

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

УДК _____

Турок
Максим Андреевич

Программное средство для устройства блокировки кодграббера

АВТОРЕФЕРАТ

на соискание степени магистра информатики и вычислительной техники
по специальности 1–40 81 02 Технологии виртуализации и облачных
вычислений

Научный руководитель

Золоторевич Людмила Андреевна

Кандидат технических наук, доцент

Минск 2020

ВВЕДЕНИЕ

Автосигнализация призвана защитить автомобиль от угона. Сложно переоценить ее актуальность и роль в сохранности автомобиля и его содержимого. Однако при выборе автосигнализации автовладелец обращает в первую очередь на уровень безопасности, который может обеспечить автосигнализация, и на ее стоимость.

Оптимальным по соотношению цена/качество являются автосигнализации с динамическим кодом. Данный вид сигнализаций имеет небольшую стоимость, но у нее существуют уязвимости, которыми успешно пользуются злоумышленники. Самым популярным техническим средством для проведения атаки являются кодграбберы – устройства, вмешивающиеся в обмен информацией между блоком управления сигнализацией и брелком.

Вносить помехи в нормальную работу автосигнализаций мобильных объектов могут также и естественные помехи.

Таким образом, разработка программного обеспечения для устройства, которое смогло бы анализировать естественные и искусственные помехи и исправлять их, является актуальной задачей.

В работе исследуются возможные угрозы информационной безопасности в автосигнализациях мобильных объектов, устройства (кодграбберы), которые используются для проведения атак, методы их парирования, а также факторы, которые могут повлиять на работу автосигнализации.

В результате проведенных исследований формируются требования к устройству для блокировки кодграббера, разрабатывается его структурная схема и осуществляется подбор компонентов, подходящих для создания данного устройства.

Итогом работы является разработка программного средства для устройства, блокирующего атаки кодграббера.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Объектом исследования являются принципы защиты информации, современные системы автомобильной сигнализации, эффективность их применения и стоимость.

Предметом исследования являются используемые в автосигнализациях способы защиты информации, передаваемой по радиоканалу, угрозы, которым подвержены исследуемые способы защиты, а также способы парирования этих угроз. **Цель исследования** – разработка программного обеспечения для принимающего и анализирующего радиосигнал программно-аппаратного комплекса, предназначенного для защиты от перехвата информации в системе автосигнализации злоумышленником при помощи код-граббера.

Задачи исследования:

1. Обзор существующих систем автосигнализации, используемых ими протоколов обмена информацией и принципов защиты информации во время ее передачи. Анализ возможных свойственных способу угроз, а также подходов к их парированию.

2. Разработка требований к аппаратной части программно-аппаратного комплекса. Разработка структурной схемы программно-аппаратного комплекса, выбор подходящих компонентов.

3. Разработка алгоритма и реализация его на языке программирования «С», проведение моделирования его работы.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

В первом разделе рассмотрены существующие системы автомобильной сигнализации с точки зрения защиты передаваемой по радиоканалу информации. Произведена классификация систем по используемому каналу связи (односторонний либо двусторонний), по способу защиты системы от перехвата сигнала (статический, динамический, диалоговый код). Подробно описан алгоритм защиты KeeLoq, использующийся в системах с односторонним каналом связи и динамическим кодированием передаваемой информации. Сделан анализ уязвимостей этой защиты. Описан принцип работы кодграбберов – класса устройств, которые используются для атак на системы автосигнализации с односторонним каналом связи. Сделаны выводы о том, как возможно обнаружить и парировать попытки атаки кодграббером.

Во втором разделе показана структурная схема устройства, для которого разработано программное средство. Устройство представляет собой дополнение к уже установленной системе автосигнализации, которое принимает сигнал, обрабатывает его и передает блоку управления автосигнализацией. Произведено сравнение и выбор среди аналогов двух ключевых компонентов устройства – приемника и микроконтроллера.

В третьем разделе описана работа реализованного алгоритма, приведена частичная блок-схема алгоритма. Произведено моделирование работы алгоритма в среде Proteus. Показаны сигналы, принятые и обработанные программно-аппаратным комплексом.

В приложении А показан исходный код программного средства на языке программирования «С» для микроконтроллера ATtiny84, находящегося в составе устройства.

ЗАКЛЮЧЕНИЕ

Исследованы системы автосигнализации, использующие различные способы защиты от перехвата передаваемой информации, более подробно рассмотрен один из этих способов.

Подробно проанализирован защищенный протокол передачи данных KeeLoq. В работе показано, что сам алгоритм шифрования до сих пор никем не взломан, однако существуют уязвимости, позволяющие с использованием специального устройства обойти защиту без взлома шифрования. Также описаны способы обнаружения попытки атаки.

Разработано программное обеспечение, которое, находясь в составе устройства, дополняющего существующую систему автосигнализации, позволяет парировать некоторые виды атак, в которых используется кодграббер с алгоритмом кодоподмены. Проведено моделирование работы программного обеспечения, при котором был получен ожидаемый результат.

Описано устройство, в котором может быть применено разработанное программное средство. Выбраны подходящие ключевые компоненты устройства.

Таким образом, показано, что при внесении производителем реализованного алгоритма в собственную систему автосигнализации, возможно защитить систему от атак с использованием описанных уязвимостей.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

Защита передаваемой информации в автомобильной сигнализации // М. А. Турок // 55-я юбилейная научная конференция аспирантов, магистрантов и студентов. Сборник тезисов докладов. Минск, БГУИР, 2019. С.

Корректировка алгоритма работы устройства блокировки работы кодграббера // М. А. Турок // Проблемы информатики, радиоэлектроники и защиты информации. Сборник трудов постоянно действующего семинара «Проблемы информатики, радиоэлектроники и защиты информации», том 1, заседание 04.01.2019. Под редакцией Г. В. Сечко / ООО «Стрим центр». – Минск, 2019.

Библиотека БГУИР