Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.4

Григоришин
Вадим Александрович

# ЗАЩИЩЕННЫЙ РАДИОКАНАЛ ДЛЯ ДИСТАНЦИОННОГО УПРАВЛЕНИЯ АВТОМАТИЗИРОВАННЫМИ ОБЪЕКТАМИ

**АВТОРЕФЕРАТ**
на соискание степени магистра технических наук
по специальности 1 - 40 80 01 Элементы и устройства вычислительной техники и систем управления

Научный руководитель

Д.С. Лихачев,
кандидат технических наук,
доцент

Минск 2019

Нормоконтроль

Д.С. Лихачев

# ВВЕДЕНИЕ

Существует множество объектов, как промышленного, так и бытового назначения, в которых присутствует в той или иной степени автоматизация различных процессов. При удаленном контроле и управлении такими автоматизированными объектами используется пакетная передача данных, по радиоканалу или другим системам телекоммуникации, непосредственно с самого автоматизированного объекта на централизованный пульт оператора.

При использовании открытого радиоканал в автоматизированных системах управления для передачи пакетных данных между составными модулями системы и централизованным пультом оператора влечет необходимость обеспечения безопасности информации от несанкционированного доступа, передаваемой по радиоканалу, используются различные методы и ограничения доступа к передаваемой и принимаемой информации.

Для защиты информации сегодня широко используются различные программные и аппаратные методы защиты информации, которые применяются в автоматизированных системах управления различных технологических процессов, различных автоматических системах управления освещением. В такие системы автоматизированного управления строятся на базе модулей, а связь между модулями осуществляется по стандартным протоколам обмена информацией.

В свою очередь, использование стандартных протоколов обмена данными дает широкую возможность применения систем аппаратного и программного шифрования в различных сегментах промышленности, где используется хоть какая–либо автоматизация каких-либо процессов.

Цель: реализация защищенного радиоканала для дистанционного управления автоматизированными объектами.

Объект исследования: методы и алгоритмы защиты информации в автоматизированных системах с открытым радиоканалом.

Предмет: процесс защиты информации отправляемой по открытому радиоканалу в составе автоматизированного объекта.

Задачи:

1. Обзор существующих методов защиты информации на предмет использования в защищенном радиоканале для дистанционного управления автоматизированных объектов.
2. Анализ существующих методов защиты информации на предмет интеграции в существующие системы управления автоматизированными объектами по средствам существующих стандартизированных протоколов.
3. Синтез нового метода защиты информации, передаваемой по радиоканалу.

# ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

## Актуальность исследования

Применение системы автоматизированного контроля и управления объектами с зашифрованным радиоканалом особенно актуально в нефтегазовой промышленности, в системах газораспределения, в газовых котельных, на газовых распределительных подстанциях, в системах контроля и учета электроэнергии, в системах дистанционного управления стратегически важными объектами, узлами, оборудованием, т.е. там, где скорость и последствия принятия решения имеют существенное значение.

## Цель исследования

Целью диссертационной работы исследование существующих методов защиты информации, передаваемой по радиоканалу, для дистанционного управления автоматизированными объектами и синтез нового метода защиты информации с учетом преимуществ и недостатков существующих методов защиты информации.

## Задачи исследования

1. Обзор существующих методов защиты информации на предмет использования в защищенном радиоканале для дистанционного управления автоматизированных объектов.
2. Анализ существующих методов защиты информации на предмет интеграции в существующие системы управления автоматизированными объектами по средствам существующих стандартизированных протоколов.
3. Синтез нового метода защиты информации, передаваемой по радиоканалу.

## Новизна полученных результатов

Научная новизна заключается в том, что был синтезирован новый метод защиты информации на базе существующих методов и алгоритмов защиты информации. Синтезированный метод имеет высокую степень криптостойкости к подбору ключа для дешифровки отправляемых и получаемых данных. Имеет высокое быстродействие выполнения алгоритма шифрования данных, что дает возможность использование синтезированного метода в системах реального времени.

Синтезированный метод можно применять в различных системах автоматизации с открытым радиоканалом, где пакетные данные передаются согласно существующих стандартизированных протоколов обмена данными, так и в системах где пакетные данные передаются по индивидуальным и собственным протоколам.

**Личный вклад соискателя.**

Соискателем выполнены все изложенные в работе разработки и исследования. Постановка задач и обсуждение результатов проводились совместно с научным руководителем и сотрудниками кафедры электронных вычислительных средств Белорусского государственного университета информатики и радиоэлектроники. Обработка, интерпретация данных, а также выводы сделаны автором самостоятельно.

**Апробация результатов диссертации**

Основные положения диссертационной работы докладывались на следующих научных конференциях:

– 54–я научная конференция аспирантов, магистрантов и студентов БГУИР, 2018 г.

# СОДЕРЖАНИЕ РАБОТЫ

Использование открытого радиоканала в качестве шлюза приема и передачи пакетных данных между модулями и централизованным пультом оператора системы автоматизации влечет за собой обеспечение надежной передачи информации с обеспечением её полной сохранности и защищенности.

В первой главе диссертационной работы приведены и рассмотрены основные способы и методы защиты информации как на физическом уровне, так и на аппаратном и программном уровнях. Названы преимущества и недостатки каждого из приведённого метода защиты информации. Дана классификация существующих алгоритмов шифрования. Приведено сравнение симметричных и ассиметричных алгоритмов шифрования информации.

Во второй главе диссертационной работы формулируются основные требования, предъявляемые к защищенному радиоканалу для дистанционного управления автоматизированными объектами, такие как:

– надежная защита от несанкционированного подключения и доступа к удаленному объекту, а также к централизованному пульту оператора;

– надежная защита от несанкционированного перехвата передаваемой информации и дальнейшего использования перехваченной информации для управления и контроля автоматизированным объектом;

– зашифрованный радиоканал должен иметь устойчивую и надежную криптозащиту информации, передаваемой на большие расстояния.

Приведены и рассмотрены спецификации основных протоколов обмена информацией между составными блоками автоматизированного объекта, которые сегодня активно используются ведущими производителями оборудования для систем автоматизации. Такие как Schneider Electric, Siemens, ABB, FINDER, ОВЕН.

Протоколы обмена информацией:

- протокол обмена информацией MODBUS RTU, MODBUS ASCII;
- протокол обмена информацией OWEN;
- протокол обмена информацией DALI.

Рассмотрены основные алгоритмы защиты информации. Приведены примеры использования каждого алгоритма защиты информации для стандартизированного протокола обмена информацией MODBUS RTU, а именно:

- алгоритм замены;
- алгоритм перестановки;
- алгоритм блочного шифрования

На базе приведенного материала во второй главе, были сформулированы основные требования для синтеза нового метода, который в наибольшей степени отвечает критериям для реализации защищенного радиоканала.

В третьей главе диссертационной приведено непосредственно программная реализация синтезированного метода на базе микроконтроллера DsPIC33FJ64GS606, с максимальной загрузкой ядра в 40 MIPS. Симбиоз синтезированного метода заключается в замене символов исходного сообщения, записанных в исходном алфавите, символами из шифрованного алфавита по определенному правилу, которое будет определяться одним из алгоритмов блочного шифрования. Также предусмотрены смена исходного алфавита с последующей сменой шифрованного алфавита, вычисляемого по секретному алгоритму.

В четвертой главе производится анализ синтезированного метода защиты информации, передаваемой по радиоканалу для дистанционного управления автоматизированными объектами на криптостойкость и на вычислительную сложность. Также приводится сравнительная характеристика с классическим методом замены. Приведены основные расчеты синтезированного метода на вычислительную сложность, а также синтезированный метод проанализирован на количества возможных вариантов подбора секретного ключа, для дешифровки получаемых и отправляемых данных, т.е. проведена оценка криптостойкости синтезированного метода.

# ЗАКЛЮЧЕНИЕ

В диссертации рассмотрены и проанализированы основные методы защиты, ограничение доступа к информации, передаваемой по радиоканалу для управления удаленными автоматизированными объектами.

Приведены и рассмотрены спецификации протоколов обмена информацией использующиеся в системах автоматического управления, в системах автоматизированных технологических процессов, в автоматизированных системах управления освещением различного назначения и применения. Даны подробное описание структуры протоколов обмена информацией между ведущим и ведомым и наоборот. Подробно рассмотрен состав отправляемых и принимаемых сообщений по протоколу Modbus.

На основании анализа существующих методов защиты информации, был синтезирован метод защиты информации на основании метода замены и метода блочного шифрования, т.к. передаваемые сообщения можно разбить на блоки. При синтезе нового метода защиты информации, передаваемой по радиоканалу для дистанционного управления автоматизированными объектами, учитывалось необходимость обеспечения высокой надежности информации к перехвату и дальнейшей дешифровки сообщений, необходимость высокоскоростной работы синтезируемого метода при шифровке и подготовке пакетов данных к отправке.

Синтезируемый метод защиты информации для дистанционного управления автоматизированными системами выполняет следующие функции:

– вычисление шифрованного алфавита на основе исходного алфавита, используя один из алгоритмов блочного шифрования. В данном случае шифрованный алфавит не будет доступен пользователю, что резко повышает степень криптозащиты шифруемой информации;

– выбор позиции при шифровании исходного сообщения при использовании шифрованного алфавита осуществлять одним из алгоритмов блочного шифрования;

– использовать определенные секретные коэффициенты при шифровании информации;

– предусмотреть смену исходного алфавита с полным пересчетом шифруемого алфавита;

– предусмотреть смену коэффициентов используемых при шифровании исходных сообщений;

– обеспечить высокое быстродействие метода шифрования, для использования в системах реального времени.

Синтезированный метод защиты информации, передаваемой по радиоканалу, обладает такими характеристиками как вычислительная сложность шифрования закрываемой информации, криптостойкость зашифрованной информации синтезированным методом к дешифровке и дальнейшего ее использования.

Вычислительная сложность синтезированного метода заключается в количестве операций, затрачиваемых на шифрование, криптозакрытие одного символа исходного текста. Вычислительная сложность синтезируемого метода защиты информации при шифровании отправляемого сообщения по радиоканалу загружает ядро микроконтроллера на $37*10^{-4}$%, что дает возможность использования синтезированного алгоритма при максимальных скоростях передачи информации без каких-либо потерь искажений, зашифрованных данных.

Криптостойкость синтезированного метода заключается в подборе шифрованного и исходного алфавита, а также в подборе коэффициентов секретных алгоритмов. Трудоемкость и количество возможных вариантов подбору ключа и исходного и шифрованного алфавита – это и есть криптостойкость зашифрованной информации ко взлому. На шаге выполнения синтезированного метода защиты информации количество возможных вариантов растет в геометрической прогрессии, и на момент окончания шифрования символа отправляемого сообщения составляет 903152589848819647119360 вариантов подбора при дешифровке зашифрованного символа.

# СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1. Григоришин, В.А. Защищенный радиоканал для дистанционного управления автоматизированными объектами / В.А. Григоришин// 54–я научная конференция аспирантов, магистрантов и студентов БГУИР 2018, Минск, 25-26 апреля 2018 г. / – с. 232