Министерство образования и науки Республики Казахстан

Восточно-Казахстанский государственный технический университет им. Д.Серикбаева

«Допущен к защите»
Заведующий кафедрой
_____Е.А. Малгаждаров
«_____» _____ 2019

ДИПЛОМНЫЙ ПРОЕКТ

На тему: «Анализ информационной безопасности современного автомобиля»

по специальности
5В071900 – «Радиотехника, электроника и телекоммуникации»

Выполнил **А.А. Жуебаев**

Научный руководитель **А.В. Русакова**

Усть-Каменогорск 2019

Министерство образования и науки республики Казахстан

Восточно-Казахстанский государственный
технический университет им. Д.Серикбаева

Кафедра «Приборостроение и автоматизация технологических процессов»

Специальность 5В071900 – Радиотехника электроника и телекоммуникации

ЗАДАНИЕ
на выполнение дипломного проекта (работы)

Студенту Жуебаеву А.А.

Тема проекта (работы): «анализ информационной безопасности современного автомобиля»

утверждена приказом по университету _____

Срок сдачи законченного проекта (работы)_____

Исходные данные к проекту (работе):характеристика связанные с анализом информационной безопасности современного автомобиля, положение на рынке выбранных устройств, планы разработки

Перечень подлежащих разработке в дипломном проекте(работе) вопросов или краткое содержание дипломной работы: написание литературного обзора по теме исследования информационной безопасности современного автомобиля, постановка задачи, программное обеспечение проекта, расчет экономической эффективности, рассмотрены вопросы по безопасности и экологичности проекта.

Перечень графического материала
Лист 1 Топология сети
Лист 2 Архитектура сети
Лист 3 Структура системы «Умный дом»
Лист 4 Блок – схема программы хранения данных

Консультации по проекту (работе) с указанием относящихся к ним разделов проекта (работы):

Раздел	Консультант (ФИО, должность, роспись)	Кафедра
1. Современное состояние информационной безопасности автомобиля	Русакова А.В – доцент	Приборостроение и автоматизация технологических процессов
2. Материалы и методы исследования	Русакова А.В – доцент	Приборостроение и автоматизация технологических процессов
3.Результаты исследований	Русакова А.В – доцент	Приборостроение и автоматизация технологических процессов
4. Экономическое и экологическое обоснование проекта	Русакова А.В – доцент	Приборостроение и автоматизация технологических процессов

Дата выдачи задания _____

Декан ШИТ _____ Н.К Ердыбаева
Руководитель проекта (работы) _____ А.В Русакова
Задание принял к исполнению студент _____ А.А. Жуебаев

Дата_____

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ADS (УСП) -	Advanced Design System	Усовершенствованная система проектирования
GPS -	Global Positioning System	Система глобального позиционирование
LVDS -	Low-Voltage Differential Signaling	низковольтная дифференциальная передача сигналов
LPI -	Low-power idle	Низкое энергопотребление
AVB -	Audio Video Bridging	Аудио видео мост
dBM -		Децибелы, миливаты
ED -		Обнаружение энергии
ESR -		Эквивалентные серии сопротивлений
EVM -		Увеличение вектора ошибки
FFD -		Полнофункциональное устройство
GPIO -		Универсальный ввод - вывод
OSI -	Open Systems Interconnection	Взаимодействие открытых систем
IEEE -		Институт электротехники и электроники
I -		Синфазная несущая
ISP -		Внутрисистемный программист
LOS -		Поле зрения
LQI -		Индикация качества связи
MAC -		Контроль доступа к среде
MIC		Код целостности сообщения
MSK		Минимальная смена
MN		Питающая сеть
OQPSK		Смещение квадратуроной фзовой модуляции
PA		Усилитель мощности
PAN		Персональная сеть
PCB		Печатная плата
PER		Частота ошибок пакета
PPU		Блок физического протокола
PHY		Физический уровень
Q		Квадратурная фазовая составлящая
RF		Радиочастота
RFD		Устройство с пониженной функциональностью
RTC		Часы реального времени
RTS		Готовы отправить
RX		Приемник

СОДЕРЖАНИЕ

		стр.
	ВВЕДЕНИЕ	6
1	СОВРЕМЕННОЕ СОСТОЯНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМОБИЛЯ	8
1.1	Поколение	12
1.2	Сети и уровни передачи данных	17
1.3	Стеки протокола	22
2	Материалы и методы исследование	24
2.1	Расчеты RAV	25
3	Результаты исследование	28
3.1	Определение качество сети	28
3.2	Подбитые кадры Ethernet	29
3.3	Демонстрация сервисных (Do S) атак	29
3.4	S OME/IP	32
3.5	Отравление ARP Cache	33
3.6	TCP угон	35
4	ЭКОНОМИЧЕСКОЕ И ЭКОЛОГИЧЕСКОЕ ОБОСНОВАНИЕ ПРОЕКТА	43
4.1	Экономическое обоснование проекта	43
4.2	Экология и безопасность проекта	47
4.2.1	Микроклиматические условия помещения	48
4.2.2	Требования по безопасности	49
4.2.3	Расчет общеобменной вентиляции на участке сборки	52
4.2.4	Защита атмосферы и сточных вод от загрязнения	54
	РЕЗУЛЬТАТЫ, ОБСУЖДЕНИЯ, ВЫВОДЫ	55
	СПИСОК ЛИТЕРАТУРЫ	57

ВВЕДЕНИЕ

Актуальность работы.

Уже более века автомобили являются неотъемлемой частью нашей жизни. Со временем эти транспортные средства становятся все более сложными, более оснащенными новейшими электронными устройствами для улучшения их эксплуатационно – технических свойств.

В 1990 г. электронные устройства и программное обеспечение составляли около 16 % стоимости автомобиля, в 2001 г. – 25 %, а в 2005 г. – до 40 % [1]. По оценкам специалистов Центра автомобильных исследований штата Мичиган, по состоянию на 2014 г. электроника и программное обеспечение составляют уже до 40-50 % [2] стоимости современного автомобиля. Также по данным Инженерной Ассоциации IEEE известно, что программное обеспечение представляет 90 % [3] инноваций в автомобилях.

Устойчивая тенденция увеличения количества электронных устройств в современных автомобилях с проводным и беспроводным подключением неизбежно приводит к росту уязвимостей, а значит – снижению безопасности и эффективности эксплуатации.

Требования к информационным системам современного автомобиля и к их пропускной способности растут вслед за появлением новых сложных приложений — например, систем обеспечения безопасности или систем обработки мультимедийной информации. Существующие сети управления транспортным средством, такие как LIN, CAN и FlexRay, не могут покрыть растущие требования по пропускной способности и расширяемости, которые нужны для различных систем помощи водителю. Новые сетевые технологии должны перенять как можно больше от бытовых и других неавтомобильных областей, но с учетом требований конкретных авто приложений. У Ethernet есть все предпосылки для такого комплексного подхода. Он может быть использован в основной магистрали для подключения различных областей, а также для подсетей, которые просто требуют большей пропускной способности.

Коммутируемая сеть Ethernet основана на связи «точка–точка», где пропускная способность более эффективно использована по сравнению с транслирующими системами, такими как CAN или FlexRay. Принцип коммутации может быть с успехом применен для преодоления границ доменов без затрат времени на упаковку и повторную сортировку передаваемых сообщений или пакетов, как это требуется в смешанном межсетевом интерфейсе.

Использование Ethernet в транспортном средстве означает смену парадигмы в разработке следующего поколения автомобильных компьютерных сетей: подключение различных сетевых доменов, транспортировки различных видов данных (управляющие сигналы, потоковая передача данных и др.) и выполнение строгих требований

надежности в тяжелых условиях расширенного температурного диапазона и электромагнитной совместимости.

Таким образом, анализ информационной безопасности современного автомобиля и поиск методов защиты информационных систем являются актуальными научными задачами и требуют изучения со стороны ученых и инженеров.

Цель дипломной работы: является повышение информационной безопасности автомобиля путем анализа возможных угроз и перспективных методов защиты информационных систем.

Для достижения поставленной цели в дипломном проекте поставлены и решены следующие задачи:

1) Проведен анализ литературных данных современного состояния информационной безопасности автомобиля
2) Сбор и наладка испытательного стенда
3) Проведение испытаний с использованием программного обеспечения Vector Informatik GmbH.
4) Выполнено технико-экономическое обоснование проекта.
5) Рассмотрены вопросы безопасности, экологичности производства и охраны труда.
6) Выводы

1. СОВРЕМЕННОЕ СОСТОЯНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМОБИЛЯ

В этой главе кратко описываются события, показывающие эволюцию до автомобильного Ethernet

Начиная с 1980-х годов производители автомобилей осознали, что им необходимо пересмотреть внутреннее устройство автомобиля. С одной стороны, использование большого количества кабелей, делали автомобиль громозким и неуклюжим, с другой стороны – появление новых функций требовали себе новые пути к управлению транспортом [4]. Вследствие того, что создание соединений точка-точка между всеми электронными блоками

На сегодняшний день новый автомобиль содержит от 50 до 100 и более электронных блоков управления [5]. В работе [6] указывается, что к 2025 г. 100 % автомобилей будут подключены к информационным системам, а в работе [7] – что к 2035 г. 75% автомобилей будут автономными.

Авторами ряда работ [8, 9] установлено, что злоумышленники могут получить удаленный доступ к электронным системам транспортных средств, управлять их компонентами или похищать личные данные автовладельцев. Помимо злоумышленников, атаки на автомобильные сети также могут проводиться в целях корпоративного шпионажа [10]. Современная аппаратура позволяет создавать различные степени повреждений – от радиочастотных помех вплоть до физического повреждения сетевых компонентов автомобиля.

Исследование состояния информационной безопасности показывает, что среди 173 исследованных автомобильных компаний по всему миру, число происшествий, выявленных в 2015 г. увеличилось на 32 % по сравнению с 2014 г. [11]. 98% всех протестированных программных приложений в автомобилях имеют серьезные дефекты, некоторые – от 10 до 15 [7]. В указанном исследовании приводятся и первые инциденты – взлом системы управления транспортом, приведший к аварии и пробкам на дорогах; кража автомобиля; блокирование GPS-отслеживания и угон инкассаторского автомобиля; взлом и перехват управления автомобилем Toyota Prius; произвольное ускорение автомобиля; подмена маршрута транспортных средств и т.д.

Стрелки» [10], установленные на дорогах Подмосковья, ущерб для областного бюджета составил около 2 млн. рублей. Причиной сбоя, как выяснили в правительстве Подмосковья, стал компьютерный вирус, который вывел из строя 130 камер из 144 на семь дней.

В 2015 г. эксперты журнала Wired [12] провели показательный дистанционный взлом компьютерной системы Uconnect нового автомобиля Jeep Cherokee. Действуя с помощью ноутбука из другого города, программисты Ч. Миллер и К. Валасек сумели получить доступ к важным функциям автомобиля, включая самопроизвольный разгон, торможение, работу стеклоочистителей и т.д. В результате 1,4 млн. автомобилей с

системой Uconnect соответствующей модификации были отправлены на сервис, а Национальное ведомство по вопросам дорожной безопасности NHTSA оштрафовало производителя на 105 млн. долларов [13] по целому ряду оснований: несвоевременный отзыв транспортных средств, недостаточный контроль безопасности, сокрытие информации от владельцев и властей и т.д.

По последним данным полиции Лондона [11], более трети всех угонов в столице Великобритании происходит с помощью перепрограммирования ключа зажигания, после чего преступникам требуется максимум 10с на кражу. Угонщики используют вредоносные компьютерные программы, в том числе для получения контроля над спутниками. Это дает им возможность послать с орбиты сигнал – разблокировать двери, отключить сигнализацию и запустить двигатель нужного автомобиля. Данная проблема касается не только премиальных моделей, все современные автомобили подвержены рискам высокотехнологичных угонов [13].

Автомобиль премиум – класса, выпуска начиная с 2012 года имеет около 100 EGUs [14]. Важным становится и сочетание информационно – развлекательной системы и вспомогательное вождение с помощью камер. В результате скорость передачи данных с одного объекта на другой не удовлетворяет всех потребностей современных транспортных средств. Ethernet для автомобилей является открытым стандартом и определяет два нижних уровня эталонной модели взаимодействия открытых систем. За последние десятилетия комитет по стандартизации IEEE 802 установил несколько физических уровней от 10 Мбит до 10 Гбит. IEEE 802.3u (100Base-TX) широко используется в бытовых и промышленных областях, а недавно был применен для диагностики автомобилей через IP, как описано в ISO 13400.

Более того, новые достижения в технологии позволили автомобильному Ethernet работать на одном кабеле неэкранированной витой пары (UTP).

В связи с тем, что Ethernet уже много лет является стандартом для соединения компьютеров, многолетний опыт взлома компьютеров может быть использован для взлома автомобилей. Только физический уровень автомобильной системы связи претерпевает значительные изменения с использованием новых схем кодирования и методов модуляции. Более высокие уровни в основном будут сохраняться в автомобильном Ethernet, поэтому безопасность стала главной проблемой.

На рисунке 1 показана типичная топология автомобильной сети с оптимальной защитой. К сожалению, не все коммуникации, обозначенные как безопасные, всегда верно. Как можно видеть, сеть состоит из нескольких сетей. Ethernet использует систему ADAS, систему помощи водителю. Это набор определенных алгоритмов, которые в разной степени помогают водителю в быстром принятии решений для безопасного и легкого управления транспортным средством. Компьютерная диагностика автомобиля (OBD, англ. On-board diagnostics) — это диагностика различных

систем автомобиля, производящаяся блоком управления автомобиля. Головным устройством, расположенным на приборной панели соединено все между собой центральным шлюзом.

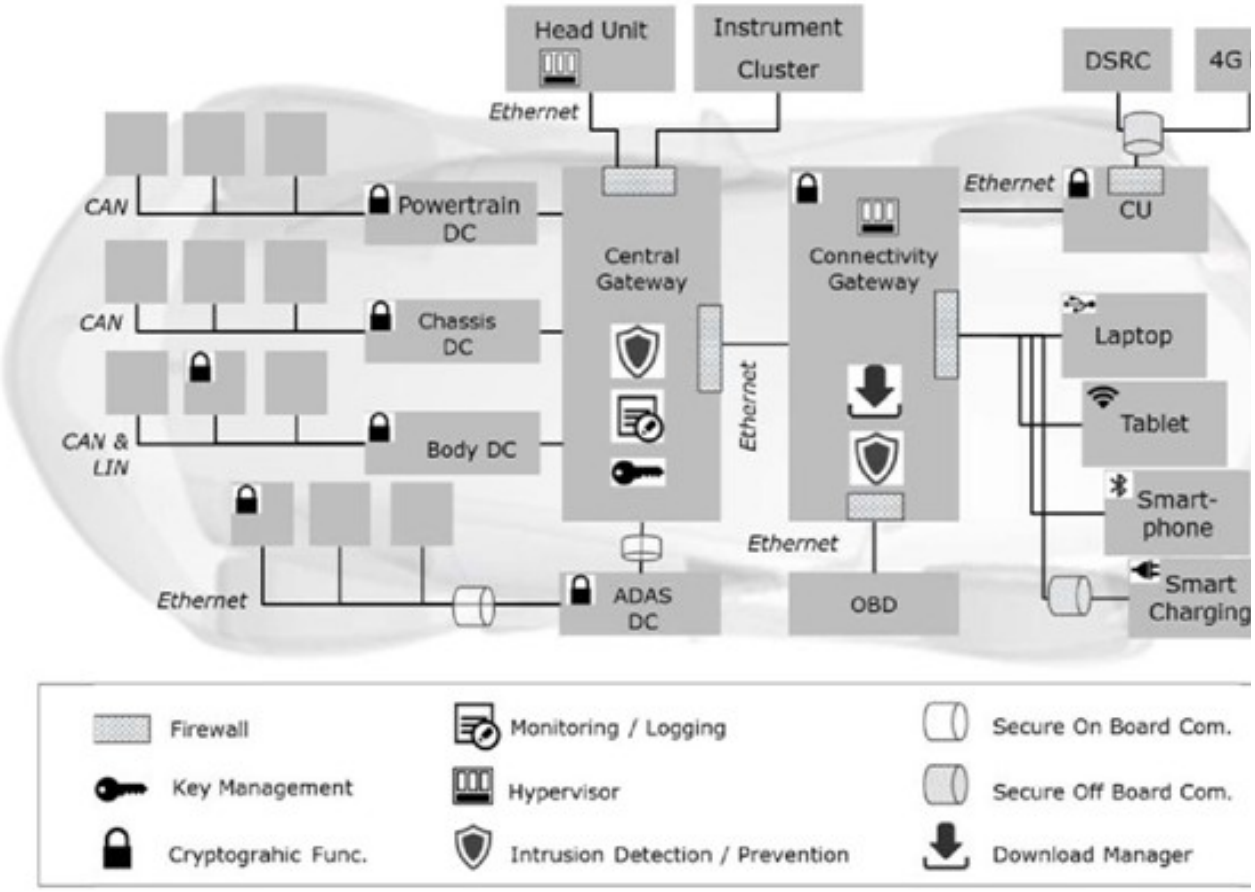


Рисунок 1 - Типичная топология современного автомобиля с оптимальной безопасностью

Группа специалистов по внедрению AVB-технологий (Audio/Video Bridging) из AVnu Альянса [15] определила IEEE-стандарты, включающие службы высокого уровня для IEEE 802-совместимых сетей (рисунок 2). Протоколы IEEE 802.1 AS, QAT, QAV и BA определяют расчет времени и синхронизации, распределение поточной передачи, перенаправление и организацию очередей в системах аудио/видео захвата. Кроме того, протокол транспортного уровня по стандарту IEEE 1722 облегчает поток чувствительного ко времени аудио и/или видео через AVB Ethernet-сети и совместимость между конечными станциями.

В системах помощи водителю для таких функций, как круговой обзор, все чаще используются видеокамеры. Деятельность по стандартизации на уровне протоколов связи и на физическом уровне недавно привела к появлению ISO 17215, который называется «Интерфейс передачи видео для камер». В целях дальнейшего развития автомобильной технологии Ethernet Broadcom сформировала организацию One Pair EtherNet (OPEN) Alliance

Special Interest Group. OPEN Alliance будет работать над стандартизацией компонентов и проводить тесты, основанные на технологии Broadcom Broad-Reach [16]. Другой целью группы является сбор требований для будущих технологий, таких как Reduced Pair Gigabit. Наконец, AUTOSAR (Automotive Open System Architecture) является открытой и стандартизированной архитектурой программного обеспечения для автомобильного Ethernet.

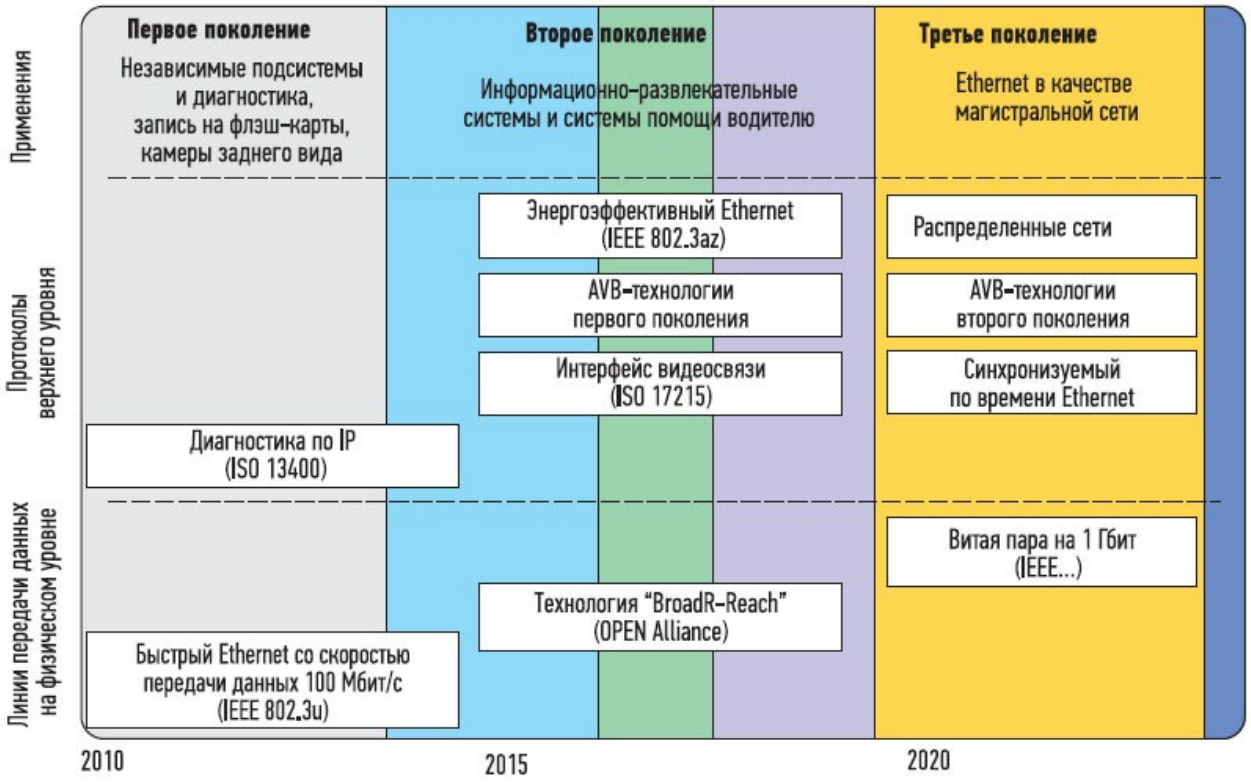


Рисунок 2 – Схема Ethernet: поколения и уровни

Ethernet не был разработан для сетей TDMA (множественный доступ со временным разделением или уплотнением, МДВУ), и все еще необходимо найти подходящее решение для достижения требуемой производительности в реальном времени и качества обслуживания. AVB уже включает в себя меры по обеспечению своевременной доставки медиа-потоков.

Для рабочей группы Automotive AVB Gen2 улучшение времени ожидания является одной из основных целей. Первое приложение синхронизированного по времени Ethernet (Time-Triggered Ethernet, TTE) было применено в авиационной технике [17] с высочайшими требованиями безопасности. Определенный в SAE AS6802 и отличный от аудио/видео технологий TTE основан на распределенном алгоритме тактовой синхронизации, который в конце концов приводит к получению точного, с детерминированным режимом, графика работы.

Хотя совместная интеграция AVB и TTE возможна [14], необходимы дальнейшие исследования, чтобы обеспечить их использование в автомобильных приложениях, где мультимедийные потоки, данные контроля в режиме реального времени, а также диагностическая информация и

обновления программного обеспечения должны передаваться в одной и той же сети.

1.1 Поколение

Поколение 1. Диагностика по IP

Первые приложения Ethernet в автомобилестроении — это встроенная диагностика и обновление flash-памяти ЭБУ. Для чтения диагностических данных и обновления программного обеспечения в течение отведенного времени производительность существующих систем, таких как CAN и FlexRay, была недостаточна. Ethernet 100 Base-TX категории 5 был выбран в качестве средства связи между автомобилем и диагностическим оборудованием. Высокая пропускная способность Ethernet экономит затраты на обслуживание и производство. ISO 13400 и ISO 14229 изменили существующие и определили новые, стабильные современные диагностические стандарты. Универсальные продукты и компоненты давно доступны, а такие требования, как прочность и температурные допуски, были смягчены для данного конкретного применения Ethernet в автомобиле.

Большая часть автомобильной электронной сети использует протокол управления передачей / Интернет-протокол (TCP/IP). Несмотря на то, что Министерство обороны США финансировало создание пакета TCP/IP, безопасность не была высокой в списке приоритеты в конце 1970-х годов, когда он был разработан, так как основной упор был сделан на коммуникацию для совместного использования ресурсов. Это привело к множественным уязвимостям, которые были обнаружены и использованы в реализациях стека протоколов TCP / IP. Некоторые из этих уязвимостей были задокументированы еще в 1989 году [6].

С учетом всего сказанного главный вопрос, который исследует этот тезис: «Является ли автомобильный Ethernet вместе с сопровождающими его протоколами безопасными и достаточно безопасными для автомобильной промышленности?»

Поколение 2. Системы помощи водителю и развлечения

Второе поколение автомобильного Ethernet будет заниматься информационно-развлекательными системами и видеонаблюдением для кругового обзора. Современные решения камер заднего вида часто используют LVDS (Low-Voltage Differential Signaling, низковольтная дифференциальная передача сигналов) для передачи видео, что хорошо работает в случае использования одной камеры. В недалеком будущем ожидается применение нескольких камер, а также получение данных с радиолокационного датчика расстояния (рисунок 3). LVDS-система становится неэффективной с точки зрения прокладки проводов и дороговизны кабелей и разъемов. Ethernet позволяет видеокамерам быть подключенными к центральному блоку управления для синхронизации и дальнейшей обработки.

Ethernet-камеры могут дополнительно использовать «энергоэффективный Ethernet» (IEEE 802.3az), в рамках которого вводится

Low-Power Idle (LPI, «режим простоя») и пробуждение по необходимости для экономии энергии, пока камеры не используются. Кроме того, решения для питания через Ethernet (PoE) являются предпочтительнее, поскольку они позволяют уменьшить количество проводов. Преимущества более высокой пропускной способности и низкого времени ожидания очевидны. Использование нескольких камер высокого разрешения для обнаружения объекта требует несжатой передачи данных, чтобы избежать образования артефактов сжатия при обнаружении препятствий, а также сильного драйвера с высокой пропускной способностью.

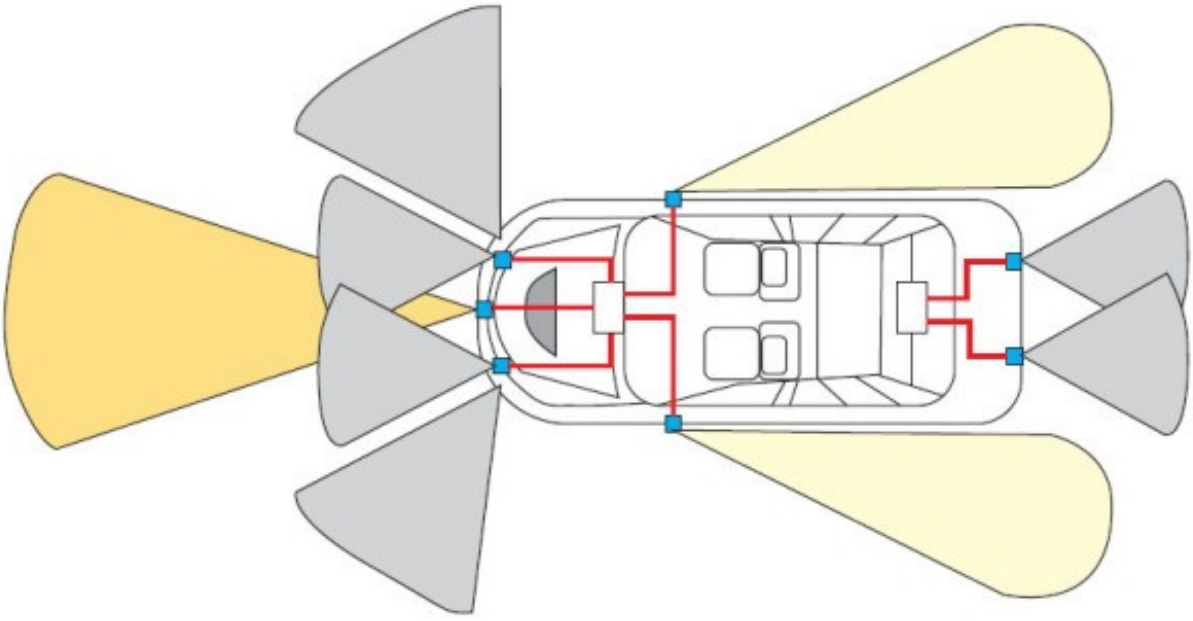


Рисунок 3 – Пример расположения камер и радаров для системы помощи водителю

Последние решения, касающиеся развлекательных систем, основаны главным образом на патентованных и не масштабируемых технологиях. Ethernet в этой новой области применения является экономически эффективным за счет использования стандарта AVB. Синхронизированная передача видео- и аудиоданных с гарантированной задержкой может быть достигнута с применением существующих AVB-компонентов Ethernet 1-го поколения. В этом направлении помогут развиваться как работа по стандартизации AVnu, так и самые последние разработки коммутирования и протоколов физического уровня (PHY) на основе Broad-Reach.

Поколение 3. Ethernet как основа сетей инфраструктуры

В то время как для первого и второго поколений работа Ethernet ограничивается устройством подсетей некоторых приложений, таких как информационно-развлекательные или системы помощи водителю, с третьим поколением Ethernet станет основой в автомобильной сети. Типичная магистраль показана на рисунке 4. При разработке такой сети основной

идеей будет двусторонняя связь между ЭБУ, которая организована через сетевое администрирование.

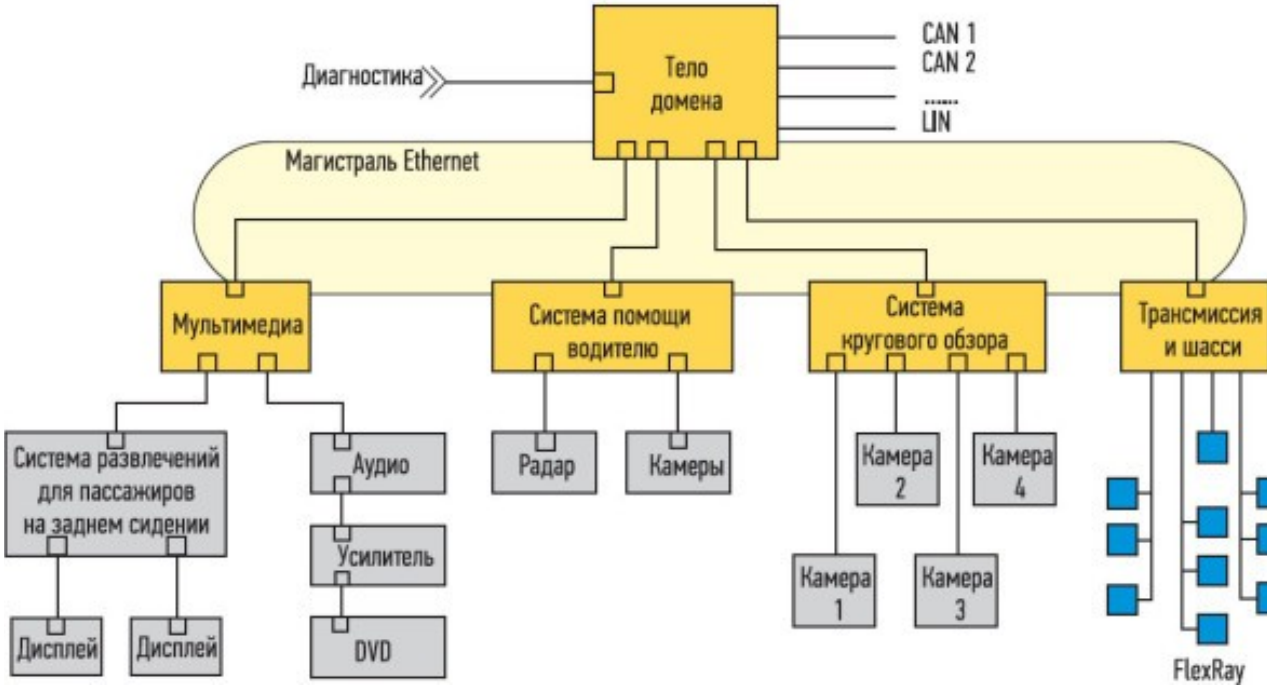


Рисунок 4 – Магистраль Ethernet в доменной архитектуре

Сеть связи будет иерархически организована с контроллерами домена, подключенными через магистраль Ethernet. Подсети ниже контроллеров домена могут также быть на основе Ethernet, с переключателями между уровнями. Эта структура обеспечивает масштабируемое решение, поскольку каждый порт коммутатора в общем случае может быть реализован как 10-Мбит, 100-Мбит и 1-Гбит без каких-либо изменений в высших уровнях протокола. Новизна подхода заключается в том, каким образом сообщение передается через доменные границы к месту назначения. В современных сетях и межсетевых интерфейсах реализация этой функции заключается в IP-маршрутизации с помощью коммутаторов и роутеров, что и предлагается для магистральных сетей. Преимущество заключается в полной независимости IP-маршрутизации от конкретной реализации, что позволяет создать единое решение для автомобильной сети. Кроме того, идея IP позволяет легко подключить автомобиль к Интернету [8] (эта возможность важна главным образом тем пользователям, кто хочет иметь в машине доступ к интернет-услугам в той же степени, что и в домашних условиях).

Еще одной особенностью новой архитектуры является то, что будет только одна магистральная сеть Ethernet, в которой должна осуществляться передача различных классов данных: диагностическая информация, видео/аудио-потоки и высоконадежные данные управления. В то время как AVB Ethernet и TTE уже могут обеспечивать различные уровни качества обслуживания в режиме реального времени, необходимо продолжать

исследования и разработки для проверки безопасного сосуществования этих различных классов передачи данных в одной сети.

BroadR-Reach — 100-Мбит Ethernet для автомобильных решений

Хотя 100-Мбит Ethernet и IP- технология были доступны с начала 1990-х гг., прошло почти два десятилетия, прежде чем появился интерес к ним как к следующему поколению стандартных сетей со стороны автомобильной промышленности. Это произошло отчасти из-за отсутствия должного физического уровня, подходящего для использования в транспортных средствах. Рисунок 5 показывает технические принципы и объясняет, почему ориентированный на потребителя физический уровень Fast и Gigabit Ethernet не применим в машине. Fast Ethernet базируется на MLT-3 сигнальной схеме (выделение трех уровней «+»/«0»/«–») и имеет однонаправленную связь по двум витым парам кабеля. Gigabit достигает десятикратного роста скорости передачи данных путем введения двунаправленного обмена на четырех витых парах кабеля и сигнальной схемы PAM-5. Чтобы компенсировать 6-дБ потери сигнал–шум в PAM-5 по сравнению с MLT-3 и избежать ошибок, используется решетчатый код (код Треллиса).

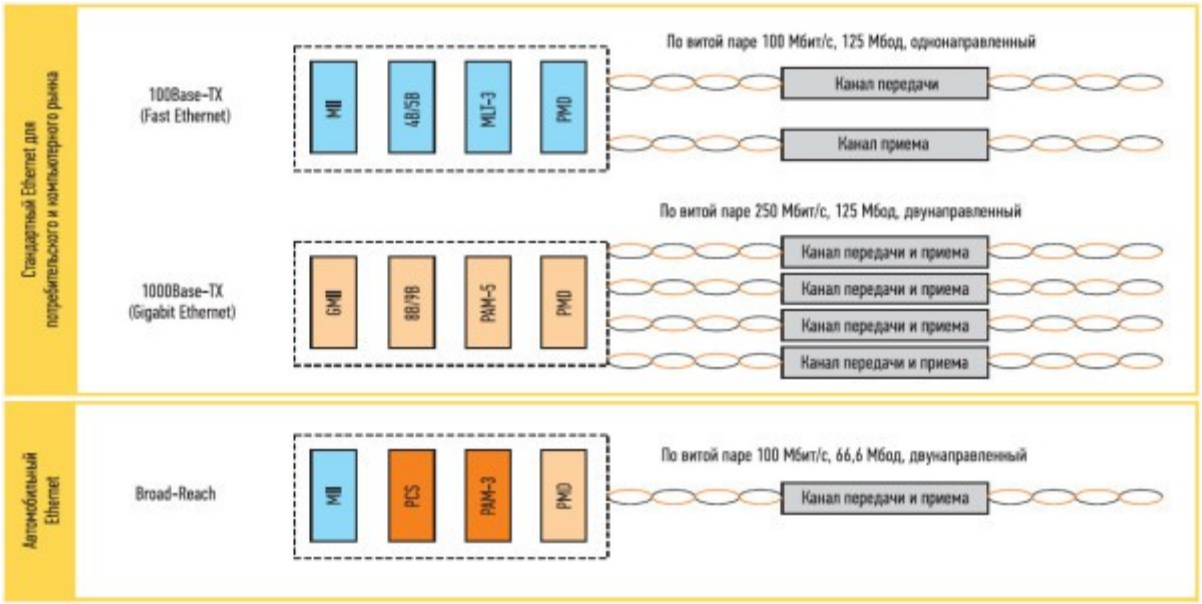


Рисунок 5 – Схемы кодирования стандартного Ethernet и BroadR-Reach

Высокая скорость передачи в 125 Мбод для Fast и Gigabit Ethernet вносит значительный вклад в электромагнитное излучение в критическом FM-радиодиапазоне и, следовательно, исключает использование недорогой неэкранированной витой пары в автомобильной среде. С использованием Broad-Reach технологии удалось почти вдвое сократить скорость передачи (до 66,6 Мбод), что позволяет использовать неэкранированную витую пару. В принципе, Broad-Reach можно рассматривать как «легкую» версию Gigabit с двунаправленной связью при использовании только одной пары проводов. Благодаря PAM-3 сигнализации может быть достигнута передача данных с погрешностью менее 10-10 даже без внесения поправок на ошибки.

Применение в автомобиле навязывает значительно более высокие требования к электронным системам и их компонентам (по сравнению с обыкновенным потребительским применением) главным образом с точки зрения электромагнитной совместимости [ISO11452] и условий окружающей среды. Первые исследования показали, что Broad-Reach подходит для использования в автомобиле. Однако для достижения надежности следующего поколения автомобильных сетей должны быть разработаны новые оптимизированные компоненты (рисунок 6). По сравнению со стандартным Fast Ethernet, спецификации могут быть значительно снижены. Применение емкостной связи вместо обычного трансформатора, усиления на аппаратном уровне — в составе протокола физического уровня, синфазных дросселей (CMC), разделительных конденсаторов, разъемов и кабеля неэкранированной витой пары — все это очень похоже на FlexRay или CAN-связь.

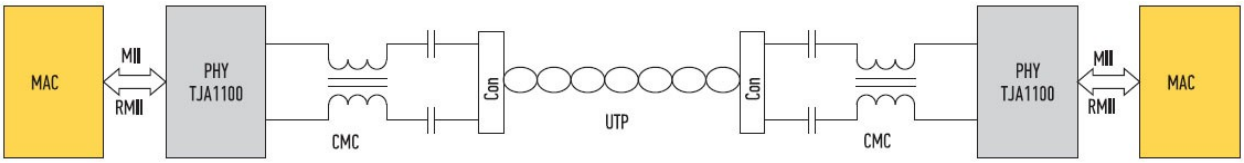


Рисунок 6 – Диаграмма Broad-Reach системы

Протокол физического уровня в качестве интерфейса между аналоговыми средствами передачи и цифровыми MAC-контроллерами во многом определяет надежность связи. В то время как потребительский протокол физического уровня оптимизирован для поддержки кабелей длиной более 100 м, в автомобиле, как правило, приходится иметь дело с длиной менее 10 м. Задача здесь состоит в том, чтобы найти источник импульсов и приемник, оптимизированные для таких длин кабеля, которые смогут удовлетворить строгим требованиям излучения и защищенности. На рисунке 7 показан спектр сигнала передатчика NXP с оптимизированным формированием импульсов, доказывающим, что проблема излучения может быть решена без использования дорогостоящего фильтра низких частот. Для сравнения: соответствующий спектр сигнала передатчика Fast Ethernet показывает более высокий сигнал в критическом FM-диапазоне.

Технология Broad-Reach, допускающая использование неэкранированной витой пары, делает Ethernet экономически конкурентоспособным для применения в автомобильной промышленности. FlexRay-кабель в состоянии справиться с тяжелыми условиями окружающей среды, поэтому он применим для автомобильного Ethernet. Однако, в отличие от бытовых применений, требуется тщательное изучение влияния условий окружающей среды (главным образом температуры) на целостность сигнала Ethernet.

Рисунок 8 иллюстрирует сравнительное моделирование глазковой индикации на 20 м кабеля FlexRay при комнатной и повышенной (+105 °C)

температурах кабеля. Большая «сжатость» глазковой диаграммы при высоких температурах указывает на рост межсимвольной интерференции (ISI) в результате ограничения пропускной способности кабеля. Пока длина кабеля составляет менее 20 м, снижение отношения сигнал–шум может быть обычно скомпенсировано адаптивным выравниванием в приемнике без увеличения частоты появления ошибочных битов.

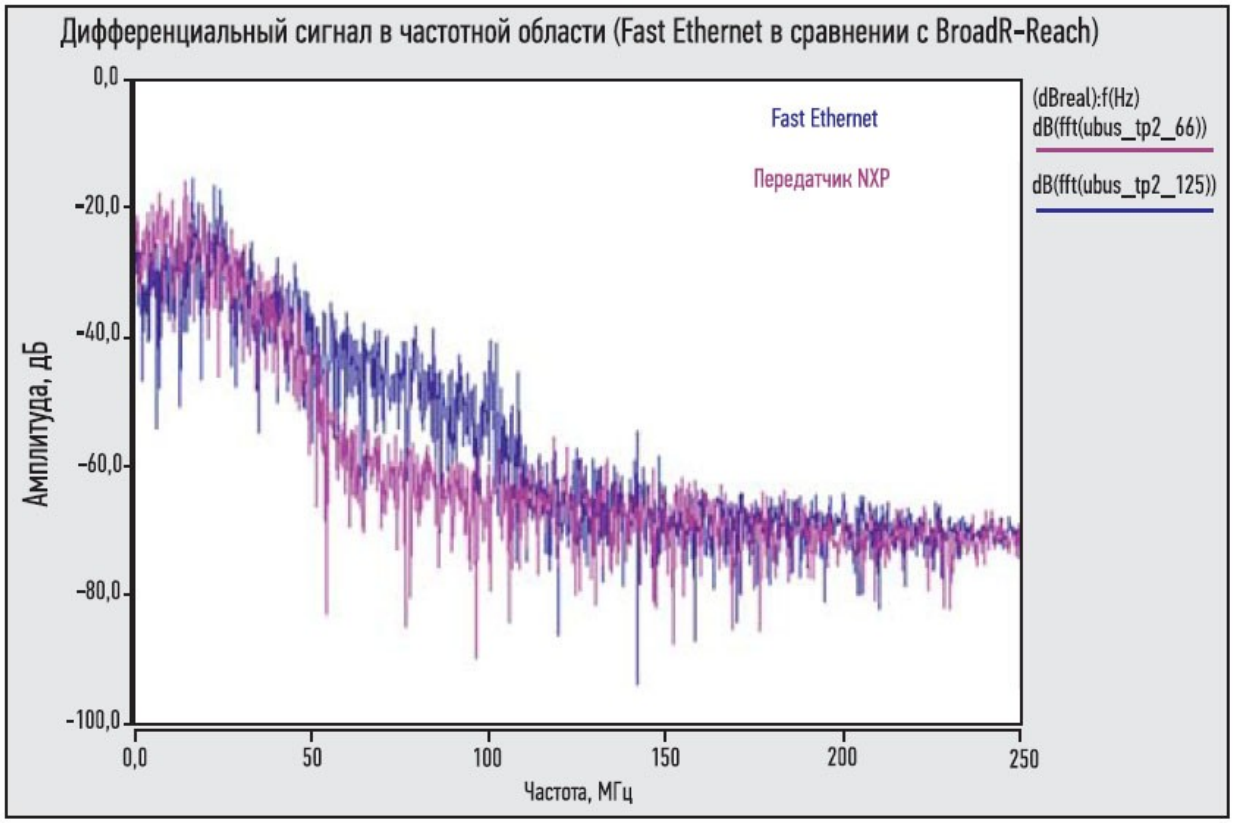


Рисунок 7 – Спектр сигналов

1.2 Сети и уровни передачи данных

В первые годы существования компьютеров люди понимали, что необходимо найти способ передачи данных с одного устройства на другое без использования портативных носителей. Кроме того, необходимо было использовать дорогостоящее периферийное оборудование, которое присутствует не на всех устройствах. В настоящее время в автомобильной сфере имеется несколько датчиков и исполнительных механизмов, которые необходимо соединить и в дальнейшем использовать эти данные для автоматизации.

Сеть объединяет группу устройств вместе для определенной цели или для нескольких целей. Эти сетевые устройства называются хостами. Интернет-протокол версии 4 (IPv4) использует термин хост для всех устройств в сети [10]. В отличие от этого, интернет-протокол версии 6 (IPv6) идет дальше и определяет узлы как «устройство, которое реализует IPv6», а хост - это «любой узел, который не является маршрутизатором» [11].

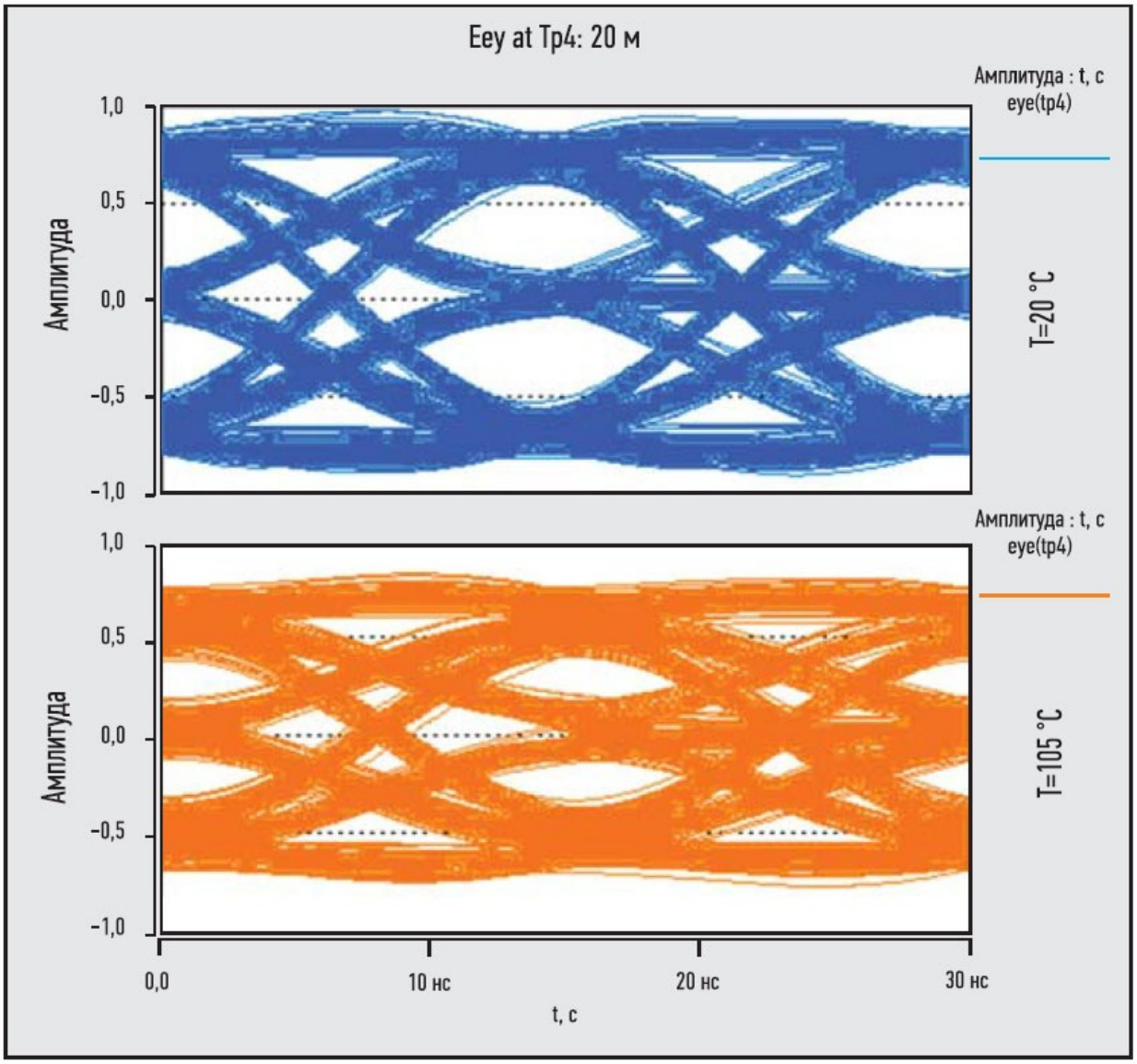


Рисунок 8 – Глазковая диаграмма сигнала

Сетевая модель OSI — это эталонная модель взаимодействия открытых систем, на английском звучит как Open Systems Interconnection Basic Reference Model. Ее назначение в обобщенном представлении средств сетевого взаимодействия. То есть модель OSI — то обобщенные стандарты для разработчиков программ, благодаря которым любой компьютер одинаково может расшифровать данные, переданные с другого компьютера. Чтобы было понятно, приведу жизненный пример. Известно, что пчелы видят все окружающее их в ультрафиолетовом свете. То есть одну и ту же картинку наш глаз и пчелиный воспринимает абсолютно по-разному и то, что видят насекомые, может быть незаметно для зрения человека. То же самое и с компьютерами — если один разработчик пишет приложение на каком-либо программном языке, который понимает его собственный компьютер, но не доступен ни для одного другого, то на любом другом устройстве вы прочитать созданный этим приложением документ не сможете. Поэтому

пришли к такой идее, чтобы при написании приложений следовать единому своду правил, понятному для всех [18,19]. Эталонная модель OSI показана на рисунке 9, а путь, по которому данные перемещаются от одной точки к другой в соответствии с моделью ISO OSI показан на рисунке 10.

Уровни OSI Для наглядности процесс работы сети принято разделять на 7 уровней, на каждом из которых работает своя группа протоколов [20]. Сетевой протокол — это правила и технические процедуры, позволяющие компьютерам, объединенным в сеть, осуществлять соединение и обмен данными. Группа протоколов, объединенных единой конечной целью, называется стек протоколов [21,22]. Для выполнения разных задач имеется несколько протоколов, которые занимаются обслуживанием систем, например, стек TCP/IP. Давайте здесь внимательно посмотрим на то, каким образом информация с одного компьютера отправляется по локальной сети на другой компьютер.

Задачи компьютера ОТПРАВИТЕЛЯ [23]:

1. Взять данные из приложения;
2. Разбить их на мелкие пакеты, если большой объем, подготовить к передаче, то есть указать маршрут следования, зашифровать и перекодировать в сетевой формат.

Задачи компьютера ПОЛУЧАТЕЛЯ [24]:

1. Принять пакеты данных;
2. Удалить из него служебную информацию;
3. Скопировать данные в буфер. После полного приема всех пакетов сформировать из них исходный блок данных и отдать его приложению.

Для того, чтобы верно произвести все эти операции и нужен единый свод правил, то есть эталонная модель OSI. Вернемся к уровням OSI. Их принято отсчитывать в обратном порядке и в верхней части таблицы располагаются сетевые приложения, а в нижней — физическая среда передачи информации. По мере того, как данные от компьютера спускаются вниз непосредственно к сетевому кабелю, протоколы, работающие на разных уровнях, постепенно их преобразовывают, подготавливая к физической передаче.

Разберем их подробнее.

1. Прикладной уровень (Application Layer) Его задача забрать у сетевого приложения данные и отправить на 6 уровень.
2. Уровень представления (Presentation Layer) Переводит эти данные на единый универсальный язык. Дело в том, что каждый компьютерный процессор имеет собственный формат обработки данных, но в сеть они должны попасть в 1 универсальном формате — именно этим и занимается уровень представления.
3. Сеансовый уровень (Session Layer) У него много задач. Установить сеанс связи с получателем. ПО предупреждает компьютер-получатель о том, что сейчас ему будут отправлены данные. Здесь же происходит

распознавание имен и защита: идентификация — распознавание имен аутентификация — проверка по паролю регистрация — присвоение полномочий Реализация того, какая из сторон осуществляет передачу информации и как долго это будет происходить. Расстановка контрольных точек в общем потоке данных для того, чтобы в случае потери какой-то части легко было установить, какая именно часть потеряна и следует отправить повторно. Сегментация — разбивка большого блока на маленькие пакеты.

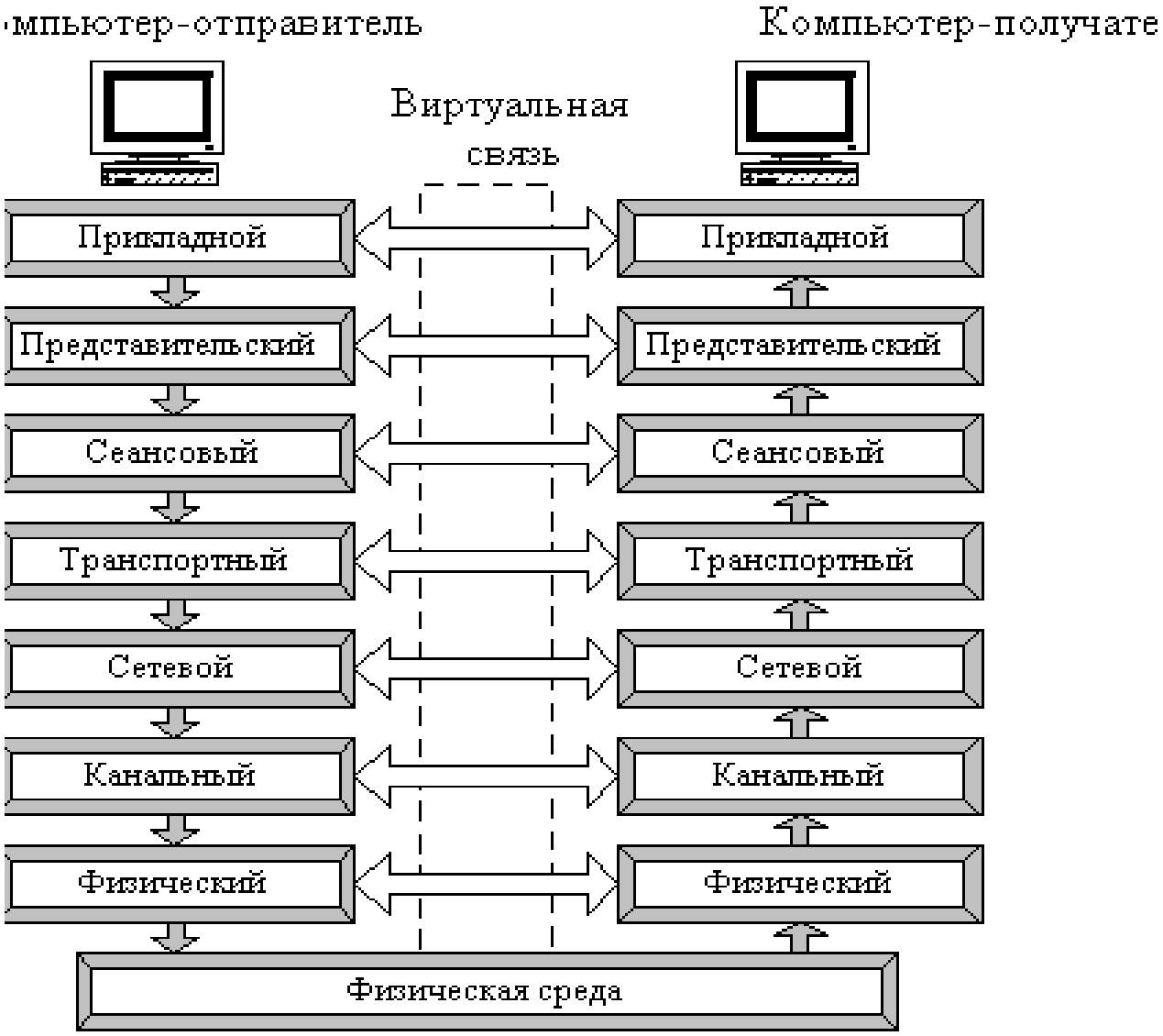


Рисунок 9 – Эталонная модель OSI

4. Транспортный уровень (Transport Layer) Обеспечивает приложениям необходимую степень защиты при доставке сообщений. Имеется две группы протоколов: Протоколы, которые ориентированы на соединение — они отслеживают доставку данных и при необходимости

запрашивают повторную отправку при неудаче. Это TCP — протокол контроля передачи информации. Не ориентированные на соединение (UDP) — они просто отправляют блоки и дальше не следят за их доставкой.

5. Сетевой уровень (Network Layer) Обеспечивает сквозную передачу пакета, рассчитывая его маршрут. На этом уровне в пакетах ко всей предыдущей динформации, сформированной другими уровнями, добавляются IP адреса отправителя и получателя. Именно с этого момент пакет данных называется собственно ПАКЕТОМ, у которого есть IP адреса (IP протокол — это протокол межсетевого взаимодействия) [25]
6. Канальный уровень (Data Link Layer) Здесь происходит передача пакета в пределах одного кабеля, то есть одной локальной сети. Он работает только до пограничного маршрутизатора одной локальной сети. К полученному пакету канальный уровень добавляет свой заголовок — MAC адреса отправителя и получателя и в таком виде блок данных уже называется КАДРОМ.

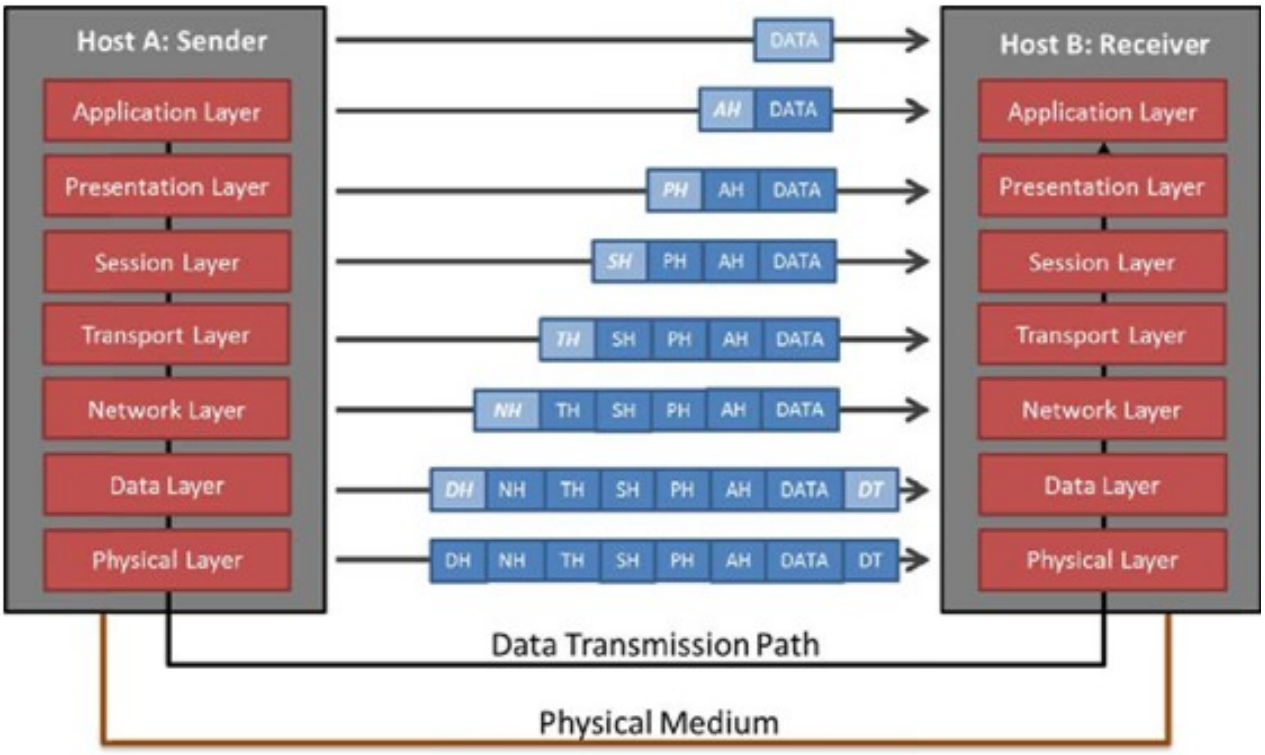


Рисунок 10 – Схема перемещения данных от одной точки к другой в соответствии с моделью ISO OSI

При передачи за пределы одной локальной сети пакету присваивается MAC не хоста (компьютера), а маршрутизатора другой сети. Отсюда как раз появляется вопрос серых и белых IP, о которых шла речь в статье, на которую была выше дана ссылка. Серый — это адрес внутри одной локальной сети, который не используется за ее пределами. Белый —

уникальный адрес во всем глобальном интернете. При поступлении пакета на пограничный роутер IP пакета подменяется на IP этого роутера и вся локальная сеть выходит в глобальную, то есть интернет, под одним единственным IP адресом. Если адрес белый, то часть данных с IP адресом не изменяется.

7. Физический уровень (Transport layer) Отвечает за преобразование двоичной информации в физический сигнал, который отправляется в физический канал передачи данных. Если это кабель, то сигнал электрический, если оптоволоконная сеть, то в оптический сигнал. Осуществляется это преобразование при помощи сетевого адаптера.

1.3 Стеки протоколов

Стеки протоколов TCP/IP — это стек протоколов, который управляет передачей данных как в локальной сети, так и в глобальной сети Интернет. Данный стек содержит 4 уровня, то есть по эталонной модели OSI каждый из них объединяет в себе несколько уровней (рисунок 11) [26].

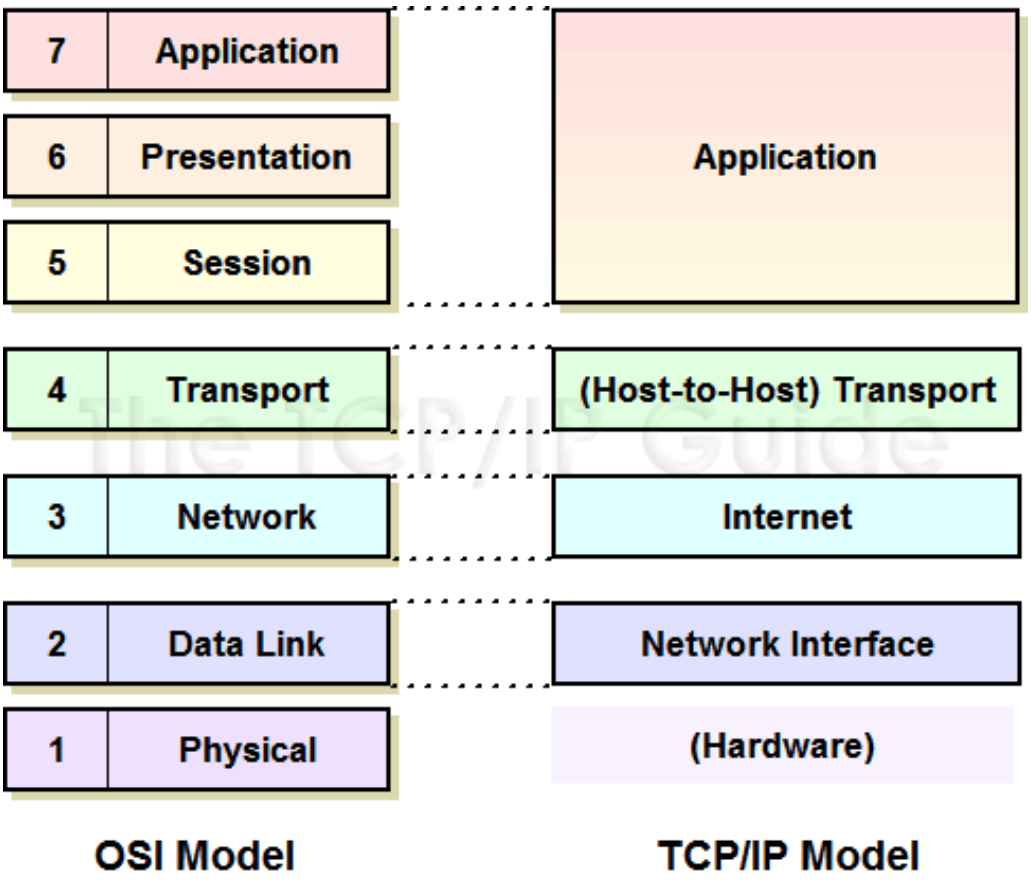


Рисунок 11 – Стеки протоколов OSI TCP/IP

1. Прикладной (по OSI — прикладной, представления и сеансовый)/
За данный уровень отвечают протоколы:
TELNET — удаленный сеанс связи в виде командной строки
FTP — протокол передачи файлов SMTP — протокол пересылки почты

POP3 и IMAP — приема почтовых отправлений
HTTP — работы с гипертекстовыми документами
2. Транспортный (по OSI то же самое) — это уже описанные выше TCP и UDP.
3. Межсетевой (по OSI — сетевой) — это протокол IP
4. Уровень сетевых интерфейсов (по OSI — канальный и физический)За работу этого уровня отвечают драйверы сетевых адаптеров.

2. МАТЕРИАЛЫ И МЕТОДЫ ИССЛЕДОВАНИЯ

В качестве основного метода исследования использовали собственно собранный испытательный стенд (рисунок 12), состоящий из

- устройства Vector VC121-12 ECU, предназначенного для прототипирования и мелкосерийного производства спортивных автомобилей и сельскохозяйственных машин. Оснащен интерфейсом Flex Ray, 6 CAN, 2 LIN и 1 Ethernet Broad-Reach. Более подробную информацию об этом можно найти в техническом описании [60];
- устройства Vector VN5 610A – для связи сетевого интерфейса в ПК.

Этот ECU использует физический уровень 100Base-T1 (как отмечалось ранее, он также известен как Broad-Reach). Для связи с персональным компьютером (ПК) необходим сетевой интерфейс для взаимодействия между двумя различными физическими уровнями 100Base-T1 блока ECU и 100Base-TX.

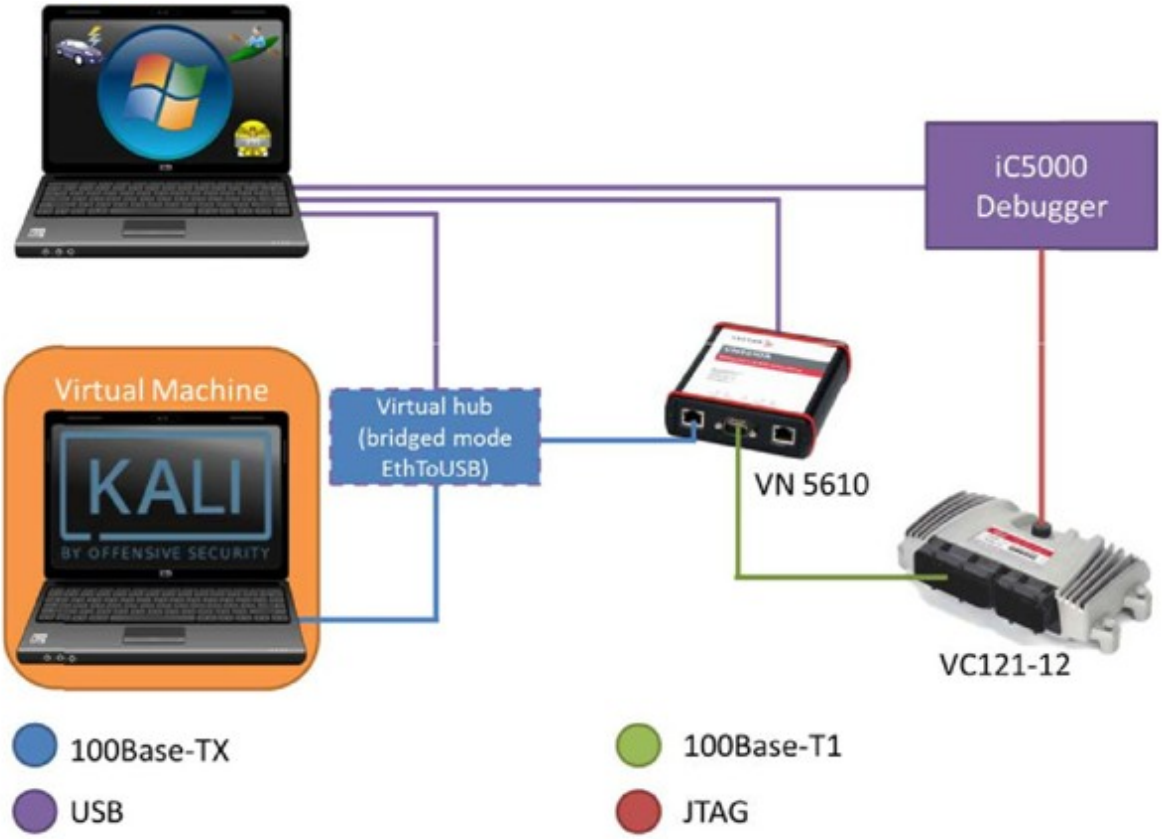


Рисунок 12 – Стенд для проведения измерений

Зеленая линия на рисунке 12 представляет автомобильное Ethernet-соединение от ECU, а синяя линия представляет стандартный Ethernet-порт 100Ba se, который подключается к конвертеру Ethernet-USB через USB-порт. На компьютере установлен виртуальный компьютер Mac с операционной системой Kali Linux [59]. Кали была выбрана по нескольким причинам. Во-первых: OS специально разработан для тестирования на проникновение, отсюда и множество необходимых инструментов. Вследствие строгой регламентации корпоративных программ, утвержденных отделом обработки данных, они могут быть установлены в Windows. В виртуальной машине, с другой стороны, единственное правило заключается в том, чтобы хранить его

и отключать доступ к файлам компании. Следовательно, виртуальная машина Kali была идеальным выбором. Виртуальная машина Ethernet Адаптер настроен для работы в режиме моста с физическим преобразователем USB-Ethernet, эффективно выступающим в качестве концентратора между Windows, Linux и ECU.

Так как инструменты Vector и другие инструменты программирования разрабатываются для Windows, настройка и настройка (т. Е. Компиляция, перепрошивка и отладка) выполняются непосредственно с ПК. Однако сетевые инструменты, интегрированные в Kali, превосходят возможности тестирования Windows. По этой причине тестирование в основном производится с виртуальной машины Kali. Основным элементом на диаграмме является встроенный в кристалл анализатор iC5000 iSY STEM AG (см. Раздел 3.4.2 .3), являющийся отладчиком, имеющим прямое соединение JT AG с ЭБУ. Это соединение JTAG делает возможным мигание и отладку ЭБУ.

Конечным результатом анализа данных является определение поверхности атаки. Как уже упоминалось, эта поверхность атаки представляет собой векторы, из которых наша область видимости уязвима. Как таковая, это очень объективная мера безопасности. Точнее, поверхность атаки определяет отношения между операциями, средствами управления и ограничениями.

2.1 Расчеты RAV

OSSTMM определяет RAV как скалярную метрику для измерения поверхности атаки. Преимущество наличия метрики для безопасности заключается в том, что она применима ко всем системам. Еще одним преимуществом оценок RAV является то, что они могут быть легко пересчитаны при изменении системы или оценке влияния дополнительного контроля. Рисунок 13 показывает как RAV-оценки могут быть использованы для отслеживания безопасности системы за определенное время. RAV выражаются через логарифмическое уравнение по основанию 10. Балл RAV, равный 100, представляет собой идеальный баланс между операциями, средствами управления и ограничениями, а реби - идеальной безопасностью. Хотя это обычно интерпретируется в процентах, на самом деле это логарифмическая шкала, значения которой могут превышать 100. Значения больше 100 указывают на избыточные контроли. Это может показаться желательным, но может быть проблематичным, так как дополнительные средства управления увеличивают сложность и в некоторых случаях добавляют взаимодействия.

Как гласит методологическая статья, тот факт, что шкала является логарифмической, помогает «понять общую картину» [6]. По этой причине термин «фактическая безопасность» был введен раньше. Этот принцип применим ко всем каналам и передает одну и ту же информацию. В руководстве приведен пример компьютерной системы 1000 и 10 компьютерной системы, в которой один и тот же показатель RAV

сопоставим. Руководство идет дальше, сравнивая компьютерные сети со зданиями, и показывает, что даже в этом случае RAV-результаты сравнимы.

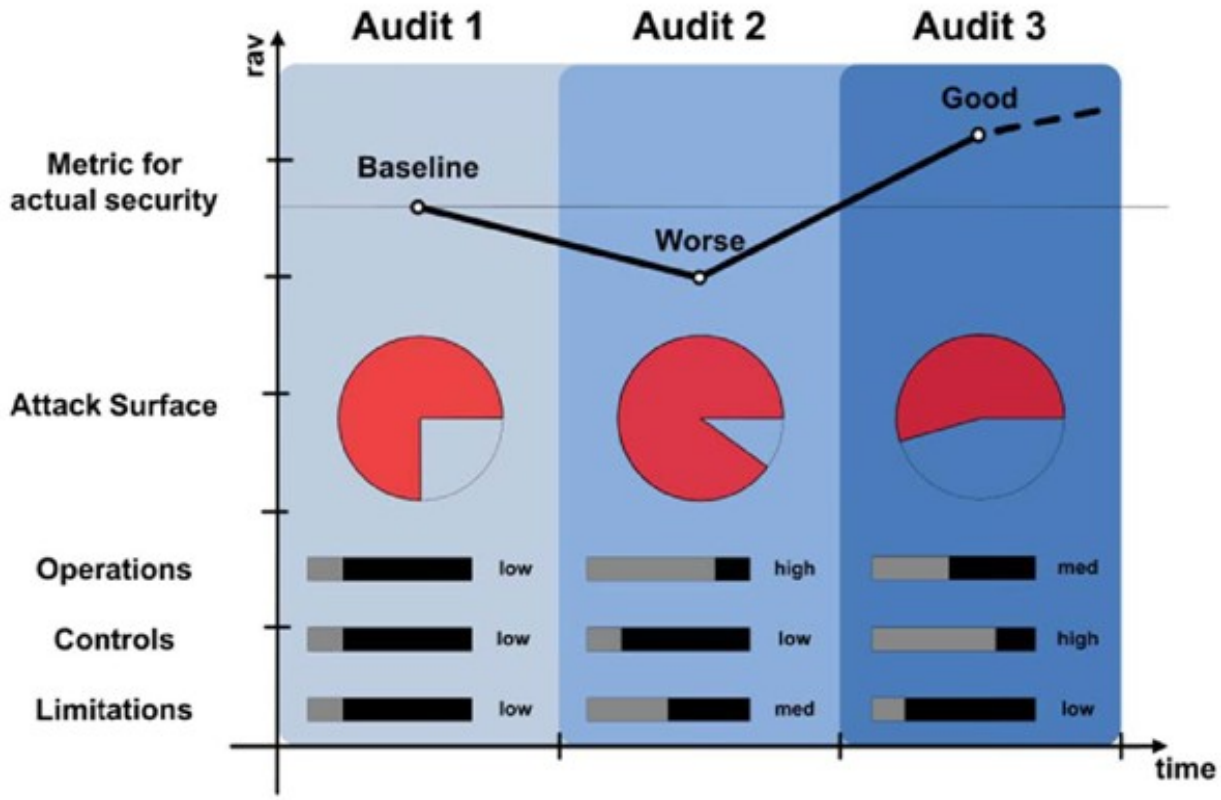


Рисунок 13 - Секретность, выраженная в RAV-показателях с течением времени [6]

Информация, собранная с помощью тестов безопасности сетей передачи данных, будет использоваться для расчета баллов RAV, тем самым описывая систему с точки зрения операций, средств управления и ограничений.

Электронная таблица калькулятора RAV, предоставленная ISECOM, будет использоваться для расчета баллов RAV. Эта электронная таблица доступна на [70].

Баллы RAV являются основным средством оценки безопасности системы. Они дают общий балл за безопасность системы, и легко увидеть последствия любых изменений в системе. Для оценки этой работы автор решил рассчитать несколько баллов RAV для разных конфигураций системы, чтобы их можно было сравнить. Различные системы были определены следующим образом:

a) Базовая оценка RAV, которая представляет реализацию стека Vector TCP / IP без каких-либо специальных настроек, связанных с безопасностью.

b) Оценка RAV для стандартной реализации стека TCP / IP со всеми уязвимыми протоколами, которые не были реализованы в стеке Vector TCP / IP.

c) Несколько оценок RAV для различных связанных с безопасностью конфигураций, которые стек Vector TCP / IP реализовал во время написания этой диссертации (статический кэш ARP, отключенные ICMP-эхо-запросы и подписи встроенного программного обеспечения).

d) Оценка RAV, в которой все связанные с безопасностью конфигурации объединены в одной системе.
e) Оценка RAV с возможными будущими реализациями для повышения безопасности (например, шифрование, подписи и т. д.).

Ожидается, что оценка RAV системы (b) будет иметь более низкую оценку RAV, чем базовая система (a), поскольку она имеет больше операций при сохранении того же числа элементов управления. Ожидается, что оставшиеся системы будут иметь более высокие оценки RAV, поскольку все они реализуют средства управления, которые отсутствуют в системе (a), или избавляются от избыточных операций, которые присутствуют в системе (a).

3. РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЙ

3.1 Определение качества сети

Ставилась задача с использованием испытательного стенда протестировать канал и определить ориентир для взаимодействия сети с системой.

Пакеты программ отправлялись туда и обратно между виртуальной машиной и ECU. Запросы по разным протоколам отправлялись в ЭБУ. Измеряли время отклика и скорость передачи пакета данных. Протестированными протоколами являются ICMP (эхо-запросы), TCP (инициализация соединения TCP с отправкой пакета с установленным флагом SYN) и UDP (используется в сообщениях запроса идентификации транспортного средства DoIP). Все пакеты отправлялись сто раз, а минимальное, среднее и максимальное время ответа сохранено.
Минимальное, среднее и максимальное время отклика приведены в таблице 1.

Таблица 1 – Результаты, по определению качества сети

Время отклика (мс)				
Протокол	Минимум	Среднее значение	Максимум	Потеря пакета
ICMP	0.490	1.335	2.108	0%
TCP	0.898	3.363	6.374	0%
UDP	495.003	497.918	500.508	0%

Для сетевого протокола ICMP были отправлены эхо-запросы и собраны соответствующие эхо-ответы. Время между моментом отправки запроса и моментом получения соответствующего ответа измеряется как время ответа.
В случае тестов TCP был отправлен сегмент TCP с флагом SYN, а соответствующий сегмент TCP с установленными флагами SYN и ACK был перехвачен. Время между исходящим и входящим сегментом было принято за время ответа.

Метод измерения был немного другим для случая UDP. Поскольку UDP является протоколом без установления соединения, и не существует такой вещи, как пинг UDP, пришлось использовать альтернативные средства. Когда дейтаграмма отправляется на открытый порт UDP, она просто использует ее, и ответ не отправляется, если не запрашивается ни один. С другой стороны, когда закрытый порт принимает дейтаграмму UDP, RFC 792 заявляет, что: «… хост назначения может отправить сообщение о недоступности пункта назначения хосту источника». [71]. Однако, поскольку недоступным местом назначения является сообщение ICMP типа 3, которое не реализовано в стеке Vector, оно не будет отправлено. Это означает, что без отправки законного запроса на известный открытый порт невозможно выполнить какие-либо измерения. Поэтому пакет DoIP на основе UDP был создан и отправлен в ECU. Отправленный запрос является сообщением запроса идентификации транспортного средства, как указано в ISO13400 [74]. Поскольку запрос требует некоторого времени обработки в ЭБУ, время ответа намного больше, чем в случае двух других протоколов.

3.2 Подбитые кадры Ethernet

Как известно, кадры локальной сети Ethernet должны иметь минимальную длину 64 байта. Из этих 64 байтов в отформатированном кадре Ethernet II, 22 байта принадлежат данным со статической длиной, таким как адреса источника и назначения, тег VLAN и проверка циклическим избыточным кодом. Преамбула и начало разделителя кадров не учитываются в 64 байтах, поскольку они обрабатываются на физическом уровне и всегда одинаковы. Оставшиеся 44 байта должны быть либо полезными данными, либо заполнением, если они слишком короткие.

RFC 894 [76] определяет, что заполнение должно состоять из октетов (байтов) нулей. Однако было отмечено, что многие производители не выполняют заполнение, как того требует RFC, а используют части памяти, иногда память ядра для заполнения кадров. В ошибочной реализации злоумышленник может просто отправить несколько эхо-запросов ICMP и в ответ получить потенциально ценную информацию о памяти. Таким образом наша цель состояла в том, чтобы убедиться, что конфиденциальные данные не передаются через заполнение кадров Ethernet.

Эхо-запросы с протокола ICMP отправляются с виртуальной машины Kali и фактической машины с ОС Windows 7. Кроме того, проверяется заполнение других пакетов.

Результаты исследований показали, что через заполнение не просачиваются конфиденциальные данные. Пакеты ответа на эхо-запросы реализуются в соответствии с RFC 792 [71], что означает, что ответ будет иметь ту же полезную нагрузку, что и запрос. Запросы от Windows и Kali с их соответствующими ответами от ECU можно увидеть на рисунке 14. Невозможно было генерировать более короткие сообщения ICMP из Windows или из Linux, потому что сетевая карта автоматически добавляет заполнение. Автору не удалось найти способ отключить автоматическое заполнение. Из-за этого были также исследованы ответы на запросы TCP и UDP. В этих ответах ECU пришлось добавить отступы, потому что данные были слишком короткими. Было установлено, что заполнение соответствует RFC 894 [76], поэтому уязвимости нет.

3.3. Демонстрация сервисных (Do S) атак

Цель DoS и распределенных DoS-атак состоит в том, чтобы перегружать каналы связи не релевантными данными, чтобы действительные запросы не могли быть обработаны. Существует множество вариантов таких взломов, и от них довольно сложно защитить себя. Обычные DoS-атаки можно предотвратить с помощью фильтров и брандмауэров. IP-адрес, с которого начинается атака, может быть полностью заблокирован, или информация, полученная с него, может быть отфильтрована. Когда это делается в сочетании с DoS-атакой, существует опасность блокирования легитимного хоста сети. Механизм, обеспечивающий непризнание, поможет в фильтрации от законного общения.

Kali Request			ECU Response		
[-] ICMPv4			[-] ICMPv4		
| Type:	Echo Request (PING)	08	| Type:	Echo Reply (PONG)	00
| Code:	0	00	| Code:	0	00
| Chcksum:	1908	0774	| Chcksum:	3956	0F74
| Id:	1814	0776	| Id:	1814	0716
| Seq Num:	2	0002	| Seq Num:	2	0002
[-] Payload			[-] Payload		
| Length	56 bytes		| Length	56 bytes	
DD 98 9A 59 00 00 00 00 A8 AE 0A 00 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37			DD 98 9A 59 00 00 00 00 A8 AE 0A 00 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37		
| ASCII			| ASCII		
Ý˜šY....¨®.....!"#$%&'()*+,-./01234567			Ý˜šY....¨®.....!"#$%&'()*+,-./01234567		

Windows Request			ECU Response		
[-] ICMPv4			[-] ICMPv4		
| Type:	Echo Request (PING)	08	| Type:	Echo Reply (PONG)	00
| Code:	0	00	| Code:	0	00
| Chcksum:	18747	493B	| Chcksum:	20795	543B
| Id:	1	0001	| Id:	1	0001
| Seq Num:	1056	0420	| Seq Num:	1056	0420
[-] Payload			[-] Payload		
| Length	32 bytes		| Length	56 bytes	
61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69			61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69		
| ASCII			| ASCII		
abcdefghijklmnopqrstuvwabcdefghi			abcdefghijklmnopqrstuvwabcdefghi		

Рисунок 14 - эхо-запросы ICMP и ответы

Цель теста: затруднить процесс перепрограммирования с помощью DoS-атаки по протоколу TCP.

Сцена: последнее ложе, как показано на рисунке 12 Сеанс прошивки работающей прошивки занял место между ECU и vFlash, работающими на ПК. Виртуальная машина Кали выполняет атаку.

Процесс: Процесс перепрошивки выполняется через DoIP. Поскольку большие файлы отправляются, связь DoIP проходит по TCP. Tcpkill, часть dsniff, - это программа, созданная для тестирования сети. Он прослушивает текущие соединения TC P на выбранных хостах и прерывает их, вставляя

пакеты с флагом RST в канал связи. Это приводит к разрыву соединения педа.

Результат: Рисунок 15 показывает, как выглядит нормальный процесс прошивки с vFlash. В дальнейшем можно увидеть захват Wi-reshark связи T CP между vFlash и ECU.

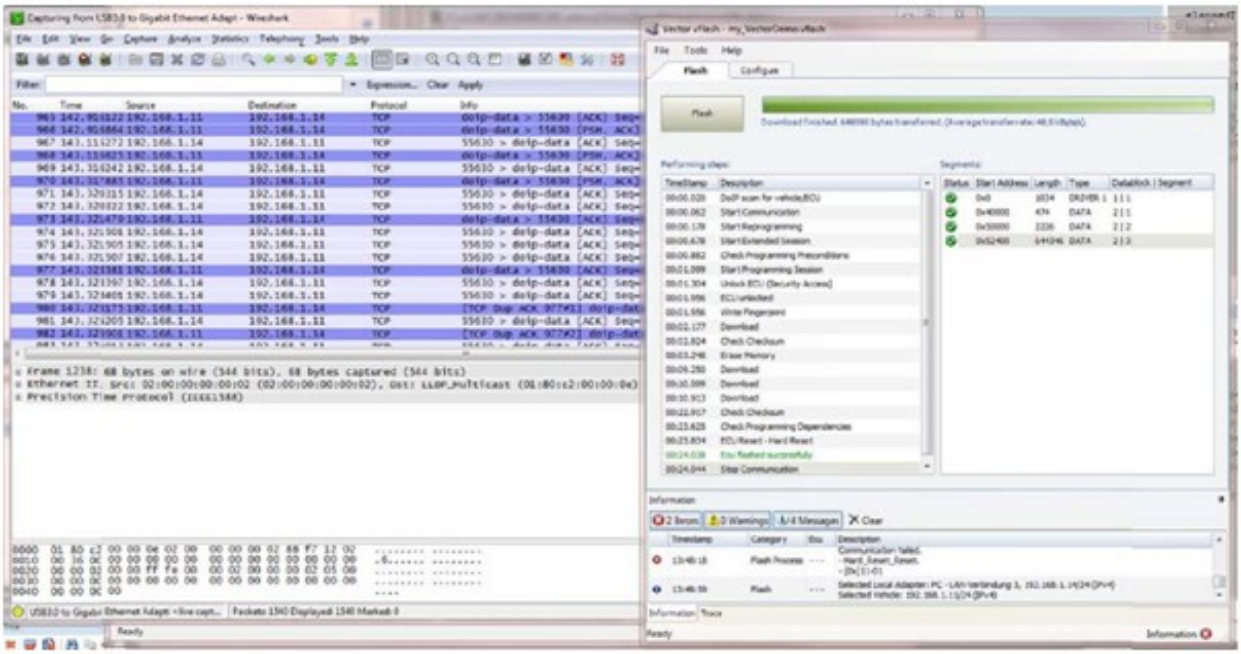


Рисунок 15 - Обычный процесс вспышки

Рисунок 15 показывает, что происходит, если tcp kill запускается до запуска процесса перепрошивки.

Появляется сообщение об ошибке «Связь не удалась» и RST помечает TCP

Сегменты можно увидеть в окне Windows. Это про одну из уязвимые возможности самого протокола TCP. Как защитить себя от атак такого типа? заключается в использовании шифрования, следовательно, последовательность следствий не будет ясной, и, следовательно, ее будет сложнее расшифровать. Другим способом могут быть криптографические подписи, которые обеспечат невозвращение источника. И то, и другое можно реализовать, отправляя трафик TCP через виртуальную частную сеть или используя IPsec.

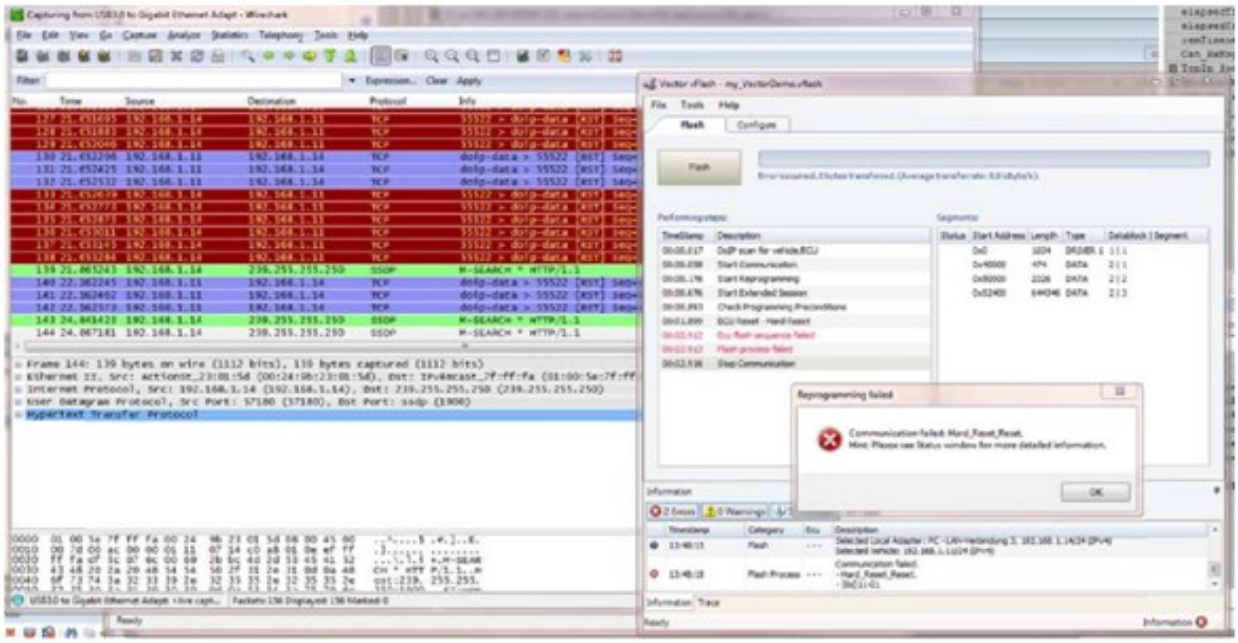


Рисунок 16 - Процесс перепрошивки прерван из-за DoS-атаки

3.4 S OME/IP

Подделка

В ответ на это злоумышленник отправляет поддельные пакеты, которые принимающий хост не может отличить от тех, которые он на самом деле ожидает.

Цель теста: доказать, что в некоторых случаях возможна подделка и подделка SOME / IP.

Сцена: испытательный стенд, как показано на рисунке 12. На ЭБУ запущено прикладное программное обеспечение с текущими сообщениями SOME / I P.

Процесс: ЭБУ обменивается НЕКОТОРЫМИ / IP-данными с ПК. Данные графически представлены в виде непрерывной функции, похожей на цепную пилу, из нескольких треугольников (как показано на рисунке 17). На Kali запускается сценарий, который отправляет специально созданные пакеты с разными данными.

Результат: как только скрипт запускается, линии на графике становятся неправильными, как показано на рисунке 17. Это доказывает, что подделка возможна. В данном примере последствия представляют собой просто некорректный график. Однако то же самое можно было бы сделать с потоком с камеры, который подается в систему управления оперативным движением, которая отвечает за поддержание заданного расстояния от автомобиля впереди. Последствия такой атаки пугающие. SOME / IP все еще является относительно новым протоколом, над которым ведется работа. Рассматриваются некоторые опции безопасности, такие как Secure Onboard Commication (SecOP) и d(TLS) [77]. Другим решением было бы

использование безопасного протокола передачи данных в реальном времени (SRTP) [78], который обеспечивает шифрование, целостность и аутентификацию сообщений в сочетании с мультимедийным интернет-ключом (MIKEY) [79], который ключевое решение для управления, которое предоставляет сеансовые ключи для SR TP.

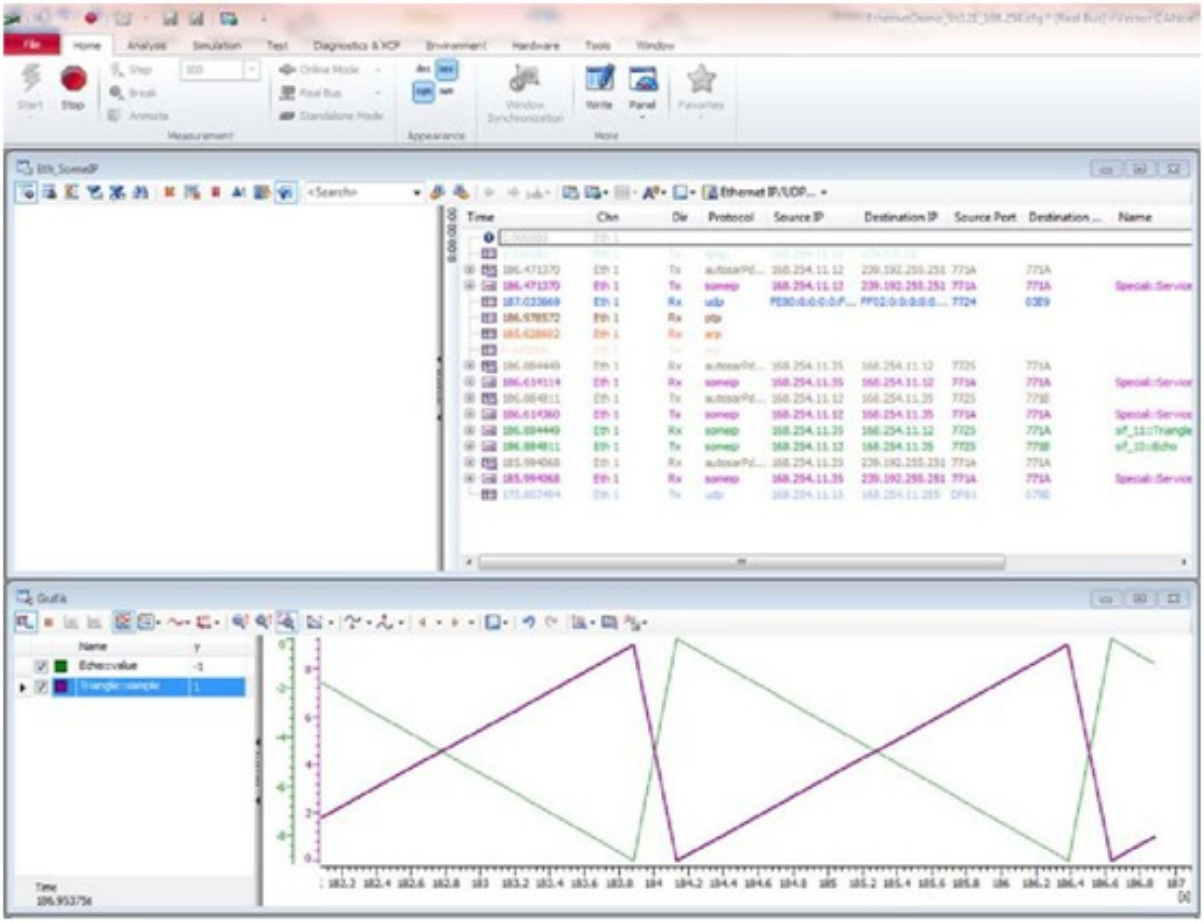


Рисунок 17 - Некоторые / IP-данные представлены графически

3.5 Отравление ARP Cache

При отравлении кэша ARP подделанный ответ ARP или запросы отсылаются злоумышленником для того, чтобы скомпрометировать (отравить) кэш ARP атакующего хоста. Таким образом, используется действительный IP-адрес, чтобы атакующий узел связывал MAC-адрес злоумышленника с действительным IP-адресом. После этого злоумышленник получает все данные, предназначенные для законного хоста. Он может фильтровать данные и пересылать некоторые данные на законный хост или контролировать весь обмен данными без пересылки чего-либо на законный хост. Отравление кэша ARP обычно делается для большинства атакующих людей. Это может быть даже полезно для атаки TCP Hijacking.

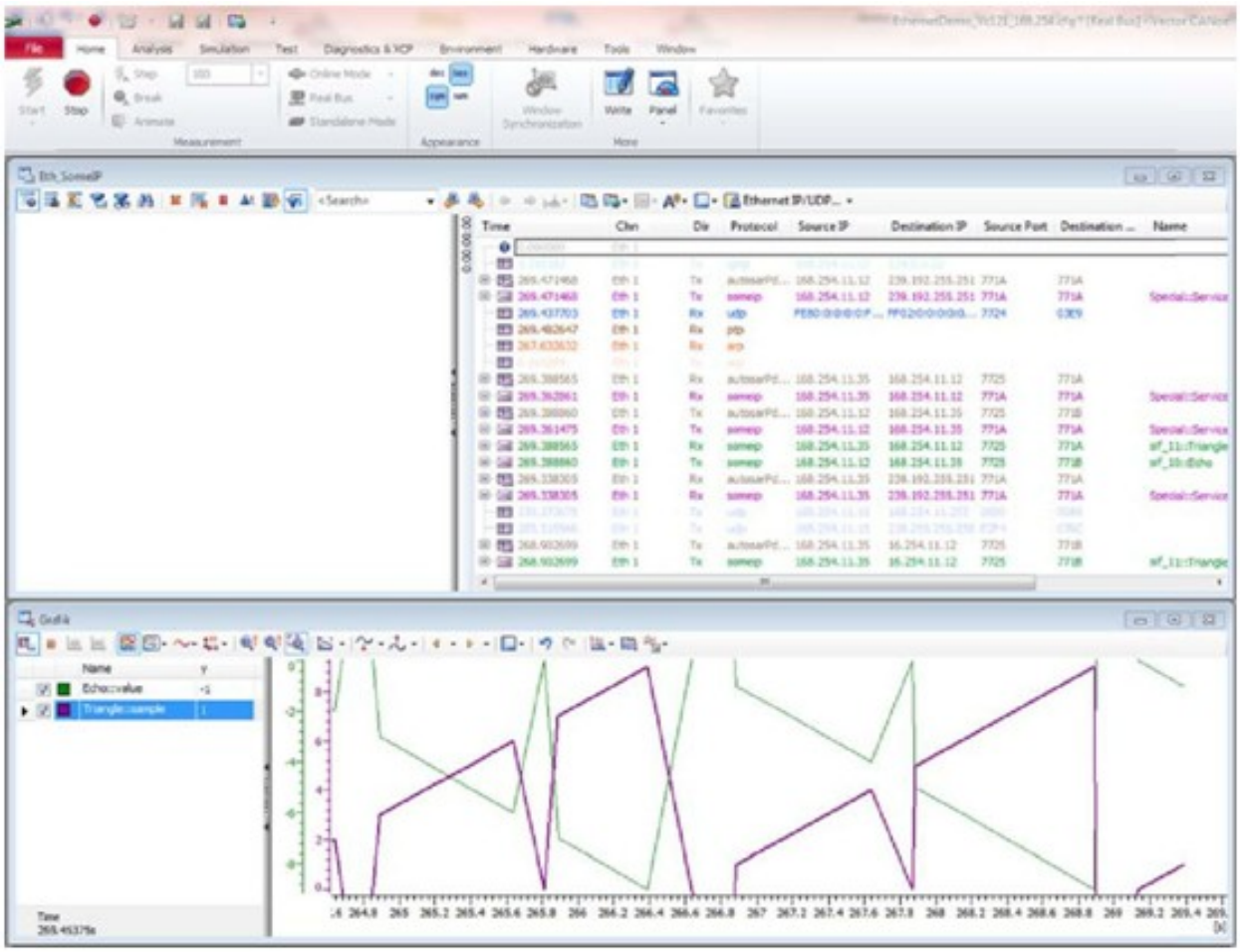
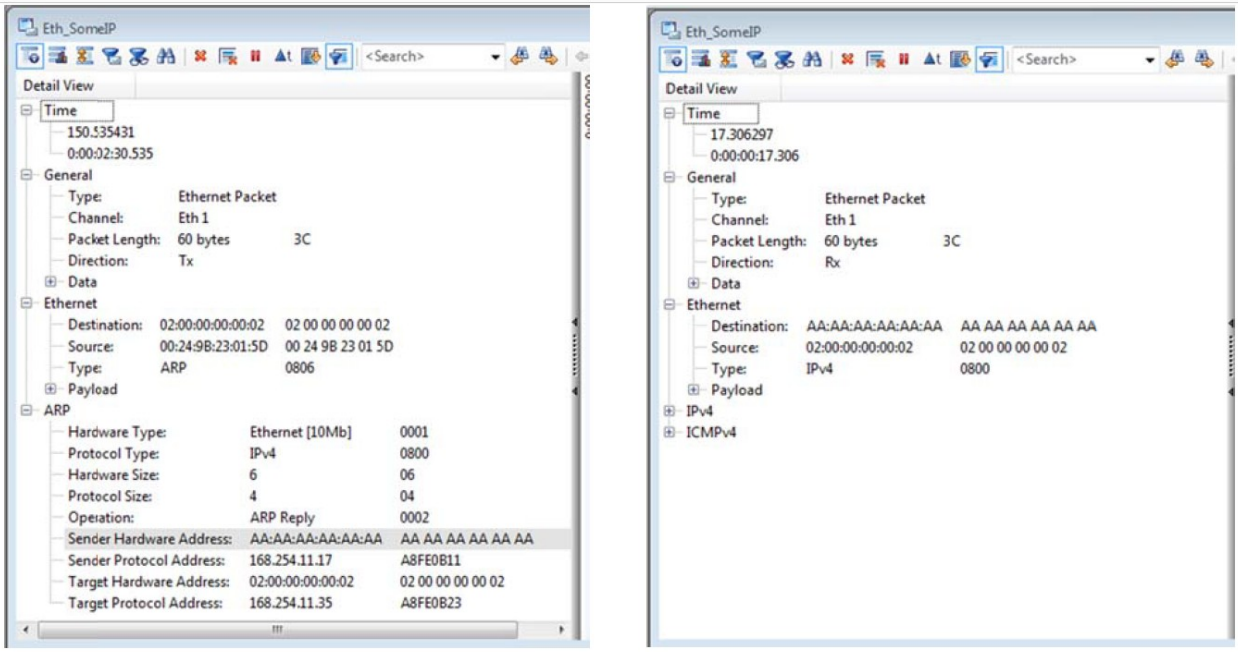


Рисунок 18 - Графические пакеты SO ME / IP, представленные графически

Цель теста: продемонстрировать отравление кэша ARP и доказать, что это возможно сделать с нестатическими таблицами ARP.
Область применения: испытательный стенд, как показано на рисунке 12. Пример прикладного программного обеспечения работает на ЭБУ. Построитель пакетов Ethernet был добавлен в настройку для генерации и отправки поддельных пакетов.
Процесс: сформирован пакет запроса ECHO и два пакета запроса / ответа ARP с соответствующими MAC-адресами AA: AA: AA: AA: AA: AA и CC: CC: CC: CC: CC: CC. Обмен пакетами происходил следующим образом:
1. Пакет запроса ECHO с 168.254.11.17 (случайный IP-адрес) был отправлен на 168.254.11.35 (ECU)
2. За пакетом запроса ECHO непосредственно следует ответ ARP с созданным MAC-адресом AA: AA: AA: AA: AA: AA (показано на рисунке 19 а).
3. После того, как ответ ARP получен от ECU и его кэш обновлен, ответ ECHO выходит, как ожидается, AA: AA: AA: AA: AA: AA: (показано на рисунке 19 б)
4. Еще один ответ ARP отправляется, только на этот раз, когда CC: CC: CC: CC: CC: CC является MAC-адресом (показано на рисунке 20 а).

5. Снова следует запрос ECHO
6. На этот раз ECU отправляет ответ ECHO в CC: CC: CC: CC: CC: CC (показано на рисунке 20 б).

Результат: тот факт, что ECU ответил на один и тот же запрос ECHO на два разных MAC-адреса после получения соответствующих ответов ARP, показывает, что возможно отравление кэша ARP. Это можно легко предотвратить, включив опцию «Статические таблицы ARP» в DaVinci Configurator, но тогда все устройства в сети необходимо будет ввести в таблицу ARP, и будет невозможно добавить устройства на лету, пока система работает. эксплуатации. Каждое добавление устройства потребовало бы перепрограммирования прошивки ЭБУ. Тем не менее, в статичной среде, как автомобиль, это не такой уж плохой вариант, учитывая все преимущества, которые он несет с собой. Многим людям, находящимся в середине атаки, было бы труднее или даже невозможно сделать, если кэш ARP не может быть отравлен.



а б

а) APR ответ с шага 2; б) ECHO ответ с шага 3

Рисунок 19 - APR и ECHO ответы с шагов 2 и 3 соответственно

3.6 TCP угон

Перехват TCP основан на том факте, что TCP является протоколом, ориентированным на соединение. Соединение основано на порядковых номерах, которые определяются случайным образом). Они увеличиваются на длину каждого нового отправляемого пакета. Пакеты с неправильными порядковыми номерами отбрасываются.

Во время процесса угона злоумышленник отслеживает текущий сеанс связи и узнает порядковые номера. Затем он вставляет тщательно созданный пакет (с подделанной информацией) в сеанс связи и, таким образом,

десинхронизирует текущую связь, выбивает один законный хост и продолжает устанавливать связь на своем месте. С этого момента пакеты, поступающие с законного хоста, будут отброшены как повторные передачи TCP из-за устаревших порядковых номеров.

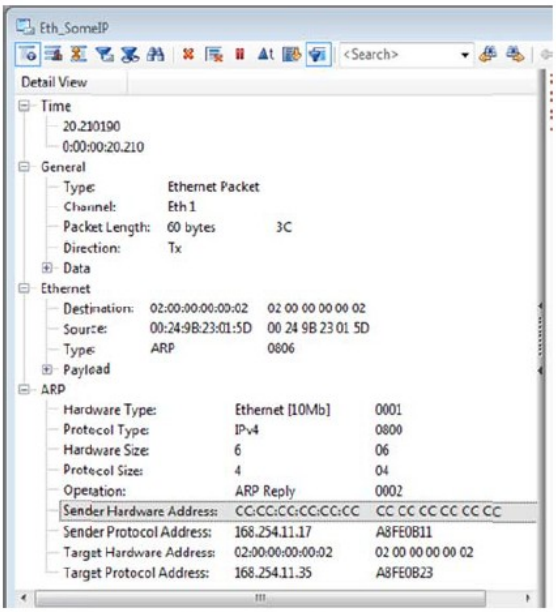


Figure 5-8: ARP Reply from Step 4.

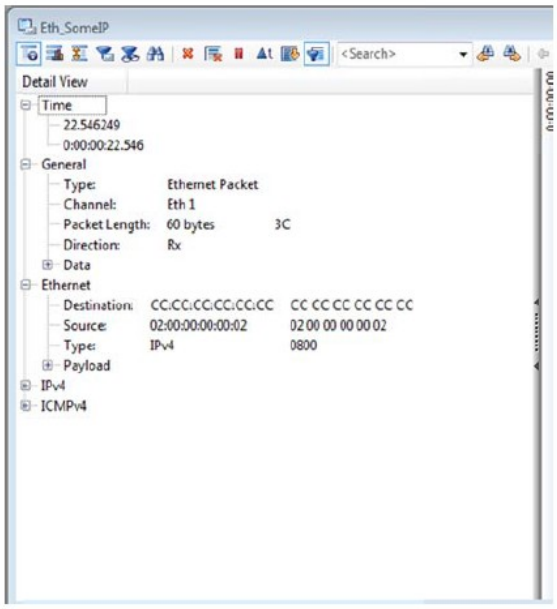


Figure 5-9: ECHO Response from Step 6.

а б

а) APR ответ с шага 4; б) ECHO ответ с шага 6

Рисунок 20 - APR и ECHO ответы с шагов 4 и 6 соответственно

Цель теста: перехватить соединение прошивки DoIP-прошивки

Область применения: испытательный стенд, как показано на рисунке 12. ПК выполняет vFlash для процесса перепрошивки, а виртуальная машина Kali запускает скрипт Python, который анализирует пакеты и десинхронизирует соединение при необходимости.

Процесс: ECU подключен к ПК. Сценарий угона запускается на виртуальной машине Kali. vFlash запускается, и начинается сеанс перепрошивки. Скрипт анализирует связь между vFlash и ECU. Как только начальный обмен ключами произошел, скрипт подключается и отправляет свой собственный пакет для десинхронизации текущего соединения из vFlash и может вместо этого отправить свою собственную полезную нагрузку.

На рисунке 21 показано сообщение об ошибке «Ошибка доступа к безопасности ...», которое генерирует vFlash после десинхронизации сеанса.

Важные пакеты помечаются следующим образом:

1. Внедренный TCP-пакет с поддельным порядковым номером для угона
2. Попытка vFlash отправить законный пакет, который распознается как повторная передача TCP из-за повторяющегося порядкового номера

3. Содержимое созданного пакета с полезной нагрузкой с надписью «Hijacked»

Результат: процесс угона был успешным. Обычные инструменты угона не могут быть использованы из-за того, что они требуют определения портов источника и назначения. vFlash, в соответствии с ISO13400, не запускает каждый сеанс на одном и том же порте источника. В связи с этим был написан скрипт на python с использованием scapy для прослушивания всех пакетов и определения пакета, который успешно прошел аутентификацию после обмена начальным ключом. Сессия была десинхронизирована. vFlash немедленно сообщает об ошибке и отправляет пакет для закрытия соединения. Это можно предотвратить несколькими способами. Кэш ARP может быть отравлен, и если человек находится в середине атаки, эти пакеты могут быть отфильтрованы. Другой вариант будет подделывать пакеты для vFlash, чтобы он не замечал что связь была ансинхронизирована. В качестве альтернативы, его можно просто отключить, но это потребует точного времени.

Эта атака возможна, если злоумышленник может обнаружить незашифрованную связь. В случае этого испытательного стенда главным фактором было то, что практически вся связь видна любому. Если бы это было не так, было бы намного сложнее угадать числа последовательностей. Сначала реализуем TCP-протокол, используемый для увеличения начальных порядковых номеров после определенного периода времени. Конечно, он был очень слабым, так как можно было легко установить соединение с хозяином, посмотреть, какую последовательность он получит, и, попробовав число вокруг него, он получит высокую вероятность угона другого. текущая сессия. Это не тот случай, в настоящее время и в этой реализации, где числа кажутся очень случайными.

Если бы связь была зашифрована, то было бы намного сложнее, если не невозможно, получить последовательность и выполнить запрос.

Следует отметить, что в случае, если микропрограмма имеет криптографическую подпись, по-прежнему невозможно установить обычную микропрограмму. С помощью подписи и открытого ключа ЭБУ может проверить достоверность данных и их достоверность.

Таким образом, определить, насколько безопасна система, можно оценить, рассчитав баллы RAV для каждой системы. Кроме того, можно рассчитать, как различные варианты и дополнения повлияют на этот показатель RAV.

После того, как баллы RAV рассчитаны и предложены контрмеры для ограничений и пористостей, эти результаты будут обсуждаться.

Благодаря тому, что RAV является скалярной метрикой, можно легко сравнивать различные системы и конфигурации. В Таблице 1 описаны различные системы. Таблица 2 показывает влияние отдельных изменений конфигурации существующего стека Vector. Он хранится отдельно из-за простоты просмотра и сравнения эффектов конфигурации. Коды,

используемые для представления операций, элементов управления и ограничений в этих таблицах, можно найти в таблицах 3, 4 и 5 соответственно.

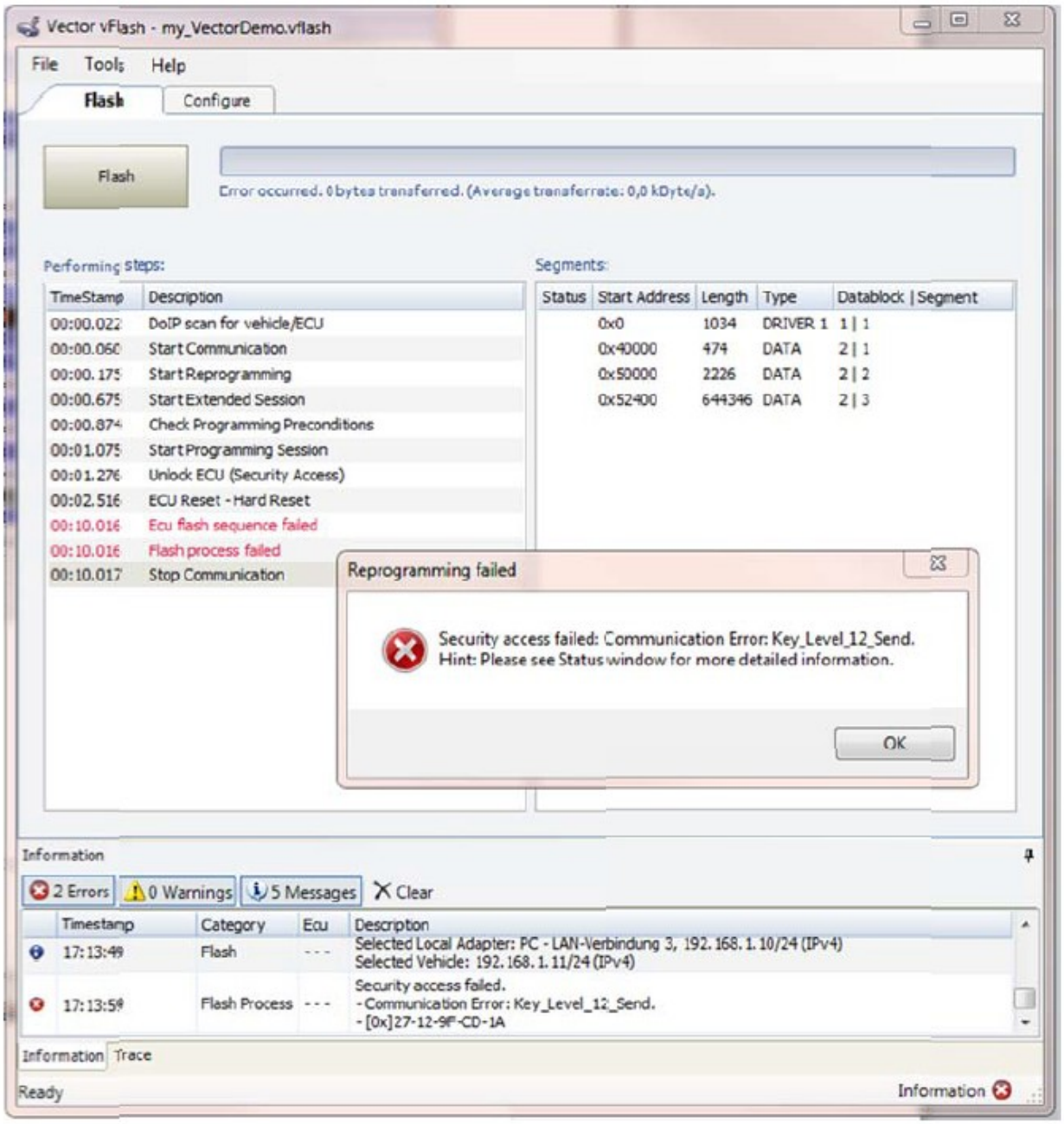


Рисунок 21 - Сбой доступа к Flash-безопасности

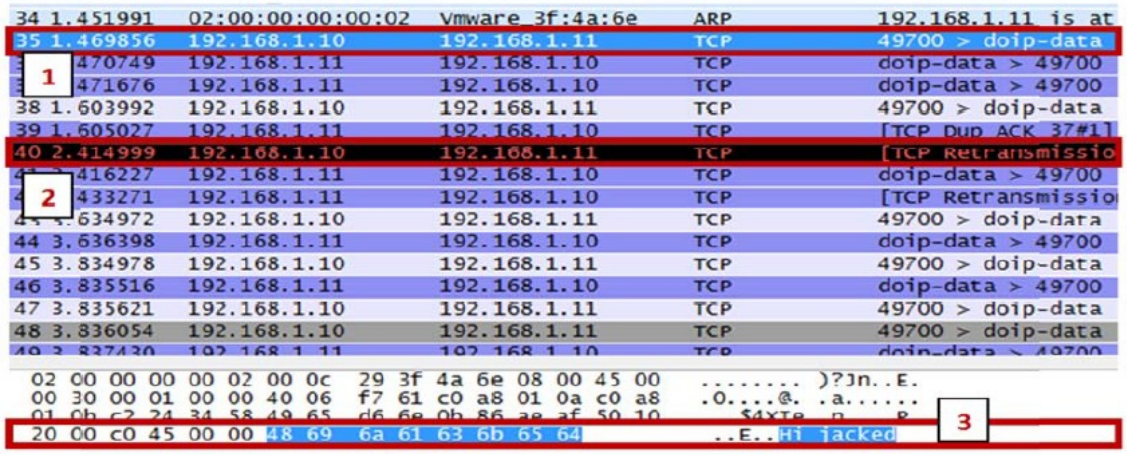


Рисунок 22 - это скриншот сообщения, снятого Wireshark.

Таблица 1 – Сравнение уровней безопасности различных стеков и конфигураций

	Протоколы определений	Векторный Стек База конфигураций	Улучшения комбинированного векторного стека	Предложения/ дополнения к векторному стеку
Visibility	V	V	V	0
Access	AC1, AC2,AC3,AC4	AC1,AC3,AC4	AC3,AC4	AC4
Trust	T1,T2	T1,T2	T1	0
Authentication	A1	A1	A1	A1
Indemnification	0	0	0	0
Resilience	R1	R1	R1	R1
Subjugation	0	0	0	0
Continuity	0	0	0	0
Non-Repudiation	0	0	NR1	NR1
Confidentiality	0	0	0	CF1
Privacy	0	0	0	0
Integrity	0	0	I1	I1
Alarm	A1,A2	A1,A2	A1,A2	A1,A2
Vulnerabilities	VW1	VW1	VW1	0
Weaknesses	W1, VW1	W1, VW1	W1, VW1	W1

				продолжение Таблицы 1
Concerns	0	0	0	0
Exposures	E1;E2;E3;E4;E5	E1;E2;E3	E2;E3	E3
Anomalies	0	0	0	0
Actual Security	82,4038 RAVs	83,7185 RAVs	85,2647 RAVs	91,8459 RAVs

Таблица 2 – Сравнение уровней безопасности различных стеков и конфигураций

	Векторный стек База конфигураций	отключение ICMP в векторном стеке	Статическое ARP Кэш включение в векторном стеке	Прошивка
Visibility	V	V	V	V
Access	AC1,AC3,AC4	AC3,AC4	AC1,AC3,AC4	AC1,AC3,AC4
Trust	T1,T2	T1,T2	T1	T1,T2
Authentication	A1	A1	A1	A1
Indemnification	0	0	0	0
Resilience	R1	R1	R1	R1
Subjugation	0	0	0	0
Continuity	0	0	0	0
Non-Repudiation	0	0	0	NR1
Confidentiality	0	0	0	0
Privacy	0	0	0	0
Integrity	0	0	0	I1
Alarm	A1,A2	A1,A2	A1,A2	A1,A2
Vulnerabilities	VW1	VW1	VW1	VW1
Weaknesses	W1, VW1	W1, VW1	W1, VW1	W1, VW1
Concerns	0	0	0	0
Exposures	E1;E2;E3	E2;E3	E1;E2;E3	E1;E2;E3
				продолжение таблицы 2

Anomalies	0	0	0	0
Actual Security	83,7185 RAVs	84,2657 RAVs	84,0709 RAVs	84,2372 RAVs

Таблица 3 – Отображение операций на коды

Тип операции	Код	Описание
Visibility	V	Имеется только один хост, который либо виден, либо нет
Access	AC1	ICMP тестовый ответ
Access	AC2	UDP тестовый ответ
Access	AC3	TCP тестовый ответ
Access	AC4	DoIP тестовый ответ
Trust	T1	Возможность замены
Trust	T2	ARP возможность отправления

Таблица 4 – Карта управления кодами

Тип операции	Код	Описание
Authentication	A1	Аунтификация ключа
Resilience	R1	Отказ соединения после двух сброшенных
Non-Repudiation	NR1	Подпись
Confidentiality, Integrity	CF1	Шифрование
Integrity	I1	Хэш
Alarm	A!1	Уведомление из vFlash
Alarm	A!2	Лог в vFlash

Таблица 5 – Отображение ограничений на коды

Тип операции	Код	Описание
Exposure	E1	Ответы на запросы ICMP Echo
	E2	Ответы на запросы TCP SYN
	E3	Ответы на запросы DoIP с любого порта IP
	E4	Ответы на запросы на закрытых портах UDP
	E5	Скачек с двойной маркировкой VLAN
Vulnerability, Weakness	VW1	TCP угон
Weakness	W1	DoS атака

Контрмеры пористости и ограничения перечислены в Таблице 6. Некоторые из них более подробно обсуждаются в главе 3. Все контрмеры можно сгруппировать по следующим трем категориям:

1. Использование существующих параметров конфигурации (например, статических таблиц ARP и отключенных эхо-ответов ICMP)
2. Дальнейшее развитие реализации стека и добавление функций, таких как шифрование и подписи с кэшами, для всех коммуникаций.
3. Изменение существующей реализации стека, чтобы она не соответствовала спецификациям протокола для большей пользы. Примером здесь является отправка помеченных RST TCP-пакетов, когда помеченные SYN-пакеты принимаются на закрытых TCP-портах. Это не будет иметь больших последствий для функциональности системы, но устранит одно воздействие.

Таблица 6 – Контрмеры

Код	Контрмеры
E1	Отключить ICMP в конфигурации
E2	Измените реализацию так, чтобы пакеты, помеченные RST, не отправлялись, когда зондирование закрытых портов TCP
E3	Измените реализацию так, чтобы она не отвечала ни на один IP-адрес, который отправляет команды DoIP
VW1	Реализуйте шифрование, чтобы порядковые номера не могли быть прослушаны
W1	Добавьте фильтры и брандмауэры для защиты от DoS-атак.
T1	MIKEY and SRTP
T2	Включение статического ARP кода

Обобщая вышесказанное можно сделать вывод, что фактическая безопасность может быть увеличена на 1,5 RAV, просто изменив конфигурации существующей реализации стека без дальнейшей разработки. При дальнейшем развитии возможно увеличение на 8 RAV. Есть две вещи, которые нужно иметь в виду:
Во-первых, оценки RAV кажутся низкими из-за того факта, что некоторые контроли вообще не исследовались, поскольку они не имеют отношения к данному исследованию.
Во-вторых, некоторые меры безопасности, такие как шифрование, потребуют дополнительных ресурсов и могут снизить производительность системы. Следовательно, существует компромисс между безопасностью и производительностью, который должен оцениваться в каждом конкретном случае в данном сценарии.

4 ЭКОНОМИЧЕСКОЕ И ЭКОЛОГИЧЕСКОЕ ОБОСНОВАНИЕ ПРОЕКТА

4.1 Экономическое обоснование проекта

В данной выпускной работе рассчитана стоимость исследования лабораторного комплекта.

Стоимость продукции включает следующие компоненты:

- стоимость приобретаемой продукции;
- затраты на содержание и эксплуатацию оборудования;
- расчетные затраты;

Цена продукции определяется по формуле:

$$Z = (C + P_{ПЕР}) * K \quad (3),$$

где С - стоимость товара;

$P_{ПЕР}$ – расходы периода;

K – коэффициент с учетом вычетов по налогу на добавленную стоимость (12%)

Стоимость затрат определяется по формуле:

$$C = S_{ПИ} + S_{НР} + S_{Р} + З_{СН} \quad (4)$$

$S_{ПИ}$ – стоимость приобретаемой продукции

$S_{НР}$ – расчетные затраты;

$S_{Р}$ – затраты на содержание и эксплуатацию оборудования;

$З_{СН}$ – расходы по социальному налогу.

Стоимость основных материалов (в случае проведения исследования в предприятии) в общей форме рассчитывается по формуле:

$$S_{ОМ} = \sum_{1}^{n} (m_i * Ц_i * k_{ТЗi}) \quad (5)$$

где m_i – скорость потребления i-го материала продукта, кг / шт.;

$Ц_i$ – средняя цена за одно устройство, тг

$k_{ТЗi}$ – коэффициент с учетом транспортных и затрат на приобретение

n - количество материалов, используемых в производстве продукции

Так как наши опыты были проведены вне специального предприятия, а домашних условиях и в любительской мастерской было решено, что рассчитывать стоимость основных материалов нет необходимости.[23]

Стоимость приобретаемой продукции рассчитывается по следующей формуле

$$S_{ПИ} = \sum_{1}^{k} (N_i * Ц_{ПИi} * k_{ТЗi}) \quad (6)$$

где $k-$ виды покупной продукции, используемой в производстве продукции;

N_i- количество элементов i-го типа

$k_{ТЗi}-$ коэффициент, учитывающий затраты на транспорт и приобретение. Всего приобретаемой продукции 5%.

$Ц_{ПИ}$ - средняя цена за одно устройство

Сведения о себестоимости приобретаемой продукции приведены в таблице 4.1 (рыночные цены на 10 марта 2019 года).

Таблица 4.1-наименование и стоимость приобретаемой продукции

Наименование закупаемой продукции	Вид продукции	Количество в одном продукте, шт.	Цена за единицу, тг	Сумма одного продукта, тг
1	2	3	4	5
Шлюз – хаб Xiaomi Gateaway	Xiaomi Gateaway	1	6500	6500
Датчик влажности и температуры	Xiaomi Gateaway	1	3500	3500
Интеллектуальный (умный) удлинитель	Agara	1	1540	1540
Интеллектуальная (умная розетка)	Xiaomi Gateaway	1	4328	4328
Многофункциональная кнопка	Xiaomi Gateaway	1	2458	2458
ИТОГО				18326

Стоимость приобретаемой продукции:

$S_{пи}$=18326 тг

С учетом затрат на транспортировку, стоимость приобретаемой продукции:

$S_{пи}$=18326*1,05=19242,3 тг

Таблица 3. Данные для расчета интенсивности труда в конструировании и размера заработной платы.

Наименование операции	График работы	Норма времени с/дет	Тарифная ставка	Заработная плата на продукцию, тг
1	2	3	4	5
Сборка	3	0,3	164,16	68,98
Тестирование	2	0,5	161,76	51,74
Настройка	4	0,4	178,4	71.36
ИТОГО				192,08

Размер основной заработной платы производственного персонала-это: S_o=192,08 *1,2=230,496 тг. Нужно уточнить, что данную работу будет делать инженер с окладом 90000 тенге и техник с окладом 60000тенге. Часовая тарифная ставка инженера составляет – 440 тенге, техника - 310 тенге

Дополнительная заработная плата принимается в размере 10% от основной заработной платы:

$S_{доп}$=230,496*0,1=23.04 тг

Фонд заработной платы для производственных работников

ФЗП =230,496 +23,04=253, 53тг

Расходы по уплате социального налога:

$$З_{сн}=(ФЗП-ФЗП*0,1)*0,11 \quad (7)$$

Мы получаем:

$З_{сн}$=(253, 53-253, 53*0,1)*0,11=25.098тг

Затраты на хранение и эксплуатацию оборудования обесценение оборудования, стоимость ремонта, мощность и т. д. б. включает. При определении общей стоимости продукции эти затраты могут включать заработную плату в соответствии с формулой:

$$S_p = ФЗП \cdot K_{об} \quad (8)$$

где $K_{об}-$ коэффициент, учитывающий отношение затрат на содержание и эксплуатацию оборудования $(K_{об}=1,5)$

$S_р$=253,53*1,5 =380,295тг

К операционным расходам относятся наем ИТК, бухгалтер и контролерский персонал, подсобные рабочие, если они не назначены на

рабочие места. Эти затраты можно рассчитать из формулы себестоимости предполагаемой продукции

$$S_{НР} = ФЗП \cdot K_y \quad (9)$$

где K_y – коэффициент, учитывающий отношение расходов магазина к заработной плате (150 – 400%).

$S_{НР}$=253,53*2=507, 06 тг

Себестоимость продукции определяется по формуле (3.2)

С=18326 +507, 06 +380,295+25,098 = 19238, 453

Период расходов определяется выражением:

$$P_П = P_{ОА} + P_{РЕЛ} \quad (10)$$

где $P_{ОА}$ - общие административные расходы (от 100-250% до SO);

$P_{РЕЛ}$ – расходы, связанные с продажей (3-5%).

Общие административные расходы:

$Р_{ОА}$=230,496 *1,5=345, 744 тг

Расходы, связанные с продажей:

$Р_{РЕЛ}$=.19,238, 453*0,03=577,153

Рассчитываются расходы периода:

$Р_{П}$=345, 744+577,153 =922,897

Доход составляет и рассчитывается 15-30% от себестоимости:

П=19 238, 453*0,2= 3847,6906 тг

Мы рассчитываем цену устройства, включая НДС (12%):

=(19 238, 453+679,897+3847,6906)*1,12=23,766,0406тг

Результаты расчетов приведены в таблице 3.3

Таблица 4-Стоимость

№	Стоимость статей	Сумма, тенге
1	2	3
1.	Материалы приобретенные	18326
2.	Фонд заработной платы для производственных работников	2535,3
3.	Социальный налог	25, 098
4.	Затраты на содержание и эксплуатацию оборудования	380,295
5.	Расчетные затраты	507, 06

Продолжение таблицы 4.

№	2	3
6.	Стоимость продукции	19 238, 453
7.	Расходы периода	922,897
8.	Прибыль	3847,6
9	Цена продукции с учетом НДС	23 766,04

Из экономического расчета следует вывод, что используемый нами лабораторный комплект полностью оправдал свои надежды. За месяц предварительной работы не наблюдалось случая, где работа устройств не осуществилась бы. Гарантией работы данных устройств является высокомощные батареи. В среднем потраченная сумма приобретенных изделий стоила того, чтобы приобрести и протестировать данный набор. В дальнейшем, если заниматься производством таких устройств или выпускать такие устройства на предприятии, я считаю, что окупаемость и прибыль предприятия будут расти, так как сейчас 21 век – это мир технологий, в котором все постепенно переходит на цифровизацию. Соответственно, можно заметить, что уже сейчас половина нашей повседневной жизни состоит из оцифрованных устройств.

4.2 Экология и безопасность проекта

Организация и улучшение условий труда на рабочем месте – является одним из важнейших резервов производительности труда и экономической эффективности производства, а так же дальнейшего развития самого работающего человека. Одной из обязанностей руководителей и инженерно-технических работников является создание на предприятии безопасных условий труда согласно правилам техники безопасности и производственной санитарии. Разработка и производство электронных устройств должно происходить в условиях минимальной вероятности заболевания или поражения работающих. Улучшение условий труда и его безопасности, правильная организация рабочего места на производстве влияют на производительность труда, на качество и себестоимость выпускаемой продукции. Нормальная и безопасная работа монтажников и настройщиков электронной аппаратуры во многом зависит от того, в какой степени условия работы соответствуют оптимальным.[24] Под условиями труда здесь

подразумевают комплекс физических, химических, биологических и других факторов, установленных стандартами по безопасности труда. На участке сборки следует поддерживать определенную температуру, влажность, чистоту, ионный состав и скорость движения воздуха, наиболее благоприятные для работающих.

4.2.1 Микроклиматические условия помещения

Рассмотрим некоторые виды неблагоприятных воздействий, характерных для участка сборки радиоэлектронной аппаратуры. Параметры микроклимата. В процессе взаимодействия с окружающей средой, человек приобрел способность регулировать свой теплообмен и сохранять температуру своего тела постоянной (~36,6 °С) вне зависимости от окружающей среды и тяжести выполняемой работы. Такая способность называется терморегуляцией. Однако при сильных отклонениях параметров микроклимата, терморегуляция нарушается, и это приводит к нарушению функционирования физиологических систем.

Оптимальные и допустимые параметры микроклимата на производстве регламентирует ГОСТ 12.1.005-76 «Воздух рабочей зоны». Согласно отраслевому стандарту ОСТ.118.ВО.005.002 помещения делят на 3 категории:

I. Помещения, предназначенные для выполнения технологических и сборочных операций.

II. Помещения, предназначенные для подготовки частей и деталей.

III. Помещения для различных вспомогательных операций.

Таблица 4.4 – Деление на категории по параметрам микроклимата

Категория по микроклимату	Температура, С		Относительная влажность, %
	Зимой	Летом	
1	2	3	4
I	21 1	23 1	45 5
II	20 2	23 2	45 5
III	По санитарным нормам СН245-71		

Исходя из требований специальной технологии по отраслевым нормам отопление помещений должно быть воздушным или совмещенным с приточкой вентиляции и кондиционированием воздуха, или водяным с нагревательными трубами (открытые нагревательные приборы и трубопроводы к ним применять нельзя). Приточные вентиляционные системы должны быть оборудованы увлажнительными установками.

Производственные излучения (шум, вибрации, ультра- и инфразвуки). Источником производственного шума и вибрации может быть работающее оборудование (насосы, компрессоры, вентиляционные установки и т.п.). Как шум, так и вибрация неблагоприятно действуют на человека, снижая работоспособность и вызывая различные физиологические отклонения в организме. В рабочей зоне производственного помещения, согласно ГОСТ 12.1.003-83 и «Гигиеническим рекомендациям по установлению уровней шума на рабочих местах с учетом напряженности и тяжести труда» для категории напряженности II уровень звука не должен превышать 70 дБ. Если по какой либо причине фактически измеренный уровень шума на участке сборки и регулировки РЭА окажется выше нормы, то следует предпринять меры по снижению шумов или обеспечить сотрудников средствами защиты.

Нерациональное освещение. Рациональное техническое освещение предупреждает развитие зрительного и общего утомления, позволяет сохранять работоспособность и улучшать качество выпускаемой продукции. Рациональной можно считать экономичную систему освещения, учитывающую свойства человеческого глаза и соответствующую СНиП П-4-79. «Нормы проектирования и искусственного освещения».При нерациональном освещении могут появиться заболевания органов зрения человека. Рекомендуемые меры по обеспечению рационального освещения.В качестве рекомендации можно предложить установить на участке сборки и монтажа радиоустройств комбинированную систему освещения (естественное и искусственное освещение) соответствующую СНиП П-4-79. В соответствии с разрядом III работы по точности и подразрядом работы «б» или «в» (печатные платы с маской - фон средний; контраст объекта с фоном малый и средний) следует использовать комбинированное освещение при газоразрядных лампах и наименьшей освещенностью на рабочем месте 1000 лк. Система освещения должна быть надежной, безопасной и подвергаться периодическому осмотру с целью замены неисправного оборудования. Следует предусмотреть аварийное и эвакуационное освещение.[25]

4.2.2 Требования по безопасности

Электробезопасность.

Электрический ток обладает комплексным поражающим действием на ткани и органы человека. Влияющими факторами являются: сила тока, его частота, продолжительность действия на организм, условия окружающей среды, возраст и эмоциональное состояние человека, состав его кожного покрова, площадь контакта с источником тока, условие подключения тела человека в электрическую цепь. При электропоражениях решающую роль играет сила тока. 2Границей опасности силы тока принято считать предел

0,06-0,1 А, Что касается напряжения, то безопасным следует считать напряжение до 36 В. Напряжение свыше 100 В считается, безусловно, опасным для жизни человека. Анализ несчастных случаев от электро травматизма на производстве показывает, что основными причинами этого является:

- монтаж и ремонт оборудования при не отключенном (оборудовании) напряжении;
- поврежденность изоляции;
- допустимость открытых токоведущих частей;
- случайные прикосновения к оборванным концам и оголенным проводам, находящимся под напряжением;
- неисправность средств защиты;
- отказ от индивидуальных средств защиты или пренебрежение ими при работе на электроизмерительных приборах;
- слабые знания правил техники безопасности

Основными задачами при организации безопасных условий труда являются:

- проведение инструктажа работающих об опасности электрического тока и мерах предупреждения ее;
- применение пониженного безопасного напряжения (36 В для помещений с повышенной опасностью);
- применение защитного заземления и/или зануления;
- правильная эксплуатация электрооборудования и измерительных приборов;
- выполнение действующих правил, норм и инструкций по технике безопасности.

Пожароопасность.

Наличие на участке производства электронагревательных приборов и легковоспламеняющихся жидкостей (флюса, бензина и т.д.) требует обратить особое внимание на опасность возникновения пожара. [26]Следует полностью исключить возможность курения на рабочем месте, не допускать загромождения проходов и аварийных выходов. Первым и обязательным правилом должно быть неукоснительное соблюдение правил, норм и инструкций по пожарной безопасности. Контроль за соблюдением должен быть возложен на специально выделенных лиц.[26]

Вредные вещества.

Технологический цикл производства радиоаппаратуры включает в себя участки монтажа и настройки, на которых используется припой ПОС-61 (61% олово, 38% свинца и 1% висмута). В процессе разработки образуются высокотоксичные соединения свинца. Для свинца и его соединений предельно допустимая концентрация (ПДК) - 0,01 мг/м3. Пары этих соединений, проникая в органы человека через дыхательные пути, могут вызвать отравление. Так как свинец относится к веществам первого класса опасности то следует обеспечить удаление паров этих соединений из

рабочего помещения, чтобы их концентрация не превышала предельно допустимую. Профессиональные заболевания могут быть вызваны и другими вредными веществами - флюсом ФКСп40 (этиловый спирт, сосновая канифоль), а также спиртом, бензином и ацетоном, которые используются на участке отмывки. По степени воздействия вредные вещества подразделяются на 4 класса опасности:

1) чрезвычайно опасные;
2) высокоопасные;
3) умеренно опасные;
4) малоопасные.

Таблица 4.5 – Классификация вредных веществ по степени воздействия

Показатель мг/м^3	Норма для класса опасности			
	1-го	2-го	3-го	4-го
1	2	3	4	5
ПДК в воздухе рабочей зоны	Менее 0,1	0,1-1,0	1,1-10,0	Более 10,0
Средняя смертельная концентрация в воздухе	Менее 500	500-5000	5001-0000	Более 50000

При лакокрасочных работах вредными факторами являются пары растворителей и лаков, которые вызывают тяжелые отравления организма. В санитарных нормах оговаривается предельно допустимая концентрация паров растворителей.Несоблюдение каких-либо из перечисленных факторов приводит к частичной потери работоспособности и профессиональным заболеваниям. Кроме этого многие из перечисленных факторов влияют на утомляемость и, как результат, на качество продукции. Для того чтобы ни один из вышеперечисленных факторов не оказывал воздействий на организм человека следует придерживаться следующих требований:

- Эксплуатация участков сборки или разборки, необорудованных вентиляцией недопустима.
- Паяльные и другие работы должны выполняться рабочими в предусмотренной для этой цели спецодежде.
- Прием пищи, питьевой воды, а также курение в помещениях, где проводится пайка, запрещается.
- После окончания работы показано принятие теплого душа.
- Сухие способы уборки участка не разрешаются. Обязательно мытье полов после каждой рабочей смены. Рабочий стол протирается 3% раствором уксуса.
- Не допускается использовать на работах связанных с пайкой, сборкой или разработкой лиц, не достигших 18 лет. Рабочие должны подвергаться

периодическим медицинским осмотрам в соответствующие указанные сроки (1 раз в 2 года).

- Все поступившие на работу должны инструктироваться о мерах предосторожности.

Монотонность работы. Работа монтажника радиоаппаратуры характеризуется своей монотонностью. Это приводит к тому, что по прошествии определенного времени у человека рассеивается внимание, повышается утомляемость. Тем самым снижается эффективность работы, создаются предпосылки для возникновения несчастных случаев. Исходя из этого, необходимо организовывать регулярные перерывы в работе, проводить производственную гимнастику.

4.2.3 Расчет общеобменной вентиляции на участке сборки

Общеобменная вентиляция производится для разбавления выделяющихся вредных веществ чистым воздухом до предельно допустимых норм и температур и осуществляется во всем объеме помещения.[27] Санитарно-гигиеническое назначение вентиляции состоит в поддержании параметров воздушной среды в соответствии с требованиями ГОСТ 12.1.005-76 «Воздух рабочей зоны. Общие санитарно-гигиенические требования». Проведем расчет необходимого количества воздуха на участке монтажа и настройки РЭА по 2 факторам: по поступлению в воздух рабочей зоны вредных веществ и по теплоизбыткам. Минимальное количество воздуха, которое необходимо замещать в рабочем помещении общеобменной вентиляцией, определяется по формуле:

$$L_1 = \frac{10^6 \times G}{C_g - C_0}, \qquad (11)$$

где L1 - объем воздуха, удаляемого из помещения (м3/ч); G - количество вредных веществ, выделяющихся в рабочем помещении (кг/ч); Cg - ПДК (мг/м3); C0 - содержание вредных веществ в подаваемом воздухе. При

- G = 8 х 10-5 (кг/ч);
- Cg = 0,01 (мг/м3);
- C0 = 2 х 10-4 (мг/м3);
- L1 = 8163 (м3/ч)

Для ассимиляции теплоизбытков воздухообмен определяется по формуле

$$L_2 = \frac{\sum Q}{c(t_{л_ь} - t_.)\rho}, \qquad (12.)$$

где $\sum Q$ - явные теплоизбытки в помещении, $c = 1 \frac{кДж}{кг}$ - массовая теплоемкость воздуха, $t_п$ - температура удаляемого воздуха, $t_п$- температура приточного воздуха, ρ- плотность воздуха.

При расчетах будем учитывать два основных источника тепла:

- количество тепла, выделяемое людьми (зависит от тяжести выполняемой ими работы).

Работа по монтажу и настройки радиоаппаратуры квалифицируется как легкая и количество тепла, выделяемого одним человеком равно 600 кДж/ч. Общее количество тепла, выделяемое на участке сборки работниками, равно:

Q1=600*3=1800 (кДж/ч);

- количество тепла, выделяемое оборудованием.

Таблица 3.3 – Количество тепла, выделяемое используемым оборудованием

Тип прибора	К-во	Потребл. мощность, ВА	Общ. мощность, ВА
1	2	3	4
Шлюз - хаб	1	250	140
Датчик влажности	1	250	80
Умная розетка	1	16	120
Умный удлинитель	1	До 2500 Ватт, 10 А	300
Мобильное устройство	1	3000мА	36
Итого:	676		

При среднем КПД около 60 %, количество тепла, выделяемое оборудованием на участке сборки приблизительно равно Q2=406 (кДж/ч). Температура удаляемого из рабочей точки (зоны) воздуха вычисляется по формуле:

$$t_{л} = t_{рК} + \Delta t(H - Z), \quad (13)$$

где tpз - температура воздуха в рабочей зоне, t - температурный градиент по высоте, H - расстояние от пола до вытяжных проемов, Z - высота рабочей зоны.

Примем, что H = 3 м, Z = 1,5 м. Отсюда:

$$t_ц=22 + 2 x (3-1.5)=25 (°C) \quad (14)$$

Подставив рассчитанные величины в формулу (4.10), вычислим суммарный воздухообмен, необходимый для удаления теплоизбытков

$$L_2 = \frac{1800 + 406}{1*1*(25 - 22)} = 735 \quad (м3/ч)$$

Таким образом, величина необходимого теплообмена выбирается по максимальному из L1, и L2 и равна

L = L1 = 8163 (м3/ч)

4.2.4 Защита атмосферы и сточных вод от загрязнения

На участке сборки и монтажа радиоустройств в вентиляционных выбросах присутствуют пары соединений свинца и паяльного флюса, которые необходимо удалять. На участке промывки также образуются вещества, загрязняющие сточные воды. Для защиты атмосферы и сточных вод от загрязнения необходимо проводить комплексную очистку выбросов. Очистка газовых выбросов основана на применении некоторых физико-химических методов.[28]К ним относится адсорбция, абсорбция, хемосорбция, каталитическое дожигание и т.д.

Адсорбция. Метод основан на поглощении из загрязненного газа одного или нескольких компонентов твердым поглотителем - адсорбентом - за счет притяжения молекул под действием сил Ван-дер-Ваальса.

Абсорбция. Метод основан на различной растворимости газов при поглощении одного или нескольких компонентов жидким поглотителем.

Хемосорбция состоит в промывке очищаемого воздуха растворами, вступающими в химические реакции с газообразными примесями такими, как двуокись серы, хлор, сероводород и т.п.

Каталитическое дожигание используется для превращения токсичных смесей газов в нетоксичные или малотоксичные.

Первичной стадией очистки стоков является механическая очистка, предназначенная для удаления взвесей и дисперсно-коллоидных частиц. Последующая очистка от химических веществ осуществляется различными методами - физико-химическими, химическими, электрохимическими, биологическими. Расчет допустимого состава сточных вод производится с учетом «Правил охраны поверхностных вод от загрязнения сточными водами». Наиболее перспективным направлением в сохранении экологического баланса является применение безотходных технологий. Так как наши опыты и исследования проводились

ОБСУЖДЕНИЕ И ВЫВОДЫ

В результате проделанной работы можно сделать следующие выводы. Связь на основе Ethernet прошла долгий путь от того времени, когда она была впервые разработана до сегодняшнего дня. В первые дни безопасность не была одним из ее главных приоритетов, но со временем было добавлено много мер безопасности, разработаны безопасные протоколы и устранены присущие им уязвимости.

В то время как в обычных компьютерных сетях основными источниками небезопасности являются незащищенные службы на открытых портах, у автомобиля не будет ни одного более открытого порта, чем необходимо, и даже тогда эти порты будут защищены. В большинстве случаев все сетевые устройства известны конечным точкам, поэтому они могут быть определены статически. Еще одна особенность, которая повышает безопасность системы, тем самым создает препятствия для злоумышленника, заключается в том, что в автомобиле не работает обычная ОС. Это означает, что все существующие эксплойты, которые атакуют известные уязвимые сервисы и повышают привилегии, неприменимы. Реализация сетевого стека в тестируемом устройстве очень надежна, и никаких ошибок реализации, которые могли бы быть использованы, выявлено не было.

Реализация стека TCP / IP была тщательно реализована. Например, протоколы (такие как ICMP), которые имеют много присущих им уязвимостей, не были полностью реализованы. Это отчасти потому, что они не нужны в автомобильной сфере. Кроме того, невыполнение этих функций позволило повысить уровень безопасности. Из всего протокола ICMP были реализованы только запросы и ответы ECHO, и даже они могут быть отключены в конфигурации.

Автомобильная среда полностью статична. Этот факт может быть использован как преимущество, поэтому это учитывалось при разработке сетевого стека. Например, ARP-кэш может быть настроен как статический. В этом случае отравление кэша ARP и многих атакующих людей невозможно. Совокупные эффекты всех этих пропущенных протоколов, статических конфигураций и даже предложений по добавлению в стек были продемонстрированы посредством вычисленных оценок RAV (для различных систем и конфигураций). Текущий стек в его базовой настройке оказался более безопасным, чем система со всеми протоколами, реализованными в соответствии с их спецификациями. Использование статических конфигураций означает, что реализации немного отличаются от спецификаций протокола. Несколько дополнений к стеку, таких как шифрование и подписи с хэшами, доказали повышение безопасности примерно на 10%. Однако, поскольку некоторые из этих дополнений требуют компромиссов между безопасностью и производительностью, их принятие должно приниматься в каждом конкретном случае.

Поставленная цель и задачи, были достигнуты. Когда дело доходит до вопроса о том, что сделал бы автор по-другому, если бы он снова сделал то же самое исследование, ответом было бы использование конкретной методологии с более раннего момента времени. OSSTMM оказался отличным ресурсом.

К сожалению, нет да / нет ответа на вопрос: «Является ли автомобильный Ethernet вместе с сопровождающими его протоколами безопасными и достаточно безопасными для автомобильной промышленности?» Можно сказать, что автомобильный Ethernet и сопровождающие его протоколы еще могут быть улучшены. Большинство протоколов все еще находятся в процессе стандартизации и разработки. Безопасность работает и учитывается. Недавние исследования показали производителям тесную связь между безопасностью и производительностью. Промышленность движется в правильном направлении. Однако следует иметь в виду одну важную вещь, связанную с безопасностью, и это тот факт, что цепочка настолько же сильна, насколько ее самое слабое звено.

.

СПИСОК ЛИТЕРАТУРЫ

1. Wolfhard Lawrenz, Ed., CAN System Engineering. London: Springer London, 2013, ISBN: 978-1-4471-5612-3 [Online]. DOI: 10.1007/978-1-4471-5613-0

2. U. Abelein, H. Lochner, D. Hahn, and S. Straube, ‘Complexity, quality and robustness - the challenges of tomorrow’s automotive electronics’, in 2012 Design, Automation Test in Europe Conference Exhibition (DATE), 2012, pp. 870–871. DOI: 10.1109/DATE.2012.6176573

3. S. M. Bellovin, ‘Security Problems in the TCP/IP Protocol Suite’, SIGCOMM Comput Commun Rev, vol. 19, no. 2, pp. 32–48, Apr. 1989. DOI: 10.1145/378444.378449

4. M. W. Eichin and J. A. Rochlis, ‘With microscope and tweezers: an analysis of the Internet virus of November 1988’, in Proceedings. 1989 IEEE Symposium on Security and Privacy, 1989, pp. 326–343. DOI: 10.1109/SECPRI.1989.36307

5. Free and Open Software Security Community, ‘OWASP Website’. [Online]. Available: https://www.owasp.org/index.php/Main_Page. [Accessed: 12-Sep- 2017]

6. Pete Herzog, ‘OSSTMM 3 - The Open Source Security Testing Methodology Manual: Contemporary Security Testing and Analysis’. ISECOM - Institute for Security and Open Methodologies, 2010 [Online]. Available: http://www.isecom.org/mirror/OSSTMM.3.pdf

7. J. Postel, ‘Internet Protocol’, Internet Request for Comments, vol. RFC 791 (INTERNET STANDARD), Sep. 1981 [Online]. Available: https://www.rfceditor.
org/rfc/rfc791.txt

8. S. Deering and R. Hinden, ‘Internet Protocol, Version 6 (IPv6) Specification’, Internet Request for Comments, vol. RFC 2460 (INTERNET STANDARD), Dec. 1998 [Online]. Available: https://www.rfc-editor.org/rfc/rfc2460.txt

9. William Stallings, ‘The Origins of OSI’, 1998. [Online]. Available: http://williamstallings.com/Extras/OSI.html. [Accessed: 30-Apr-2017]

10. Deon Reynders and Edwin Wright, Practical TCP/IP and ethernet networking for industry. Amsterdam; Heidelberg [u.a.: Newnes, 2003, ISBN: 978-0-7506-5806-5.

11. Andrew L. Russell, ‘OSI: The Internet That Wasn’t - IEEE Spectrum’. IEEE Spectrum, 30-Jul-2013 [Online]. Available: http://spectrum.ieee.org/computing/networks/osi-the-internet-that-wasnt

12. Google, ‘IPv6 – Google’, 2009-2017. [Online]. Available: https://www.google.com/intl/en/ipv6/statistics.html. [Accessed: 10-Sep- 2017]

13. Marc Heuse, ‘IPv6 Insecurity Revolutions’, Kuala Lumpur, 2012 [Online]. Available: https://www.yumpu.com/en/document/view/1924942/d1t2-marcheuse-ipv6-insecurity-revolutions/1. [Accessed: 06-May-2017]

14.J. Postel, ‘Transmission Control Protocol’, Internet Request for Comments, vol. RFC 793 (INTERNET STANDARD), Sep. 1981 [Online]. Available: https://www.rfc-editor.org/rfc/rfc793.txt

15. Margaret Rouse, ‘UDP (User Datagram Protocol)’, TechTarget, 2014. [Online]. Available:76 | References http://searchmicroservices.techtarget.com/definition/UDP-User-Datagram Protocol. [Accessed: 06-May-2017]

16. ‘Karl Benz’, Biography.com, Apr-2014. [Online]. Available: https://www.biography.com/people/karl-benz-9208256. [Accessed: 10-Sep- 2017]

17. ScienCentral Inc., ‘An Outline of the History of the Transistor’, PBS: Public Broadcast Service, 1999. [Online]. Available: http://www.pbs.org/transistor/album1/. [Accessed: 30-Apr-2017]

18.ScienCentral Inc., ‘Integrated Circuit’, PBS: Public Broadcast Service, 1999. [Online]. Available: http://www.pbs.org/transistor/background1/events/icinv.html. [Accessed: 30-Apr-2017]

19. Lisa Wade, ‘A Short History of the Airbag’, Consumer Affairs, 25-Sep-2006. [Online]. Available: https://www.consumeraffairs.com/news04/2006/airbags/airbags_invented. html. [Accessed: 10-Sep-2017]

20. W. Ziebart, ‘Car electronics-key factors of success for the ’90s’, in 1991 Eighth International Conference on Automotive Electronics, London, 1991, pp. 1–6 [Online]. Available: http://ieeexplore.ieee.org/document/152000/?arnumber=152000

21. Vector Informatik GmbH, ‘Introduction to CAN’, Vector E-Learning, 19-Oct- 2016. [Online]. Available: https://elearning.vector.com/vl_can_introduction_en.html. [Accessed: 15-Apr-2017]

22. Pat Richards, ‘AN228 - A CAN Physical Layer Discussion’. Microchip Technologies Inc., 2002 [Online]. Available: http://ww1.microchip.com/downloads/en/AppNotes/00228a.pdf. [Accessed:06-May-2017]

23.Steve Corrigan, ‘Controller Area Network Physical Layer Requirements’. Texas Instruments, 2008 [Online]. Available: http://www.ti.com/lit/an/slla270/slla270.pdf. [Accessed: 06-May-2017]

24.International Organization for Standardization, ISO 11898-1:2015 – Road vehicles -- Controller area network (CAN) -- Part 1: Data link layer and physical signalling. 2015, p. 65 [Online]. Available: https://www.iso.org/standard/63648.html. [Accessed: 02-Jul-2017]

25.Microcontroller Division Applications, ‘AN1278 - LIN (LOCAL INTERCONNECT NETWORK) SOLUTIONS’. STMicroelectronics, 2002 [Online]. Available: http://www.st.com/content/ccc/resource/technical/document/application_note/

10/30/18/b5/90/bc/4c/73/CD00004273.pdf/files/CD00004273.pdf/jcr:content/translations/en.CD00004273.pdf. [Accessed: 06-May-2017]