

вались источники [1,2,6]. При срабатывании прерывания, эти значения будут проанализированы и, затем скорректированы углы поворота соответствующих сервоприводов. Данный алгоритм управления минимизирует нагрузку на микроконтроллер, позволяя ему решать другие более важные задачи, кроме того количество сервоприводов, подключаемых к микроконтроллеру и управляемых отдельно, может достигать количества выводов на портах.

Единственным недостатком является отсутствие реализации плавного управления в фоновом режиме, т.е. используя основную программу реализовать плавное перемещение вала удалось, а в фоновом режиме пока это не реализовано, что приводит к неэффективному использованию ресурсов микроконтроллера или к рывкам при работе сервоприводов. Но проблема в принципе решается, нужно лишь сделать решение максимально простым и быстрым, так как наш микроконтроллер (ATMEGA8, 8 MHz) не может похвастаться высокой скоростью обработки информации, особенно для реальных чисел. Данной цели в работе не ставилось, но это является целью следующей разработки.

Литература.

1. Richard H Barnett, Sarah Cox, Larry O'Cull; Embedded C Programming and the Atmel AVR; 560 pages; 2006; ISBN 978-1-4180-3959-2.
2. Joe Pardue; C Programming for Microcontrollers Featuring ATMEL's AVR Butterfly and WinAVR Compiler; 300 pages; 2005; ISBN 978-0-9766822-0-2.
3. Maik Schmidt; Arduino : A Quick Start Guide; 276 pages; 2011; ISBN 978-1-934356-66-1.
4. F Barrett, Daniel Pack, Mitchell Thornton; Atmel AVR Microcontroller Primer : Programming and Interfacing; Steven; 194 pages; 2007; ISBN 978-1-59829-541-2.
5. Ronald Willem Besinga; Microcontrollers and Electronics Project Blog: Working with Atmel AVR Microcontroller Basic Pulse Width Modulation (PWM) Peripheral; <http://www.ermicro.com/blog/?p=1971>; 2011.
6. Steven F. Barrett and Daniel J. Pack; Atmel AVR Microcontroller. Primer: Programming and Interfacing; 195 pages; 2008; ISBN: 9781598295412

## НЕКОТОРЫЕ ВОПРОСЫ ЗАЩИТЫ ПЕРСОНАЛЬНОЙ ИНФОРМАЦИИ

*М.В. Момот, к.т.н., доцент*

*Юргинский технологический институт (филиал) Национального исследовательского*

*Томского политехнического университета*

*652055, Кемеровская обл., г. Юрга, ул. Ленинградская, 26, тел. +79235036074*

*E-mail: momotmvu@ya.ru*

В современном мире (2014 год) зависимость человечества от компьютеров и компьютерных сетей стала критично высокой, более того, за счет роста скоростей обмена информацией в сети Интернет, происходят качественные скачки. Так, согласно информации международной консалтинговой компании J'son&Partners Consulting, рынок он-лайн игр динамично развивается и постоянно растет и вырос с 16,4 млрд. USD (2010 г.) до 26,7 млрд. USD (2013 г.) [1]. За последние годы значительно вырос рынок интернет торговли, по данным из различных источников рынок растет приблизительно на 15% в год. Буквально все мировые банки на сегодняшний день применяют электронные системы управления счетами клиентов посредством удаленных каналов связи (в основном, для физических лиц, это интернет). Успешно, хоть и не столь динамично развиваются sms сервисы (из-за дороговизны).

В этой среде, естественно, как и в любой среде деятельности человека, появляется возможность незаконного обогащения, и наша задача рассмотреть какие опасности подстерегают современного человека, пользующегося современными банковскими сервисами и другими сервисами, которые также используют интернет.

**Вредоносные программы.** Ранее это были вредоносные вирусы (самостоятельно распространяющиеся программы), которые повреждали информацию или просто безобидно множилось. Основная цель вирусописателей была - самоутверждение. Но со временем, стало очевидно, что на данном типе программ можно зарабатывать, например, воруя пароли к различным интернет ресурсам, или почтовым службам, и вынуждая владельцев за плату их выкупать. Затем, когда появился интернет-банкинг, пароли стали предоставлять доступ к более интересной информации, и у злоумышленников появились возможности завладеть управлением чужими банковскими счетами, что позволило уже работать более масштабно и безнаказанно. Взламывался аккаунт, деньги переводились на другие счета, и к тому времени, когда владелец счета уже начинает что-либо понимать, деньги вернуть было уже практически не возможно.

**А теперь рассмотрим наиболее распространенные современные опасности.** Я думаю бессмысленно рассматривать типы вирусов, но их влияние рассмотреть гораздо важнее. Как правило, но не обязательно, установке пользователем вредоносного кода на свой компьютер предшествует установка распространенных программ взятых с сетевых ресурсов сомнительной репутацией. Более подробно узнать о типах вирусах можно на сайтах производителей антивирусных программ, более подробно они (антивирусы) будут рассмотрены ниже.

Программы, ворующие пароли. После установки программа либо сканирует клавиатуру, либо считывает пароли, сохраненные на компьютере. Затем данная информация передается злоумышленникам (посредством интернет), анализируется в автоматическом либо полуавтоматическом режиме. И, если информация оказалась интересной, злоумышленники начинают действовать от вашего имени, например, управляют вашим банковским счетом, начинают рассылку подложных электронных писем от вашего имени и т.д.

Программы, предоставляющие злоумышленникам возможность управления компьютером. После установки программа вносит изменения в операционную систему компьютера с целью подключения его к бот-сети, такое возможно, если сама по себе информация, хранимая и обрабатываемая на вашем компьютере, не представляет интереса для злоумышленников, но их интересуют технические ресурсы машины (скорость обработки информации, наличие канала связи, наличие свободной дисковой памяти). Теперь ресурсы компьютера используются для целей злоумышленников, например, для дешифровки документов, для взлома паролей, для рассылки спама, для организации сетевых атак, для замечания следов своей деятельности по отношению к другим объектам информационной сети.

Программы, модифицирующие отображение информации в браузерах - всплывающие окна с рекламой, подмена рекламных баннеров. Данные программы устанавливаются в качестве дополнений к браузерам и модифицируют получаемую пользователем информацию, дополняя ее навязчивой рекламой, которая, из-за ошибок в коде, в некоторых случаях может блокировать доступ к определенным сайтам и службам. Несмотря на свою кажущуюся безвредность, данные программы не исключают возможность нанесения более серьезного урона, например, в них встречаются функции сбора паролей.

Сайты, вводящие в заблуждение, выманивающие конфиденциальную информацию. Здесь о заражении речи не идет, хотя не редко переходу на данный сайт предшествует установка программ модифицирующих отображение информации в браузере. Сайты подобного типа предлагают определенные услуги, бесплатно, либо за небольшую плату, но требуют для "проверки" клиента ввода дополнительной информации, например ответного кода на СМС или реквизитов кредитной карты. Как правило, это заканчивается для клиентов потерей денег.

Программы вымогатели блокируют работу компьютера, требуя отправки платной смс на определенный телефонный номер, и разблокируют работу после ввода ответного кода.

По более детальной информации о вредоносных программах обратитесь на сайты производителей антивирусов, на них обязательно есть соответствующие разделы, в которых довольно детально объясняется все, что касается данной темы.

**Теперь рассмотрим степень вредоносного влияния данных групп.** С точки зрения рядового пользователя наиболее опасны программы ворующие пароли и сайты вводящие в заблуждение, с точки зрения интернет-бизнеса, например интернет-магазин, опасны бот-сети т.к. могут полностью блокировать работу и привести к серьезным финансовым потерям. Программы, модифицирующие отображение информации в браузерах могут привести к потерям компаний путем отмены их рекламы, но вряд ли это влияние существенное, сайты вводящие в заблуждение или похожие на серьезные интернет-проекты до смешения могут отрицательно повлиять на имидж компании и привести к потере клиентов, но степень их опасности нельзя оценить как высокую. Программы вымогатели блокируют работу конкретного компьютера и не причиняют более вреда помимо случаев, если вы решили платно по смс попытаться решить проблему и потеряли некоторое количество денег.

**Теперь рассмотрим, каким образом можно противостоять данным угрозам.** Конечно, все зависит от того, для каких целей используется компьютер. Если только для работы с текстовыми документами и выхода в интернет, то я рекомендую, как наиболее дешевый и надежный вариант, использовать операционную систему семейства Linux, например, Debian, Fedora, Gentoo, Mandriva, Slackware SUSE/openSUSE, Ubuntu, Android, но если на компьютере требуется запускать специализированные Windows приложения, пользоваться расширенными функциями MSOffice, то могут возникнуть трудности. В этом случае на компьютер нужно устанавливать ОС Windows, а это стоит зна-

чительных средств (при соблюдении лицензионных соглашений) более того, значительные средства стоит программное обеспечение, но речь не об этом. Дело в том, что на персональном компьютере с ОС Windows вам не обойтись без антивирусной программы, которая также не бесплатна, стоит отметить, что стоимость лицензионного программного обеспечения при этом приближается к стоимости "железа". Конечно, хорошо, если вы работаете в огромной корпорации, которая заботится о своих сотрудниках и предоставляет лицензии бесплатно, например, я пользуюсь подобной лицензией, как на ОС так и на ряд специализированного и довольно дорого ПО, но антивирус приходится оплачивать самому. Если же вы не имеете лицензии на ОС Windows и воспользовались установкой взломанной ОС, то не исключена вероятность, что в нее уже встроены вредоносные программы, которые активизируются с установкой. Если же вы пытаетесь установить взломанный антивирус, то столкнетесь с подобной проблемой в 100% случаев.

Рассмотрим теперь самые распространенные антивирусные пакеты, сравним их стоимость и функционал, упор сделаем на рядового не корпоративного пользователя, например пытающегося защитить свои домашние компьютеры.

Таблица

Наиболее распространенные антивирусные программы.

Компания производитель	Наличие бесплатной версии без ограничения по времени	Стоимость одной лицензии стандартной (нерасширенной на 1 год - руб.)	% скидки на следующий год (продление)	Затраты за 3 года (руб.)	Каким антивирусом пользуетесь (опрос)*
Avast	Да	600	50%	1200	22,8%
AVG	Да	743	30%	1783,2	6,4%
Avira	Да	1198	50%	2396	3,7%
Bitdefender	Нет	764,25	34%	1773,065	0
COMODO	Да	1,521,26	34%	3529,322	0
Dr.web	-	990	40%	2178	12,8%
Emsisoft	Нет	895	25%	2237,5	0
ESET	Нет	1180**	36%	2690,4	16,4%
G DATA	Нет	950		2850	
Kaspersky	Нет	1200***	35%	2760	35,6%
McAfee	Нет	999	54%	1918,08	2,3%
Microsoft Security Essentials	Да	****	-	0	0
NANO AntiVirus	Да	0	0	0	0
Panda	Да *****	878	20%	2282,8	0
Simantec	Нет	990	66%	1663,2	0
Trend micro	Нет	797,50	32%	1882,1	0
TrustPort	Нет	760	65%	1292	0

\*опрос проводится в социальной сети «ВКонтакте», ссылка есть на моей странице ([vk.com/id161424404](https://vk.com/id161424404)); \*\*на 3 устройства (по одному не продается); \*\*\*на 2 устройства (по одному не продается); \*\*\*\*распространяется в составе Windows XP, 7, 8; \*\*\*\*\*в облаке.

Представленные антивирусные программы наиболее популярны и/или представлены продавцами на российском рынке. Можно долго и разносторонне описывать их преимущества и недостатки, приводить примеры тестирования данных продуктов различными аналитическими группами с выставлением им рейтинга, но, к сожалению или счастью, разные рейтинги публикуют абсолютно разные результаты ([2,3,4,5,6]). Поэтому функциональности антивирусных программ мы касаться не будем. Примем, и это является почти истинной, что все данные продукты обладают примерно одинаковой функциональностью и защищают от всех угроз приблизительно на одинаковом уровне (за исключением чисто бесплатных продуктов (Microsoft Security Essentials, NANO AntiVirus), функциональность которых ограничена. Из этого и будем исходить, и проанализируем другую составляющую - стоимость владения. В таблице приведены затраты за 3 года владения продуктом, здесь ценовым лидером оказался Avast. При использовании нескольких устройств неплохой альтернативой является

антивирус лаборатории Касперского. Фирма Simantec, предоставляет свой продукт на 60 дней (тестовый период) вместе с новыми компьютерными материнскими платами, а затем можно продлить продукт, это обойдется в 250-300 рублей в год за лицензию, что тоже очень выгодно. У компании Dr.web тоже неплохие показатели, но, не смотря на былую популярность, продукты данной фирмы лишь на 4 месте согласно опросу. Лично мною был опробован Microsoft Security Essentials, но имеет длительную (до недели) задержку с обновлением сигнатур вирусов, но в целом довольно не плох и прост в применении. McAfee также распространяется с новыми компьютерами, видимо за счет этого и имеет некоторую популярность 2,3%.

Мы проанализировали рынок антивирусных продуктов в разрезе домашнего использования, провели опрос их популярности, отразили ценовые характеристики, сделали некоторые выводы. Но конкретных рекомендаций дать довольно трудно, т.к. любой антивирус ограничен и нуждается в умелом использовании. Но если вам хочется бесплатный продукт, пользуйтесь Avast или Microsoft Security Essentials, а в некоторых случаях можно и не использовать антивирус, а установить операционную систему семейства Linux.

Литература.

1. Российский рынок онлайн-игр, 2010-2016 гг. [Электронный ресурс]. - Режим доступа: [http://www.json.ru/files/reports/2012-10-03\\_MW\\_Online\\_Games\\_RU.pdf](http://www.json.ru/files/reports/2012-10-03_MW_Online_Games_RU.pdf), свободный. – Загл. с экрана.
2. Рейтинг антивирусов [Электронный ресурс]. - Режим доступа: <http://bezopasnostpc.ru/antivirusi/rejting-antivirusov-faerovolov-kompleksnyih-resheniy-2012>, свободный. – Загл. с экрана.
3. Рейтинг антивирусов 2013 [Электронный ресурс]. - Режим доступа: [http://securico.ru/tests/raiting\\_antivir\\_2013](http://securico.ru/tests/raiting_antivir_2013), свободный. – Загл. с экрана.
4. В. Чугунков Масштабное тестирование быстродействия и эффективности антивирусов (март 2013) [Электронный ресурс]. - Режим доступа: [http://www.compbegin.ru/articles/view/\\_94](http://www.compbegin.ru/articles/view/_94), свободный. – Загл. с экрана.
5. Best Antivirus Software Review [Электронный ресурс]. - Режим доступа: <http://anti-virus-software-review.toptenreviews.com/>, свободный. – Загл. с экрана.
6. John Corpuz Free Antivirus Software: The Best of 2013 [Электронный ресурс]. - Режим доступа: <http://www.tomsguide.com/us/best-free-antivirus-software-2013,review-1788-3.html>, свободный. – Загл. с экрана.

### **АНАЛИЗ МЕДИАРЫНКА РОССИИ**

*А.В. Сушко, ассистент кафедры ЭиАСУ*

*Юргинский технологический институт (филиал) Национального исследовательского  
Томского политехнического университета  
652055, Кемеровская обл., г. Юрга, ул. Ленинградская, 26, тел. 8 (38451) 6-44-32  
E-mail: sushko.a.v@mail.ru*

Каждый вид рекламы по-своему привлекателен и уникален. Чтобы реклама приносила пользу, прежде всего, необходимо правильно выбрать средство массовой информации, с помощью которого рекламодатель хочет сообщить о себе или своей продукции. Реклама – средство достаточно дорогое, поэтому необходимо грамотно планировать рекламный бюджет с учетом аудитории, на которую ориентируется организация при составлении рекламного обращения.

Реклама на ТВ – отлично, очень дорого, в общем, как и все хорошее. При подаче рекламы на телевиденье необходимо правильно выбрать канал, эфирное время и частоту показом, и все это делается, непосредственно, с учетом интересов аудитории, к которой и будет направленно рекламное сообщение. Реклама на телевидение создает сказку, её не надо читать, как в газете, либо просто слушать – как по радио, она проникает в наше сознание. При помощи данного вида рекламы можно достаточно много рассказать о товаре и способов его употребления. Дорого, но эффективно! По аудиторным показателям, лидерами в данном сегменте медиа по России являются - «Первый Канал», «Россия 1», и «НТВ».

С помощью радио очень хорошо передать всю необходимую информацию в течение всего дня. Радио охватывает такие категории людей, до которых не доходит ТВ и пресса, например, отдыхающих на природе, автомобилистов и дальнобойщиков и т.п. Мобильность, гибкость и дешевизну радио высоко ценят рекламодатели. Притом, что цены на радиоролик гораздо меньше, чем цены на