

**Ministerul Educației, Culturii și Cercetării al Republicii Moldova**  
**Universitatea Tehnică a Moldovei**  
**Departamentul Telecomunicații și Sisteme Electronice**

Admis la susținere

Șef departament TSE: conf. univ., dr. Sava Lilia

„ \_ ” \_\_\_\_\_ 2020

**Dezvoltarea platformei hardware și software cu  
un canal de comunicație criptat pentru  
dispecerizarea obiectelor industriale la distanță  
(partea Hardware)**

**Разработка программно-аппаратной  
платформы с зашифрованным каналом связи  
для диспетчеризации удаленных  
промышленных объектов  
(аппаратная часть)**

**Teză de master**

Student: \_\_\_\_\_ Pascal Victor, gr. SISRC-191M

Coordonator: \_\_\_\_\_ Șestacova Tatiana, conf. univ., dr.

Chișinău, 2020

## REZUMAT

PASCAL VICTOR

**Tema:** Dezvoltarea platformei hardware și software cu un canal de comunicație criptat pentru dispecerizarea obiectelor industriale la distanță (partea Hardware).

**Structura lucrării:** Introducere, 3 Capitole, Concluzii, Bibliografie, Anexe, 75-de imagini.

**Cuvinte-cheie:** hardware, canal de comunicație, ADC, AES-128, AVR, RS485.

**Scopul lucrării:** Dezvoltarea platformei hardware și software cu un canal de comunicație criptat pentru dispecerizarea obiectelor industriale la distanță.

**Obiectivele lucrării:** Analiză soluțiilor existente. Dezvoltarea unui controler pentru comunicarea cu un server la distanță. Furnizarea unui canal de comunicare criptat prin standardul AES-128 prin rețeaua 2G. Dezvoltarea unui controler de analizator de tensiune trifazată, cu capacitatea de a proteja împotriva asimetriei fazelor, de întrerupere a fazele și de a proteja împotriva alternării necorespunzătoare a fazelor. Asigurarea transferului de date către serverul de setări la distanță și starea controlerului analizatorului de tensiune trifazată.

**Metodele aplicate:** Programul Proteus7. Pentru dezvoltarea circuitelor și plăcilor a fost utilizat programul DIPTRACE.

**Rezultatele obținute:** A fost proiectat și creat propriul controler pentru a comunica cu serverul, a fost scrisă o bibliotecă pentru criptarea canalului de comunicații conform standardului de criptare AES-128, ceea ce a permis reducerea semnificativă a riscurilor de intervenție și atac asupra sistemelor noastre. Un algoritm software proiectat vă permite să modificați cu ușurință acest sistem pentru a lucra cu criptarea AES-256 și AES-512, fără o creștere semnificativă a memoriei utilizate. Un controler de analiză a rețelei a fost proiectat și conectat printr-o conectare galvanică la magistrala RS-485, la controlerul principal, pentru a transmite date despre starea rețelei trifazate. Toate aceste echipamente au fost instalate într-un scut de dispecerizare, instalat și conectat la serverul principal de colectare a informațiilor.

## АННОТАЦИЯ

PASCAL VICTOR

**Тема:** Разработка программно-аппаратной платформы с зашифрованным каналом связи для диспетчеризации удаленных промышленных объектов (аппаратная часть)

**Структура работы:** Введение, 3 Раздела, Заключение, Библиография, Приложение, 75 рисунков.

**Ключевые слова:** аппаратная часть, канал связи, АЦП, AES-128, AVR, RS485

**Цель работы:** Разработка аппаратной части платформы с шифрованным каналом связи для диспетчеризации удаленных промышленных объектов.

**Задачи:** Провести анализ существующих решений. Разработка контроллера для управления связи с удаленным оборудованием. Обеспечить шифрованный канал связи по стандарту AES-128 через сеть 2G(GPRS). Разработка контроллера анализатора трехфазного сетевого напряжения, с возможностью защиты от перекоса фаз, от обрыва фаз и защиты от неправильного чередования фаз. Обеспечить возможность передачи данных удаленному серверу параметров и состояния контроллера анализатора сети. Разработка конструкции аппаратной части проекта.

**Применяемые методы:** Программа виртуализации Proteus7. Для разработки схем и плат была использована программа DIPTRACE.

**Полученные результаты:** Был спроектирован и создан собственный контроллер для связи с сервером, написана библиотека для шифрования канала связи по стандарту шифрования AES-128, что позволило значительно снизить риски вмешательства и атаки на системы, оборудование, канал связи. Разработанный программный алгоритм позволяет легко модифицировать эту систему для работы с шифрованием AES-256 и AES-512, без значительного увеличения используемой памяти. Был спроектирован контроллер-анализатор сети и подключен гальванически отвязанной частью на шину RS-485 к основному контроллеру, для передачи данных о состоянии трехфазной сети. В совокупности все это оборудование было установлено в щит диспетчеризации, установлено на объекте и подключено к главному серверу сбора информации.

## ANNOTATION

PASCAL VICTOR

**Title:** Development of a hard- and software platform with an encrypted communication channel for dispatching of remote industrial objects (Hardware part)

**Thesis structure:** Introduction, 3 Sections, Conclusion, Bibliography, Appendix, 75 figures.

**Keywords:** hardware, communication channel, ADC, AES-128, AVR, RS485

**Thesis purpose:** Development of the platform hardware with an encrypted communication channel for dispatching remote industrial objects.

**Objectives:** Analyze existing solutions. Development of a controller for communication with remote equipment. Provide an encrypted communication channel according to the AES-128 standard through the 2G network (GPRS). Development of a controller for the analyzer of three-phase mains voltage, with the possibility of protection against phase imbalance, phase failure and protection against incorrect phase sequence. Provide the ability to transfer data to a remote server of parameters and status of the network analyzer controller. Development of the design of the hardware part of the project.

**Applied methods:** Program Proteus7, the DIPTRACE program was used to develop circuits and boards.

**The Obtained Results:** A proprietary controller for communication with the server was designed and created, a library was written for encrypting the communication channel according to the AES-128 encryption standard, which significantly reduced the risks of interference and attacks on systems, equipment, and communication channels. The developed software algorithm makes it easy to modify this system to work with AES-256 and AES-512 encryption, without significantly increasing the used memory. A network analyzer controller was designed and connected by a galvanically isolated part to the RS-485 bus to the main controller to transmit data on the state of the three-phase network. In total, all this equipment was installed in the dispatch panel, installed at the object and was connected to the main data collection server.

## СОДЕРЖАНИЕ

### ВВЕДЕНИЕ

<b>1. АНАЛИЗ СУЩЕСТВУЮЩИХ РЕШЕНИЙ .....</b>	<b>11</b>
1.1 Контролеры автоматики и диспетчеризации. ....	12
1.2 Анализ готовых устройств телеметрии. ....	16
<b>2. СТРУКТУРНАЯ СХЕМА СИСТЕМ ТЕЛЕМЕТРИИ И ДИСПЕТЧЕРИЗАЦИИ .....</b>	<b>19</b>
2.1. Требования к разрабатываемой системе .....	21
2.1.1. Общие требования. ....	21
2.1.2. Требования к контролеру автоматики и связи. ....	22
2.1.3. Требования к контроллеру сетевой защиты и анализатору сети. ....	22
2.2. Программное обеспечение реализации проекта .....	23
<b>3. РАЗРАБОТКА АППАРАТНОЙ ЧАСТИ ПРОЕКТА .....</b>	<b>23</b>
3.1. Выбор микроконтроллера и компонентов периферии. ....	24
3.2. Выбор дисплея .....	30
3.3. Построение электрической принципиальной схемы .....	32
3.3.1 Кварцевый резонатор и супервизор .....	32
3.3.2. Обвязка реле .....	33
3.3.3. Интерфейс RS-485 .....	34
3.3.4. DC-DC преобразователь .....	34
3.3.5. Символьный LCD индикатор .....	34
3.3.6. Энкодер управления .....	35
3.4. Разработка печатной платы .....	36
3.5. Обработка управления энкодера .....	40
3.6. Работа с LCD индикатором .....	42
3.7. Организация меню .....	44
3.8. Работа с UART .....	46
3.9. Протокол MODBUS RTU .....	48
3.10. Коммуникация по сети 2G .....	52
3.11. Внешний вид разработанного устройства .....	56
3.12. Метод шифрования AES-128 .....	58

3.13. Разработка анализатора сети с функцией контроля фаз.....	65
3.14. Описание принципа измерения.....	65
3.15. Щит автоматики и телеметрии.....	70
<b>ЗАКЛЮЧЕНИЕ .....</b>	<b>72</b>
<b>ПРИЛОЖЕНИЯ.....</b>	<b>74</b>

## ВВЕДЕНИЕ

В наше время все больше и больше требуется различных автоматизированных систем управления. Такие системы способны работать, как с человеком, так и без него, в зависимости от назначения системы. Современные станки и различное автоматическое и полуавтоматическое оборудование, способно работать с высокой точностью и скоростью, значительно повышая производительность и качество изготавливаемых изделий. Устройства автоматики способны заменить человека, если требуется работа суровых условиях, или в местах где человек не способен долго находится. При этом контроллеры способны передавать свое состояние и состояние различных датчиков на значительные расстояния, если это необходимо. Контроллеры и различные датчики нашли очень широкое применение во многих сферах производства и автоматизации, в измерениях. Существует большое количество датчиков для измерения температуры, давления, состава вещества, положения приводов и прочие...

Основой любой системы автоматики с диспетчеризацией является контроллер. Многие современные контроллеры оснащены функцией удаленного мониторинга, а иногда и управления. Такие контроллеры позволяют следить за процессом и управлять удаленно посредством радиосвязи, сети интернет, проводной сети. Эти устройства очень надежны и могут проработать десятки лет. Для обеспечения совместимости датчиков, контроллеров и прочих устройств было принято несколько промышленных стандартов, как цифровых так и аналоговых. Самые распространенные из них это протоколы Modbus, Profibus, Profinet. Для аналоговых датчиков и сигналов принято использовать токи 4..20 ма и напряжения 0..10В.

Контроллеры могут быть расширяемые и не расширяемые как законченное устройство. Модули беспроводной связи могут быть как внутренние, так и внешние. Для контроллеров производятся различные блоки расширения под любые нужды. Контроллеры, анализируя приходящие данные с датчиков, в соответствии с внутренней программой определяют дальнейшие действия, либо просто передают эти данные посредством беспроводных или проводных сетей на сервер управления, а сервер в свою очередь уже определяет, что с ними делать и какие команды управления передавать обратно контроллеру. Таким образом, системы могут быть неуправляемые извне – только наблюдение, телеметрия. И системы, которые управляются сервером – системы диспетчеризации.

**Цель работы:** Разработка аппаратной части платформы с шифрованным каналом связи для диспетчеризации удаленных промышленных объектов.

Для достижения поставленной цели надо решить следующие **задачи**:

1. Провести анализ существующих решений.
2. Выбор контроллера для управления связи с удаленным оборудованием.
3. Обеспечить шифрованный канал связи по стандарту AES-128 через сеть 2G(GPRS).
4. Разработка контроллера анализатора трехфазного сетевого напряжения, с возможностью защиты от перекоса фаз, от обрыва фаз и защиты от неправильного чередования фаз.
5. Обеспечить возможность передачи данных удаленному серверу параметров и состояния контроллера анализатора сети.
6. Разработка конструкции и аппаратной части проекта.



## БИБЛИОГРАФИЯ

1. Maxim Integrated: Copyright © 2020 Maxim Integrated Disponibil: <https://www.maximintegrated.com/en/products/interface/transceivers/MAX485.html>
2. 8-bit Atmel Microcontroller with 128Kbytes In-System Programmable. Disponibil: Flash <http://www.atmel.com/images/doc2467.pdf>
3. <https://ru.wikipedia.org/wiki/HD44780>
4. LM809/LM810 3-Pin Microprocessor Reset Circuits. Disponibil: <http://www.ti.com/lit/ds/symlink/lm809.pdf>
5. Modile Sim900B Disponibil: <http://we.easyelectronics.ru/part/gsm-gprs-modul-sim900.html>
6. Modile Sim900-GPRS Disponibil: <https://alex-exe.ru/radio/wireless/gsm-sim900-gprs/>
7. Microcontroller SIMATIC S7-1200 Disponibil: [https://www.siemens-ru.com/taxonomy/term/17](https://www.siemens.ru.com/taxonomy/term/17)
8. Универсальный асинхронный приемопередатчик (UART). Disponibil: <http://masters.donntu.org/2004/fema/kovalenko/library/art7.html>
9. Программный способ избавления от дребезга. Disponibil: <https://uscr.ru/drebezg-kontaktov-i-sposoby-podavleniya-drebezga/>
10. Визуальная среда Arduino и ESP8266/. Disponibil: <https://habr.com/ru/company/flprog/blog/262521/>
11. Стандарт RS-485. Disponibil: <https://www.softelectro.ru/rs485.html>
12. Протокол Modbus. Disponibil: [https://wirenboard.com/wiki/index.php/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB\\_Modbus](https://wirenboard.com/wiki/index.php/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_Modbus)
13. Внутренняя документация на контроллер RT700. Disponibil: <http://raxus.md/content.php?id=16>