычи/давления (АДД) базируется на трех этапах. На первом этапе (рис.1) происходит поиск скважин-кандидатов для проведения анализа с помощью идентификации событий на скважинах. На втором этапе (рис.2) происходит оценка целесообразности проведения анализа по разработанным алгоритмам: однозначный ответ, последовательность проверки условий выхода, критичность мероприятий. Если хотя бы по одному из алгоритмов вышла оценка «Нецелесообразно», то создание и проведение исследования является нецелесообразным. По результатам второго этапа на скважинах, потенциальных к проведению исследования, специалист ГДИС проводит интерпретацию в ПК «РН-ВЕГА» [5] и анализ накопленных динамических данных на найденном информативном интервале (рис.3).

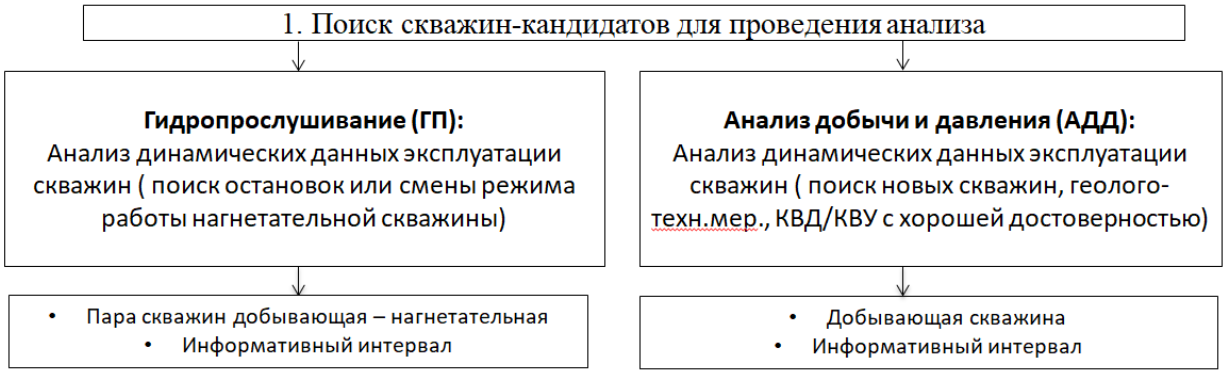


рис.1. Первый этап проведения внеплановых исследований ГП и АДД

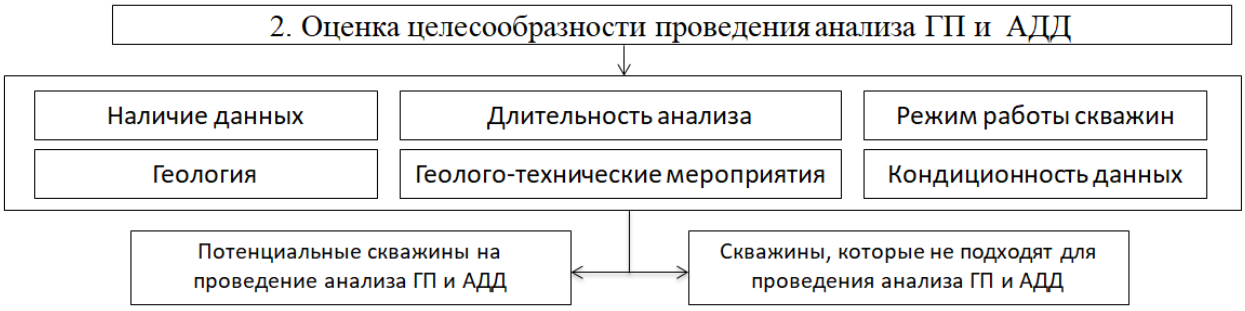


рис.2. Второй этап проведения внеплановых исследований ГП и АДД

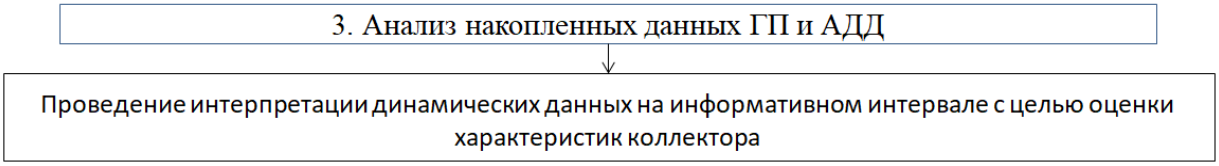


рис.3. Третий этап проведения внеплановых исследований ГП и АДД

Разработанные алгоритмы поиска и создания внеплановых ГП и АДД были протестированы на исторических данных на скважинах месторождения Республики Башкортостан. В результате тестирования найдены кандидаты на проведение исследований. В табл.1 представлены результаты работы модуля по поиску кандидатов методами АДД и ГП для тестирования расчетного сервиса поиска и сопровождения ГДИС.

Табл.1. Результаты тестирования алгоритмов поиска и создания ГДИС методами АДД и ГП

Вид ГДИС	Проанализировано проведение ГДИС	Создание ГДИС целесообразно	Часто встречающиеся причины при создании ГДИС	Проведение ГДИС целесообразно	Часто встречающиеся причины при проведении ГДИС
АДД	177	26	Достаточная точность ТМС, Риски интерференции, Отсутствие данных PVT	0	Разрывы данных давления/дебита по времени, Недостаточное кол-во точек давления
ГП	214	52	Отсутствие данных по давлению, Риски интерференции	3	Отсутствие данных по давлению/дебиту, Разрывы данных давления/дебита по времени, Недостаточное кол-во точек дебита

Можно заметить, что наиболее частые нецелесообразные причины при накоплении данных для проведения ГДИС методом ГП и АДД связаны с кондиционностью данных давления и дебита. Достоверность и информативность результатов интерпретации исследований напрямую зависят от полноты и качества исходных данных. Поэтому рекомендуется оснащение скважин датчиками телеметрии, позволяющими замерять давление не менее 1 раза в 5 минут, а расходы замерять как минимум 1 раз в двое суток.

Таким образом, разработанный подход по поиску и созданию внеплановых ГДИС методами ГП и АДД был протестирован и позволил выявить скважины с некондиционными динамическими данными.

Список публикаций:

[1] Питюк Ю.А., Акмурзина Г.Р., Давлетбаев А.Я., Азарова Т.П., Фаргер Д.В., Кривуляк А.С. Зылева С.А. Разработка инструмента для проведения гидродинамических исследований скважин в режиме реального времени // Российская нефтегазовая техническая конференция SPE. – SPE-201898-RU. – 2020.

[2] Фахреева Р.Р., Питюк Ю.А. и др. Автоматизация оценки целесообразности, подготовки и проведения ГДИС в режиме реального времени по данным телеметрии. // Инженерная практика. – № 10/2022. – 2022.

[3] Деева Т.А.. Гидродинамические исследования скважин: анализ и интерпретация данных. – Томск: центр профессиональной переподготовки специалистов нефтегазового дела ТПУ, 2010. – 240 с

[4] Кременецкий М.И., Ипатов А.И. Долговременный мониторинг промысловых параметров, как знаковое направление развития современных ГДИС // Инженерная практика. – 2012. – № 9. – С. 4–8.

[5] https://rn.digital/rnvega/

Исследование одноканальной оптической линии связи с внешней модуляцией сигнала

Лопатюк Алена Викторовна

Полканова Алина Михайловна, Сидорова Олеся Владиславовна

Уфимский университет науки и технологий

Лопатюк Алена Викторовна.

alyona-lopatyuk@yandex.ru

Одноканальная линия связи используется во многих оптических системах, поэтому рассмотрение данной темы остается актуальной на сегодняшний день. В данной работе мы собрали одноканальную оптическую линию связи с внешней модуляцией сигнала, которая показана на рис.1 (а). Она состоит из следующих элементов: PRBS генератор, генератор сигнала, лазер с синхронизацией мод, электрооптический модулятор, волокно, оптический усилитель, оптический фильтр, оптический нормализатор мощности, фотоприемник, BER-тестер [1].

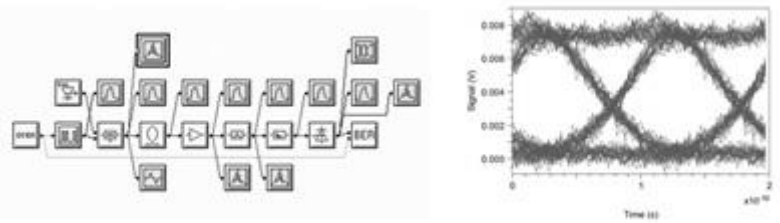


рис.2 а) Одноканальная оптическая линия связи; б) Глаз-диаграмма

Для визуального контроля степени искажения, зашумленности сигнала, текущего контроля состояния тракта передачи и приёма цифровых сигналов используется глаз – диаграмма, показанная на рис.1 (б).

На полученной диаграмме мы видим, что 7,5 мВ – это уровень принятия решения «1», а 0,5 мВ – уровень принятия решения «0», тогда раскрытие глаза составляет 7 мВ.

Для измерения коэффициента ошибок в оптическом канале используется метод на основе оценки Q-фактора, который представляет собой отношение (1):

$$Q = \frac{|\mu_1 - \mu_0|}{\sigma_1 + \sigma_0} = \frac{7{,}5 - 0{,}45}{0{,}5 + 0{,}5} \approx 7{,}05 \tag{1}$$

Отношение сигнал/шум (2), (3) позволяет оценить мешающее воздействие помех на сигнал. Чем больше это значение, тем меньше шум влияет на полезный сигнал при его передаче по каналу связи и ведет к хорошему распознаванию сигнала приемником.

$$\frac{S_1}{N_1} = \frac{7{,}5\ \text{мВ}}{0{,}5\ \text{мВ}} = 15 \tag{2}$$

$$\frac{S_0}{N_0} = \frac{0{,}45\ \text{мВ}}{0{,}5\ \text{мВ}} = 0{,}9 \tag{3}$$

Качество цифрового тракта по критерию ошибок считается нормальным, если $\text{BER} < 10^{-6}$.

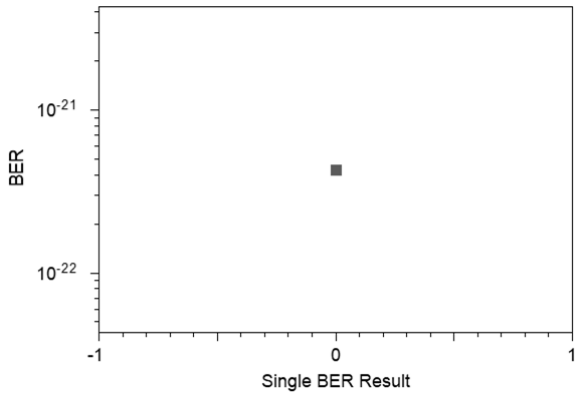
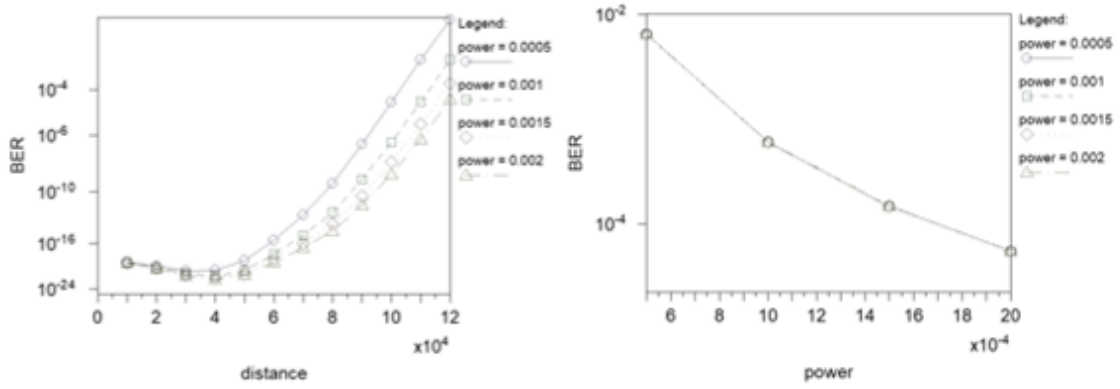


рис.2 Результаты BER-тестера

Из рисунка видно, что значение битовой ошибки 10^{-21} хорошее, линия передачи информации работает в нормальном режиме.

Исследуя работу оптической линии при изменении мощности сигнала лазера от 0.0005 до 0.002 с шагом 0.0005, получили следующие зависимости при разной длине оптической линии [2].

Зависимости получились практически одинаковыми, так как через каждые 40 км устанавливается оптический усилитель, который восстанавливает уровень сигнала. На графиках видно, что битовая ошибка BER увеличивается с ростом расстояния рис.3а), увеличение мощности сигнала лазера приводит к уменьшению битовой ошибки рис.3б) , длина линии связи была взята 120 км, поэтому качество связи в волоконно-оптической системе передаче информации низкое.



а) *б)*

рис.3 Графики зависимости битовой ошибки от длины линии: а) длины оптического волокна, б) мощности излучения лазерного диода

Также меняли усиление оптического усилителя от 0 до 50 с шагом 10, получили зависимости при разной длине оптической линии. Коэффициент усиления равный 30 достаточен для работы линии в номинальном режиме, т.к. наступает насыщение. Таким образом, дальнейшее увеличение коэффициента усиления не влияет на улучшение работы линии передачи информации.

Список публикаций:

[1] Лопатюк А.В. Моделирование и исследование ВОСП-СР, в C И L диапазонах.
Сборник трудов VIII Международной школы-конференции для студентов, аспирантов и молодых ученых «Фундаментальная математика и ее приложения в естествознании». 27 октября -1ноября 2015г. Том 2, Физика Химия Научные статьи, Стр.37-40, г.Уфа, 2015г
[2] Лопатюк А.В., Полканова А.М., Мирзаянова Ч.Д. Исследование отрезка прямого волоконного световода. Тезисы докладов XIII Международной школы-конференции студентов, аспирантов и молодых ученых, посвященной 50-летию образования математического и физического факультетов БашГУ., стр.54.
г. Уфа, 19 – 22 октября 2022 г

Оценка возможности утечки информации, обрабатываемой на моноблоках по каналу ПЭМИН

Полянский Дмитрий Александрович
Яценко Алексей Андреевич
Дальневосточный федеральный университет
polyanskiy.da@dvfu.ru

В настоящее время большинство офисов мелкого и среднего бизнеса, а так же филиалов крупных компаний расположены либо на первых этажах жилых зданий, либо в бизнес-центрах, следствием чего является ограниченный размер контролируемой зоны, что делает более уязвимой информацию, обрабатываемую на компьютерах в данных офисах. Это усугубляется тем, что сотрудники отделов информационной безопасности сводят всё внимание к борьбе с сетевыми угрозами, упуская из внимания такой технический канал утечки информации как побочные электромагнитные излучения и наводки (ПЭМИН), в англоязычной литературе - «TEMPEST». Один из самых опасных видов ПЭМИН – это излучение кабелей видео-интерфейсов, так как по ним передается не кодируемая информация для отображения на устройствах вывода, и они работают, по сути, как слабые передающие антенны. Перехват по каналу ПЭМИН изображения мониторов не является чем-то новым, он был осуществлён впервые в середине 80-х и известен с тех пор как «перехват Ван Эйка», но опасность его для коммерческой информации на сегодня в РФ всё ещё недооценена. Целью данной работы было исследовать различные видео-интерфейсы на предмет интенсивности их ПЭМИН и оценка возможности перехвата и восстановления изображения.

Широкое распространение моноблоков естественным образом ставит вопрос о интенсивности их ПЭМИН, дальности их распространения, возможности перехвата и дальнейшего восстановления информации В работе исследовались ПЭМИН интерфейсов LVDS и eDP, применяемых в моноблоках для передачи изображения на монитор. В качестве измерительного оборудования применялись Спектральный коррелятор «OSC-5000» и самосборное устройство контроля радиочастотного диапазона в составе SDR–приемника «FOXWEY RTL SDR» (Realtek TL2832u) и логопериодической антенны «RTA–302–20 S».

Первым из исследованных ТСПИ был моноблок «Lenovo ThinkCentre Edge 92z 21.5». Тип видеоинтерфейса – LVDS. Непосредственно вблизи моноблока фиксируется широкий спектр частот создаваемых им излучений, однако при удалении на расстояние в 2 метра их интенсивность спадает практически до нуля, оставляя различимый набор пиков в диапазоне 430-440 МГц, где и была обнаружена несущая частота 432,5 МГц, на которой было восстановлено изображение, которое было, однако, весьма нечетким. Перейдя к следующему моноблоку, «Lenovo S50–30», с тем же типом видеоинтерфейса, дальнодействующий диапазон был обнаружен на частотах 630-650 МГц. На частоте 641,5 МГц было перехвачено изображение с хорошим качеством (рис.1).

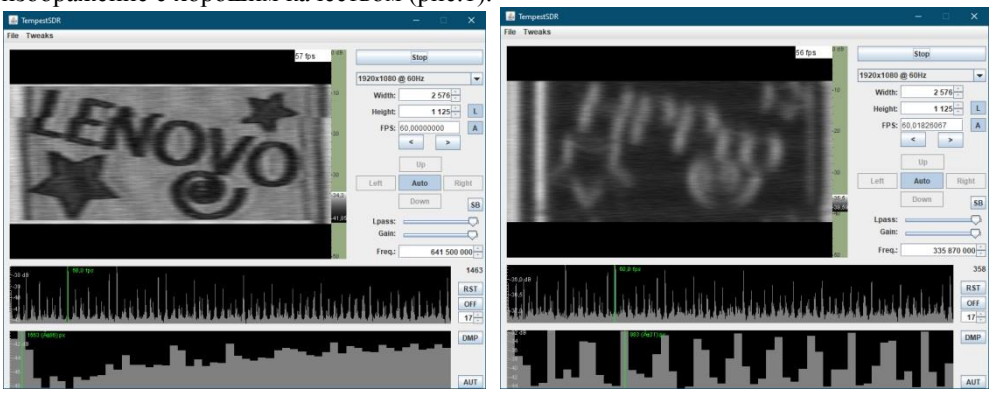


рис.1. Перехваченное изображение с дисплея моноблоков «Lenovo S50–30» и «HP ProOne 400»

Далее был исследован моноблок« HP ProOne 400» с видеоинтерфейсом LVDS. Дальнодействующая составляющая ПЭМИН была обнаружена в диапазоне 321–342 МГц. Изображение перехвачено на частоте 335,87 МГц, картинка нечеткая, однако надпись и фигуры все еще различимы (рис.1).

Моноблок «Acer Veriton Z4870G» с видеоинтерфейсом LVDS показал наличие диапазона частот 510–525 МГц. На частоте 519,1 МГц было перехвачено изображение в высоком качестве, аналогичном качеству перехвата для «Lenovo S50–30».

В результате было показано, что, не смотря на малую длину шлейфа видеоинтерфейса, ПЭМИН моноблоков представляет потенциальную опасность при обработке конфиденциальной информации. Разброс несущих частот разных моделей моноблоков, даже в рамках одного типа видеоинтерфейса и производителя. Это весьма неочевидный момент. Чисто теоретически основная несущая частота должна зависеть только он типа интерфейса и разрешения экрана. Но в рамках нашего исследования выставлялось одинаковое разрешение, а частота могла отличаться в 2 раза при одном и том же типа интерфейса. Отсюда следует вывод что для защиты информации по каналу ПЭМИН в офисе желательно использовать моноблоки одной модели. Предварительно необходимо протестировать их спектр ПЭМИН, определить основные несущие частоты и дальность их распространения. Работа большого количества однотипных моноблоков создаст эффект пространственного зашумления, что снизит вероятность выделения и перехвата сигнала нужного моноблока. В случае применения генераторов пространственного зашумления это повысит эффективность их противодействия перехвату.

Результаты перехвата изображения, выполненные в одинаковых условиях, наглядно показывают, что качество перехваченного сигнала сильно зависит от модели. Поэтому малому и среднему бизнесу, ограниченному в средствах и возможностях защиты информации, имеет смысл использовать моноблоки типа ThinkCentre Edge 92z 21.5., дающие максимально зашумленную, раздваивающуюся картинку, получаемую по итогам перехвата ПЭМИН, и требующую увеличения финансовых, временных и интеллектуальных усилий на восстановление изображения.

Оценка возможности несанкционированной установки систем слежения и прослушивающих устройств в гибридных автомобилях ПЭМИН

Полянский Дмитрий Александрович
Каменев Кирилл Ярославович
Дальневосточный федеральный университет
polyanskiy.da@dvfu.ru

В настоящее время существует множество различных способов несанкционированного получения информации. Прослушивание разговоров с помощью закладных устройств и отслеживание подвижного объекта с использованием технических средств определения местоположения являются такими способами. Устройства

устанавливаются скрытно и предполагают передачу информации по каналам, которые не влияют на человеческие органы чувств, при этом способны распространяться на большие расстояния. Ввиду доступности и большого выбора средств слежения и прослушки утечка информации является серьезной проблемой как для частных лиц, так и для компаний и государственных структур. Ввиду этого возникла потребность в использовании средств и методы обнаружения устройств негласного съёма информации.

Наличие в автомобилях большого объема электроники, которая уменьшает эффективность использования нелинейных локаторов для поиска закладных устройств, наличие большого числа труднодоступных мест для установки, невозможность визуального осмотра, все это усложняет поиск закладных устройств, по сравнению с задачей поиска в помещениях. Применение в автомобилях не только устройств прослушки, но и слежения ещё несколько усложняет работу специалиста по безопасности. Для обеспечения использования гибридной силовой установки в автомобиле установлено дополнительное оборудование с некоторыми особенностями, которыми могут воспользоваться злоумышленники. Автомобили с гибридной силовой установкой появились в широком потреблении, по сравнению с обычными автомобилями, недавно. Немногие люди имеют опыт обслуживания и знания устройства электроники гибридного автомобиля. Это снижает вероятность обнаружения закладного устройства при обследовании оборудования человеком не имеющего опыта обслуживания гибридного автомобиля. В данной работе будут рассмотрены места характерные для автомобиля с гибридной силовой установкой, которые могут быть использованы для установки закладных устройств на примере автомобиля Toyota Prius C.

В результате анализа технических особенностей конструкции автомобиля было выявлено, что наиболее удобным местом установки средств негласного съёма информации является разъём вентилятора охлаждения высоковольтной батареи. Помимо возможности быстрого подключения оно имеет 3 питающие линии с номиналом 14.4, 9.2, 4,4 В, что позволяет подключать устройства с разыми требованиями по питанию. Но мест установки можно предложить ещё множество, поэтому на примере этой линии было проверено, насколько изменяются параметры электрических цепей при подключении типичных радиозакладки и GPS-теркера. Разница оказалась минимальной (6,47А и 6,5А для закладки и 6,78А и 6,84А для трекера соответственно). Из этого был сделан вывод, что необходимо проводить паспортизацию электрических цепей автомобилей с использованием максимально точного оборудования и при периодических проверках обращать внимание даже на минимальные отклонения.

Установка закладных устройств непосредственно на высоковольтную батарею имеет ряд очевидных деконспиративных признаков. Периодическое сканирование состояния ВВБ может обнаружить факт установки закладного устройства на ВВБ. Довольно распространенным и дешёвым прибором для диагностики неисправностей автомобиля является диагностический адаптер ELM327 на базе микроконтроллера PIC18F25K80. Среди программ для диагностики автомобилей с гибридной силовой установкой, есть несколько, предлагающих проверку состояния батареи, такие как Hybrid Assistant, DR.Prius и MotorData. Наиболее точную информацию о состоянии элементов ВВБ даст приложение Hybrid assistance. При разборе ВВБ для установки устройств необходимо отключить аккумулятор автомобиля и разъединить контакты ВВБ путем извлечения специальной защитной чеки. Отключение электропитания автомобиля повлечет сброс данных с устройств имеющих ОЗУ. Компьютер, который отслеживает расход топлива и, исходя из этого, рассчитывает запас хода, теряет статистику и устанавливает запас хода по умолчанию, который очень завышен. Сбрасывается время. Сбрасываются настройки дополнительных устройств. Это является одним из деконспиративных признаков. Неправильная установка закладного устройства может вызвать возникновение ошибок, которые отображаются на приборной панели автомобиля.

Следующим этапом работы было изучение возможностей выявления подобных устройств в автомобиле с помощью приборов контроля радиочастотного диапазона. Использовался спектральный коррелятор OSC-5000. Сперва было выполнено определение зависимости интенсивности сигнала от расстояния между трекером и спектральным коррелятором, тем самым определены границы ближней зоны. Интенсивность сигналов от GPS-трекера на частотах 1580.87 MHz и 1584.94 MHz оказалась аналогична. Значимое превышение над фоновым уровнем излучения наблюдаются на расстоянии до 20 метров. Для типичного прослушивающего устройства с питанием 9В, нестабилизированного, использующего модуляцию WFM на частоте 71.01 МГц радиус ближней зоны оказался 60 метров. Необходимость использования достаточно мощных устройств вызвана тем, что съём информации необходимо осуществлять в движении, и следует обеспечить достаточную дальность до автомобиля с принимающим устройством, чтобы его присутствие не стало дополнительным деконспиративным признаком.

В результате проделанной работы выработаны методические рекомендации по поиску и противодействию установки закладных устройств в гибридные автомобили.

Разработка программного обеспечения сканера для поиска закладных устройств

Свинцицкий Михаил Юрьевич
Дальневосточный федеральный университет
Полянский Дмитрий Александрович
bandirart@gmail.com

В настоящее время защита от радиозакладных устройств является необходимой мерой для защиты конфиденциальной информации и сохранения коммерческой тайны. Радиоустройства могут использоваться для незаконного прослушивания, подслушивания, шпионажа и других противоправных действий. Проблема особенно актуальна для таких организаций как правительственные учреждения, банки, малые и крупные коммерческие компании.

Наиболее эффективным методом обнаружения радиозакладных устройств является анализ спектра сигналов с помощью анализаторов электромагнитного излучения, благодаря которым есть возможность обнаруживать электромагнитные волны на определенных частотах, определять тип модуляции, оценивать мощность сигнала и быстро сканировать радиочастотный диапазон. Однако, в связи с высокой стоимостью необходимого оборудования, не все компании имеют возможность провести контрразведывательные мероприятия данным способом. Создание недорогих, мобильных и простых в эксплуатации устройств контроля радиочастотного диапазона является важным направлением развития технологии, которое может помочь защитить частные и корпоративные сети от внешних угроз и обеспечить безопасность информации.

Целью данной работы является разработка программного обеспечения сканера радиочастотного спектра сигналов, который позволит заменить дорогостоящие профессиональные устройства для поиска простых радиозакладных устройств и существенно сократить расходы малобюджетных предприятий.

Для того, чтобы обрабатывать сигнал в режиме реального времени, анализатор должен иметь достаточные вычислительные мощности, обладать графическим интерфейсом и устройством вывода изображения для удобной настройки параметров и отображения результатов, поэтому в качестве обрабатывающего оборудования будет использоваться персональный компьютер с предустановленной операционной системой Windows.

В качестве приемника радиосигнала выбрано устройство SDR (Software Defined Radio). В зависимости от конкретной модели устройство может принимать сигнал с частотами от 500 кГц до 1,75 ГГц. Также, среди основных преимуществ SDR можно выделить встроенный аналого-цифровой преобразователь и USB интерфейс, с помощью которого полученный оцифрованный радиосигнал передается напрямую в программное обеспечение анализатора спектра.

Архитектура программного обеспечения включает в себя модули для получения данных от сканера, обработки и анализа сигнала, вывода результатов на экран пользователя. Исходный код программного средства написан на языке программирования C++ с использованием библиотеки SoapySDR для взаимодействия с устройствами SDR и получения потоковых данных. Важным аспектом работы является использование технологий языка C++ для реализации параллельных вычислений методами многопоточного программирования. Такой подход позволит увеличить производительность анализатора и скорость обработки данных. Пользовательский интерфейс и вывод результатов реализованы возможностями фреймворка Qt.

Особый интерес представляет применение преобразования Фурье для восстановления исходного сигнала из дискретизированного по времени, и последующего вывода его визуального представления на экран пользователя.

Обзор эксперимента Google на 53-кубитном процессоре Sycamore

Шауро Виталий Павлович
Shaurkin@hotmail.com

В 2018 году компания Google опубликовала результаты эксперимента, демонстрирующего так называемое «квантовое превосходство» на 53-кубитном процессоре Sycamore [1]. Под «квантовым превосходством» понимается некий условный порог, когда квантовый компьютер демонстрирует значительные преимущества в решении какой-либо задачи по сравнению с современными классическими суперкомпьютерами. Публикация вызвала большой резонанс не только в научном сообществе, благодаря широкому освящению в популярных СМИ и соцсетях. К тому же интерес к данной работе подогревался еще до

публикации различными слухами о якобы большом прорыве, сделанном Google в области квантовых вычислений.

Суть эксперимента состояла в выполнении на квантовом процессоре сложной квантовой сети, содержащей большое количество случайно генерируемых однокубитных гейтов (рис.1). Подобная квантовая сеть является крайне сложной для симуляции на классическом компьютере и требует экспоненциального увеличения вычислительных ресурсов при линейном росте числа задействованных кубитов. Условным классическим аналогом такой сети может служить сеть, где однокубитные гейты заменены на классический логический оператор NOT, срабатывающих с вероятностью 50%. Очевидно, что такая классическая сеть каждый раз будет выдавать случайную битовую строку, т.е. генерировать белый шум. Однако в квантовом случае из-за наличия фазы и запутывающих гейтов CNOT в процессе вычисления будет происходить интерференция состояний кубитов. В результате, на выходе квантовой сети мы будем наблюдать экспоненциальное распределение вероятностей (распределение Портера-Томаса), когда получение некоторых битовых строк будет гораздо более вероятным, а для других вариантов вероятность может быть близка к нулю. Данная особенность квантовой случайной сети является ключевой для эксперимента, поскольку позволяет на несколько порядков уменьшить количество запусков квантовой сети, необходимых для анализа полученного распределения вероятностей битовых строк. Так, например, для сети из 53 кубитов всего возможно 2^{53} или $\sim 10^{16}$ различных вариантов выходных битовых строк. В обычной ситуации для корректной оценки распределения вероятностей этих строк, количество запусков алгоритма должно быть минимум на пару порядков больше этого числа. Однако из-за экспоненциального распределения можно ограничиться лишь $N \sim 10^6 - 10^7$ запусков, при этом связанная с этим упрощением ошибка пропорциональна $1/\sqrt{N}$.

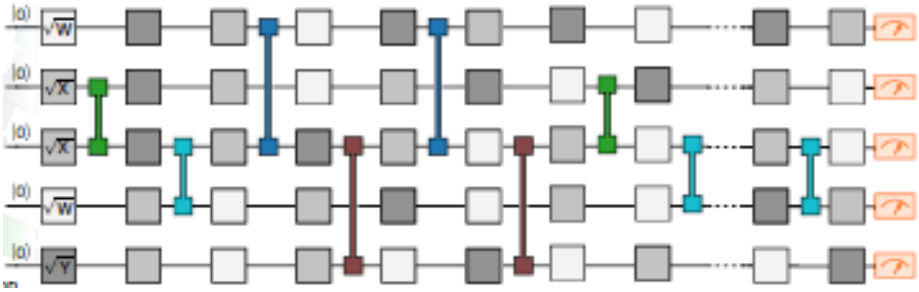


рис.1. Один из вариантов экспериментально реализованной квантовой сети [1]. Квадраты – однокубитные гейты, случайно выбираемые из 3 возможных вариантов $\sqrt{X}, \sqrt{Y}, \sqrt{W}$, где $W = (X + Y)\sqrt{2}$. Маленькие соединённые квадраты – гейты CNOT.

Для оценки точности экспериментальных данных авторы использовали методику кросс-энтропийного сравнения (cross-entropy benchmarking, XEB). Рассчитываемая функция точности F_{XEB} [1] в этом методе показывает, насколько полученное в эксперименте распределение вероятностей для битовых строк отличается от точного распределения, полученного из симуляции квантовой сети на классическом суперкомпьютере. При значении функции равном 1 мы имеем точное совпадение распределений, а значение 0 указывает, что квантовый процессор генерирует белый шум, т.е., по сути, переходит в классический режим работы. Рис.2a показывает значения F_{XEB} для трех вариантов квантовых сетей при увеличении количества кубитов в сети. Данный график является основным научным результатом эксперимента. Видно, что F_{XEB} быстро убывает с ростом числа кубитов, что связано с накоплением ошибок при выполнении квантовых гейтов. Тем не менее, экспериментальные значения хорошо согласуются с предсказаниями (сплошная линия), сделанными на основе теоретических моделей источников ошибок в процессоре. Данный результат, во-первых, показывает, что даже при большом количестве кубитов не возникает никаких непредвиденных новых механизмов ошибок. Во-вторых, процессор действительно работает в квантовом режиме, несмотря на высокий уровень ошибок при большом числе кубитов.

Рис.2b показывает уже больше «медийные» и дискуссионные результаты эксперимента. Увеличивая количество гейтов в сети, авторы перешли некий порог («квантовое превосходство»), когда уже невозможно выполнить симуляцию полной схемы (наиболее сложный вариант сети, с множеством связывающих кубиты вентилей CNOT) на классическом суперкомпьютере за приемлемое время. Путем экстраполяции авторы вычислили, что на симуляцию самой сложной экспериментально реализованной квантовой сети (более 1500 гейтов) суперкомпьютеру потребуется порядка 10000 лет, в то время как квантовый процессор выполняет 30 миллионов запусков за 200 секунд. Данные оценки вызвали немало критики в научном сообществе, как в части оценки времени классической симуляции, так и относительно «искусственности» выбранной задачи и, как следствие, невозможности ее практического применения.

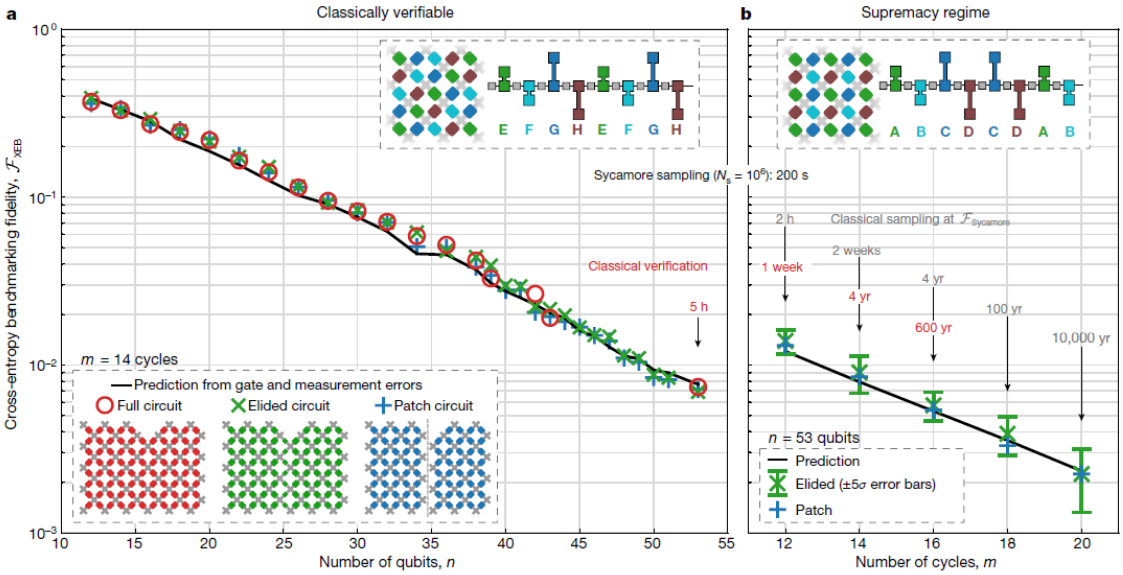


рис.2.Основные результаты эксперимента Google [1]: (a) Значения F_{XEB} при увеличении числа кубитов для трех вариантов квантовых сетей (полная и 2 упрощенных), сплошная линия – теоретические предсказания. (b)То же самое для 53 кубитов при увеличении числа гейтов в упрощенных схемах, приведены оценки для времени классической симуляции для полной схемы.

Список публикаций:

[1] Arute, F., Arya, K., Babbush, R. et al. // Nature 574, 505–510 (2019).