ПЕРЕДАЧА ДАННЫХ С ПРИМЕНЕНИЕМ АЛГОРИТМОВ ШИФРОВАНИЯ В МУЛЬТИПЛАТФОРМЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ УПРАВЛЕНИЯ КЛИМАТОМ ЗДАНИЙ.

Иняминов Юлдаш Арифханович

Джизакский политехнический институт.

кафедра Радиоэлектроники,

ассистент inyaminovyoldosh@gmail.com

Аюпов Дамир Шамилович
Студент.кафедра Радиоэлектроники

АННОТАЦИЯ: В данной публикации описываются технологии и разработки шифровальных и дешифровальных ключей, генерируемых с целью повышения их криптографической устойчивости, обеспечения защищенной передачи данных и ключей по открытому каналу связи для надежной передачи данных в многоплатформенной информационной системе климат-контроля зданий.

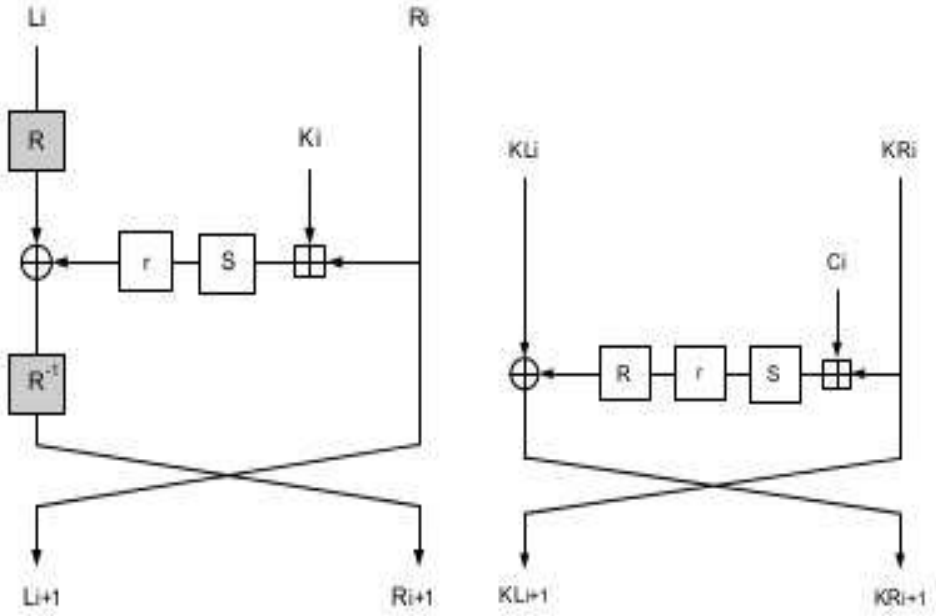
КЛЮЧЕВЫЕ СЛОВА: системы климат-контроля,шифровальных и дешифровальныхключей, декодированию, криптографической устойчивост, RAD Studio, декодированию.

В настоящее время в строительстве активно используются системы климат-контроля зданий, которые обязательно обмениваются данными с информационными системами интеллектуальных зданий и интеллектуальных домов, контролирующих не только отопление, вентиляцию и кондиционирование воздуха, но и освещение, мониторинг параметров энергопотребления, системы безопасности и др. работа таких систем, объединяющих программное и аппаратное обеспечение для управления деятельностью любого здания, сосредоточена на четырех основных функциях:
мониторинг: непрерывный мониторинг измерений датчиков;

- управление: алгоритмы управления строительными системами;
- оптимизация: повышение производительности системы;
- отчетность: документирование промежуточных и окончательных результатов.
- Поскольку информация в многоплатформенной информационной системе климат-контроля здания обычно передается по открытым каналам связи, необходимо обеспечить защиту передаваемых данных. Однако исследования в этой области только начинаются. Авторы провели исследования в этой области в смежных отраслях.
- В результате проведенного исследования было проведено оперативное моделирование устройства с гибридным принципом шифрования данных и с несколькими уровнями шифрования. Данное устройство может работать в любой системе мобильной связи.
- Используя эти и другие разработки, авторы провели дальнейшие исследования применительно к многоплатформенной информационной системе климат-контроля зданий.
- RAD Studio это самый быстрый способ для разработки кросс-платформенных приложений с использованием облачных сервисов и широкого подключения IoT. Она предоставляет мощные компоненты VCL для Windows 10 и обеспечивает

разработку на FMX для Windows, Mac и мобильных устройств. RAD Studio поддерживает Delphi или C++ с широким спектром услуг для корпоративно-ориентированного развития

- Принцип работы симметричного алгоритма шифрования (SEA) основан на применении информационной свертки – специальным образом организованной процедуры поглощения битов. Для ее демонстрации рассмотрим процедуру информационного свертывания на примере произвольной битовой строки. Свертка данных происходит следующим образом: берутся два смежных входных бита и на основе их значений устанавливается значение выходного бита. Далее процесс повторяется, т.е. рассматриваются следующие два смежных бита.



Разработки программы на языке программирования Delphi на компиляторе RAD Studio, по шифрованию и дешифрованию информации

В результате проведенных разработок была скомпилирована программа на языке программирования Delphi на компиляторе RAD Studio, по шифрованию и дешифрованию информации на основе работы алгоритма LEA-128 SEA и кодированию, декодированию ключей по алгоритму Base64, для повышения их криптостойкости при передаче по открытым каналам связи.

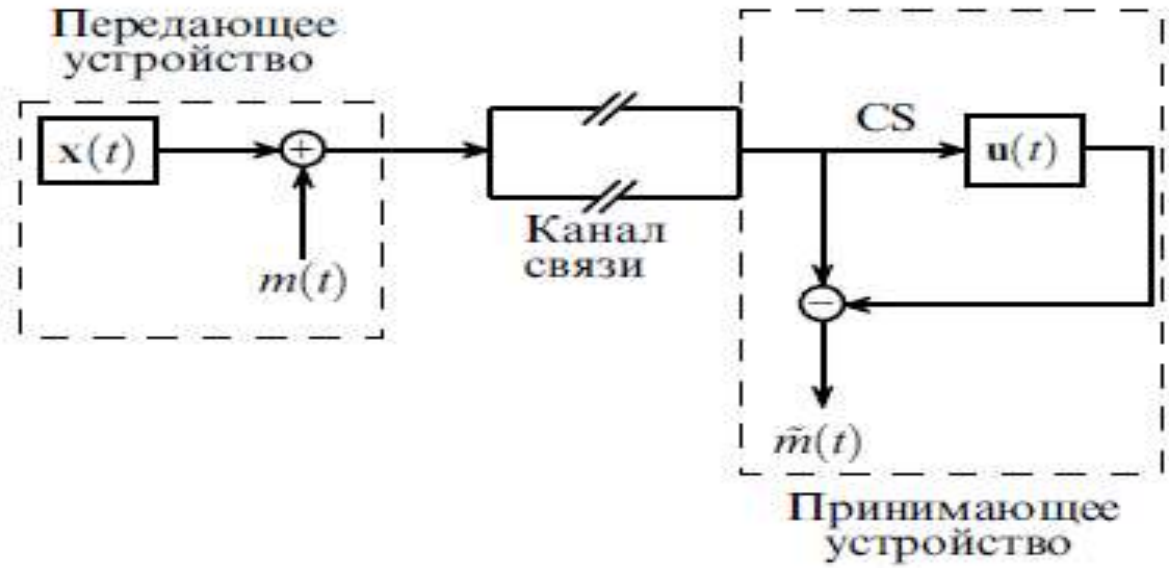
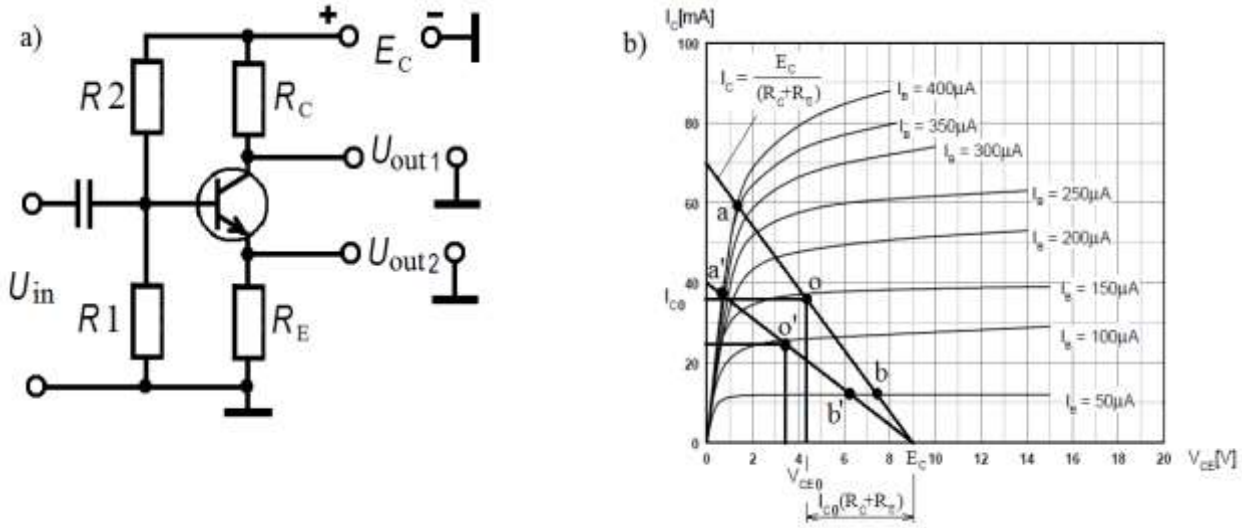
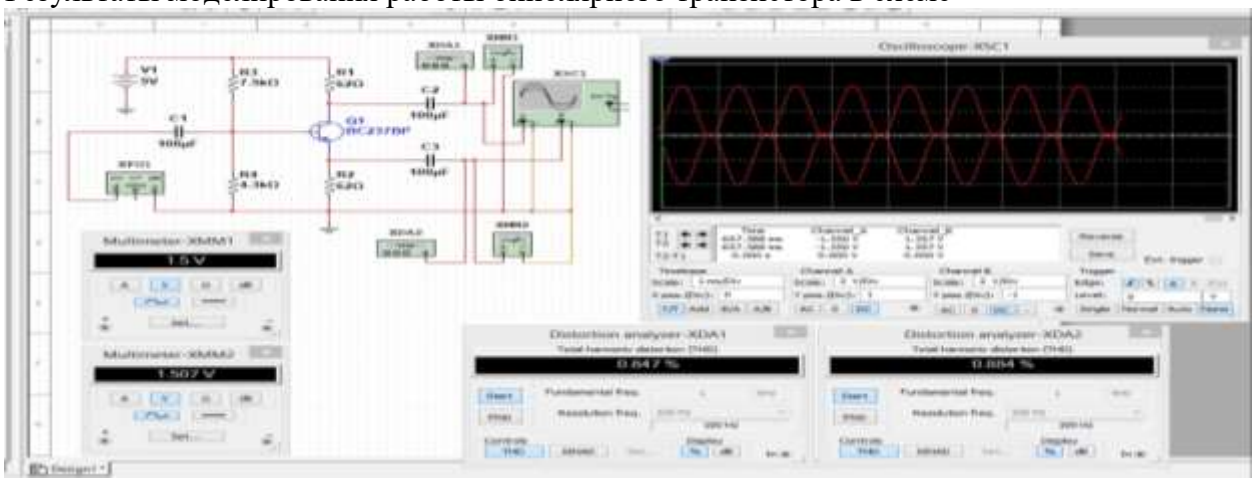


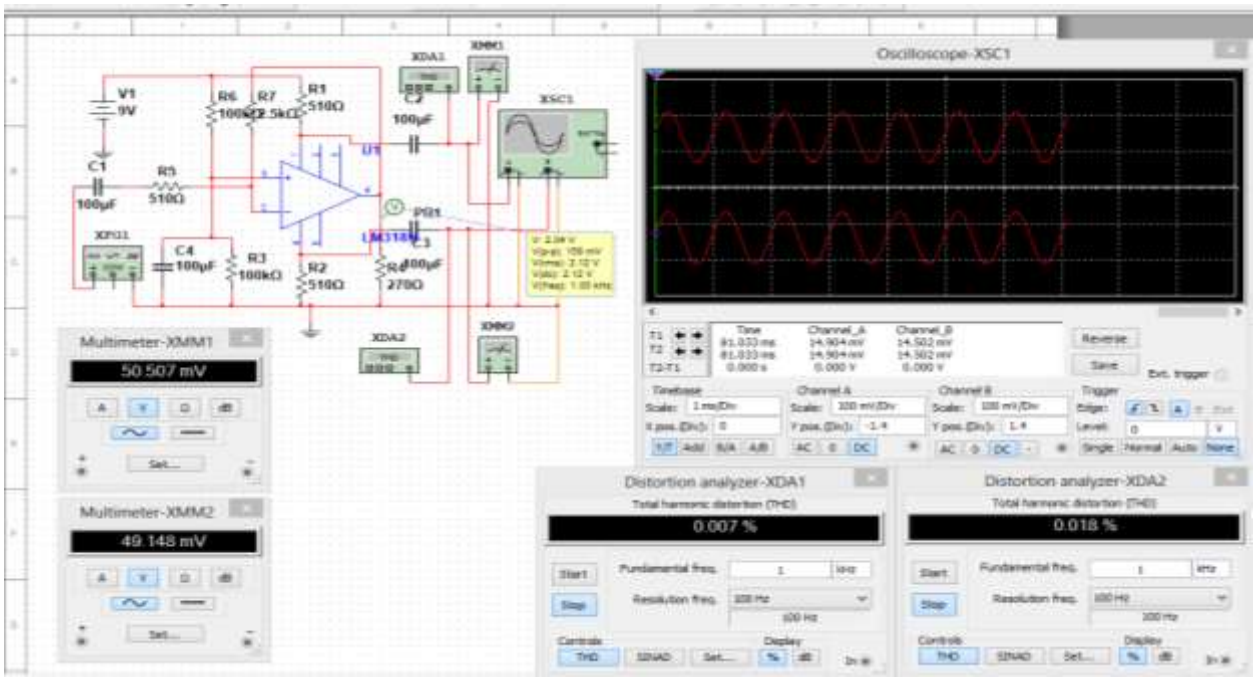
Схема фазоинверторного каскада на биполярном транзисторе(а); пример построения линий нагрузки в режиме большого сигнала на тразисторе (б)



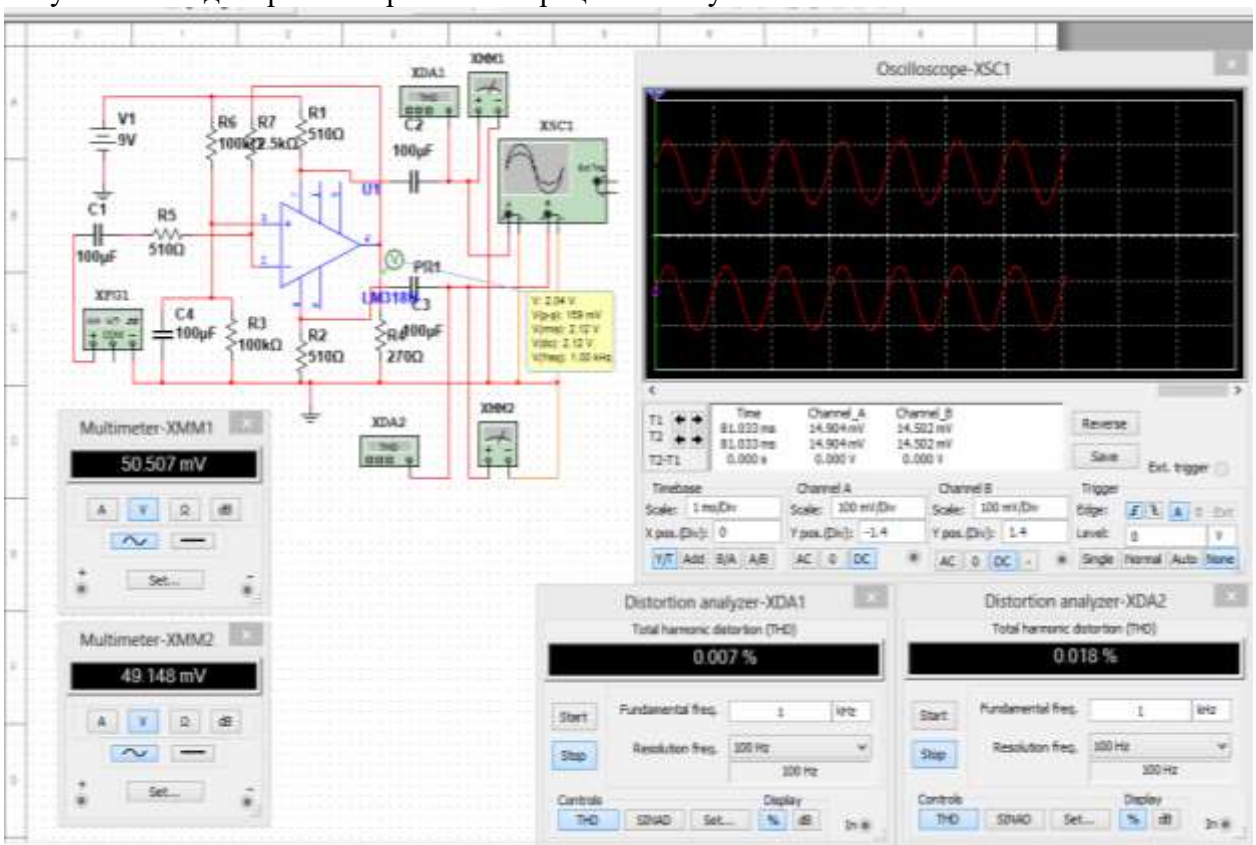
Результаты моделирования работы биполярного транзистора в схеме



Результаты моделирования работы полевого транзистора в схеме



Результаты моделирования работы операционного усилителя в схеме



Выводы

Из рассмотренных простейших схем фазоинверторных каскадов наилучший результат дала схема на биполярном таранзисторе каскада с параллельной отрицательной обратной связью по коллекторному напряжению. Даная схема имеет минимальное число компонентов, что позволяет использовать её для выностных датчиков, где требование к масса габаритным показателям и к потребляемой мощности жесткие. Для образования противофазного сигнала достаточного для подачи на АЦП через активный элемент требуется порядка нескольких десятков мА, что во многом определяет минимально необходимую мощность для данного каскада.