



Для определения статистических характеристик максимальных значений давления на наш взгляд целесообразно применить микроконтроллер, который сможет обработать поступающие на его входы значения с датчика.

В качестве микроконтроллера было решено взять аппаратную платформу Arduino Uno. Эта платформа удобна тем, что на одной плате распложен, как сам микроконтроллер, так и программатор [2]. Для вывода информации используется LCD дисплей 1602А.

Алгоритм работы программы для регистрации максимальных давлений в цилиндре двигателя выглядит следующим способом:

- 1) На аналоговый вход микроконтроллера подается сигнал с датчика температуры
- 2) Записываются 10 значений аналогового сигнала в массив
- 3) После заполнения первого массива, записываются следующие 10 значений аналогового сигнала во второй массив (Рисунок 3).
- 4) Вычисляются средние значения в каждом из массивов
- 5) Сравниваются полученные два значения
- 6) Если значение второго среднего больше, чем значение первого среднего, то программа возвращается ко 2 пункту, это означает, что значение еще растет, и оно не достигло пикового значения
- 7) Если значение второго среднего меньше первого, то это означает, что значение сигнала начало убывать, и было достигнуто пиковое значение
- 8) Далее выполняется условие, где сопоставляется полученное значение с аналогового входа микроконтроллера с напряжением на выходе датчика ($0 - 5$ вольт = $0 - 1023$), где, например, $0-1.25$ В соответствует значению $0 - 256$, полученный с входа МК
- 9) Число пиковых значений записывается в соответствующий счетчик.

Таким образом, разрабатываемый программно-аппаратный комплекс позволит построить закон распределения давления в цилиндре, что дает возможность в штатном режиме работы двигателя диагностировать первые признаки неисправной его работы.

Литература

1. Проверка компрессии (давления) в цилиндрах двигателя автомобиля. Электронный ресурс: <http://cartore.ru/77-proverka-kompressii-v-cilindrah-dvigatelya.html>. Дата обращения: 15.03.2016.
2. Arduino Uno | Аппаратная платформа Arduino. Электронный ресурс: <http://arduino.ru/Hardware/ArduinoBoardUno>. Дата обращения: 15.03.2016.
3. Исследование неидентичности рабочего процесса двигателя ВАЗ-11194 с помощью индентирования / К.В. Приходьков, К.И. Лютин, В.В. Осин, Д.Н. Авдеюк // Известия ВолгГТУ. Сер. Наземные транспортные системы. Вып. 11. - Волгоград, 2015. - № 5 (165). - С. 51-55.
4. Авдеюк, Д.Н. Исследование межциклового неидентичности процесса сгорания в двигателе с искровым зажиганием / Д.Н. Авдеюк, В.В. Осин, К.В. Приходьков // Сборник тезисов докладов по внутривузовскому смотру-



конкурсу научных конструкторских и технологических работ студентов (г. Волгоград, 12-15 мая 2015 г.) / ВолгГТУ, Совет СНТО. - Волгоград, 2015. - С. 153-154.

Е.О. Васюкова, М.А. Пеливан, А.В. Яковлев

ИСПОЛЬЗОВАНИЕ RFID-КАРТ КАК АУТЕНТИФИКАТОРА В ПРОГРАММНО-АППАРАТНОМ КОМПЛЕКСЕ ПО ПРЕДУПРЕЖДЕНИЮ КРАЖ ВЕЛОСИПЕДОВ

(Тамбовский государственный технический университет)

В наше время кражи велосипедов очень часто встречающееся явление. Это одно из самых распространённых преступлений не только в России, но и в Европейских странах со спокойной криминогенной обстановкой. По статистике очень мало велосипедов возвращаются к своим владельцам. В основном велосипеды крадут с велостоянок в общественных местах либо пристёгнутого замком, либо оставленного на время без средств защиты. Современные противоругонные устройства для велосипеда только частично помогают бороться с воровством.

Условия содержания «железного коня» в безопасности от краж ничтожна, а именно этому способствуют плохо оборудованные и небезопасные места парковки.

Программно-аппаратный комплекс по предупреждению краж велосипедов предназначен для снижения количества краж велосипедов, а также обеспечения возможности поиска украденных велосипедов по БД на основе применения RFID-меток.

На сегодняшний день известно большое количество средств идентификации и аутентификации, но не все они одинаково пригодны для реализации проекта. RFID-метки обладают следующими преимуществами, которые важны для реализации программно-аппаратного комплекса [1]:

- запись большого объема информации на метку;
- шифрование и защита данных: возможна установка пароля на операции чтения и записи, вследствие чего защита от краж и подделок;
- защита меток от вредных факторов и более долгий срок службы (RFID-метка может быть использована до 100000 раз);
- распознавание движущихся объектов.

Принцип функционирования RFID-меток основан на использовании электромагнитной индукции, наводимой в антенне RFID-метки, в качестве источника питания, внедренной в нее микросхемы [1,2].

Рассмотрим применение RFID-метки на примере оборудования велопаркомата. Владелец велосипеда обладает RFID-картой, подтверждающей его право собственности. Для осуществления парковки владелец устанавливает свой велосипед в блокирующее устройство и осуществляет его фиксацию. Для раз-



блокировки велосипеда владельцу необходимо приложить RFID-карту к считывателю паркомата, при этом будет вычислена хэш-функция карты, значение которой будет сравнено со значением хэш-функции, полученной от RFID-метки, внедренной в велосипед (рис. 1).

Протокол обмена между считывателем RFID-карты программно-аппаратным комплексом и считывателем RFID-метки велосипеда при операции аутентификации формально может быть представлен следующим образом:

- 1) $T \rightarrow R_r: XYZ | H_r(XYZ + SALT);$
- 2) $T \rightarrow R_i: XYZ | H_i(XYZ + SALT);$
- 3) если $H_r(XYZ + SALT) = H_i(XYZ + SALT)$, то разблокировка.



Рисунок 1 – Формализованный протокол оборудования велопаркомата

Так как у велосипеда есть уникальный номер – номер рамы, его и будем использовать в качестве идентификатора (на рис. 1 XYZ). Сейчас на рынке представлено большое количество велосипедных марок, например: «Merida», «Stels», «GT» и другие. Количество символов в номере рамы, соответственно, у каждой марки разное. Допустим, максимальное количество, используемое в номере – 11 символов, но для большей универсальности зарезервируем 15 символов под идентификатор. Исходя из существующего стандарта KOI-8(ASCII), в котором на 1 символ приходится 8 бит, получаем, что для хранения идентификатора потребуется 110 битов. Исходя из анализа литературы [2-4] была выбрана хеш-функция SHA-2, с длиной дайджеста – 224 бита. Соответственно длина соли составит 114 бит, а степень образующего полинома должна быть не меньше 7. Таким образом, подходящей для наших целей полином, имеет вид: $x^7+x^3+x^2+x+1$ [5]. А длина всей последовательности, из которой будет выбрана соль, равна 128 бит.

Рассмотрим пример формирования данных, которые будут содержаться на RFID-карте и RFID-метке. На рисунке 2 представлено соответствие различных символов их десятичному эквиваленту по стандарту KOI-8.



48 0	49 1	50 2	51 3	52 4	53 5	54 6	55 7
56 8	57 9	58 :	59 ;	60 <	61 =	62 >	63 ?
64 @	65 A	66 B	67 C	68 D	69 E	70 F	71 G
72 H	73 I	74 J	75 K	76 L	77 M	78 N	79 O
80 P	81 Q	82 R	83 S	84 T	85 U	86 V	87 W
88 X	89 Y	90 Z	91 [92 \	93]	94 ^	95 _
96 "	97 a	98 b	99 c	100 d	101 e	102 f	103 g
104 h	105 i	106 j	107 k	108 l	109 m	110 n	111 o
112 p	113 q	114 r	115 s	116 t	117 u	118 v	119 w
120 x	121 y	122 z	123 {	124	125 }	126 ~	127

Рисунок 2 – Таблица ASCII

Имеется номер рамы велосипеда *T2098R0137*, его же принимаем за идентификатор. Десятичное представление идентификатора имеет вид *84504857568248495155*. Также, для удобства, приведем двоичное и шестнадцатичное представления: *0101010000110010001100000011100100111000010100100011000000110001001100110111* и *54323039385230313337 h*. Выбираем начальное заполнение для генератора псевдослучайных чисел (рис. 3), например *00011001 (19 h)*. Получается следующая последовательность, из которой будет формироваться с определенным символом криптографическая соль: *100110000001000111110100110100010111011011011111100001010110010011110010100100101101010101000001100100001110101110011100011011 (9811F4D17B77F0AC4F292D50643AE71B h)*. Символ, с которого будем считываться соль, случайно генерируется программой, написанной на языке C++. Допустим, криптографическая соль будет формироваться с 24 символа, тогда она будет иметь вид: *01110111111000010101100010011110010100100101101010100000110010000111010111001110000010001111010011 (1DFC2B13CA4B54190EB9C6E6047D3 h)*.

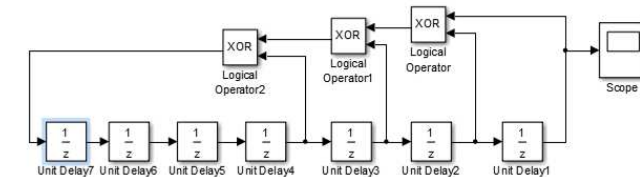


Рисунок 3 – Генератор случайной последовательности

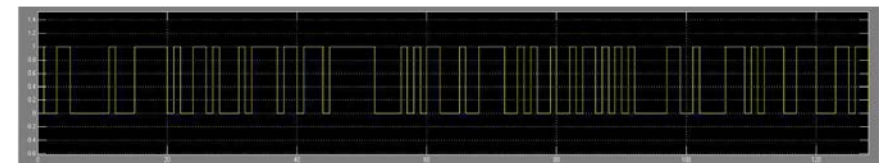


Рисунок 4 – Представление случайной последовательности

Таким образом на RFID-карте будут храниться три атрибута, а именно: идентификатор, длина последовательности и смещение относительно начального значения ПСЧ (для формирования соли) (рис. 5).



Кроме того, на карте возможно будет храниться, реализация ПСЧ. Поэтому при взаимодействии со считывателем, на выходе с устройства получим идентификатор и соль.

Используя ту же схему взаимодействия карты, но только с мобильным считывателем, возможно следующее применение – поиск угнанных велосипедов. Владелец украденного велосипеда предоставляет в органы полиции RFID-карту, подтверждающую право собственности и заявление о краже. Полученная информация заносится в БД угнанных велосипедов.

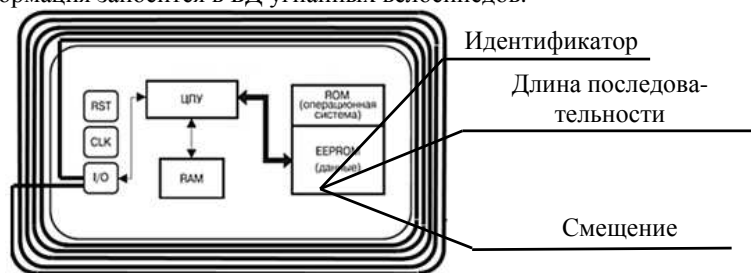


Рисунок 5 – Атрибуты, хранящиеся на карте

Полицейский с портативным считывателем осуществляет бесконтактную проверку велосипедов и в автоматическом режиме производится анализ, находится ли в розыске данный велосипед (рис. 6).

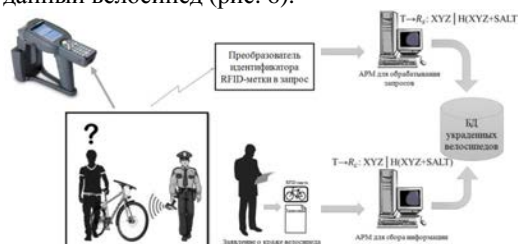


Рисунок 6 – Протокол обработки информации по угнанным велосипедам

Таким образом, данный программно-аппаратный комплекс позволит значительно снизить количество краж велосипедов, а также облегчит работу сотрудников полиции в мониторинге и поиске украденных велосипедов. Он будет полезен для бизнеса – в реализации сервиса проката, для полиции – в поиске украденных велосипедов по БД и для городского коммунального хозяйства – в обеспечении безопасных велопарковок.

Литература

1. Finkenzeller, K. RFID handbook / K. Finkenzeller. – UK: Wiley, 2010. – 462 с.
2. Фергюсон, Н. Практическая криптография / Н. Фергюсон, Б. Шнайер. – М.: «Диалектика», 2004. – 432 с.



3. SHA-2. FIPS 180-3 NIST, Federal Information Processing Standards Publication 180-3, Secure Hash Standards (SHS), August 2001.

4. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. – М.: Триумф, 2002. – 610 с.

5. Кнут, Д. Искусство программирования. Сортировка и поиск / Д. Кнут. – 2-е изд. – М.: Вильямс, 2007. – С. 824.

О.К. Головнин, Е.О. Кондратьева

ИНТЕЛЛЕКТУАЛЬНАЯ ГИС ITSGIS В УПРАВЛЕНИИ ТРАНСПОРТНОЙ ИНФРАСТРУКТУРОЙ Г. САРАНСКА

(Самарский национальный исследовательский университет
имени академика С.П. Королёва)

В крупных городах конфигурация улично-дорожной сети (УДС) сложна, на нее накладываются сети различных видов общественного транспорта. Поэтому для управления такой системой и для решения серьезных транспортных задач в крупных городах используются транспортные модели [1]. Под транспортной моделью будем понимать представление УДС с ее характеристиками, такими как скоростной режим, фазы светофоров, знаки регулирования и количество полос, информацию о маршрутах движения общественного транспорта, размещении остановок, расположении зданий и растительности. Наличие транспортной модели позволяет планировать транспортную систему урбанизированной территории, в которой изменения в одной из частей ведут к изменению в других частях. С помощью такой модели можно оценить будущую загрузку проектируемого участка УДС, результаты изменения маршрутов общественного транспорта [3].

Создание транспортной модели г. Саранска выполняется в интеллектуальной геоинформационной системе ITSGIS [2]. Сбор данных осуществляется панорамной геоинформационной лабораторией, которая осуществляет геопривязанную видеозапись определенного участка (рис. 1) УДС. Далее в системе обработки данных полевых обследований WayMark оператор производит обработку полученных материалов: определяет типа и вычисляет точное место дислокации геообъекта транспортной модели.

При построении транспортной модели на электронную карту г. Саранска дислоцируются технические средства организации дорожного движения, такие как: дорожные знаки, остановки общественного транспорта, дорожные и пешеходные ограждения, светофоры, световые опоры со светильниками, линии дорожной разметки (рис. 2).

При нанесении конкретного геообъекта заносится сопутствующая ему информация. Так при установке ограждения указываются класс ограждения, назначение, материал, геометрические характеристики, а также дата установки